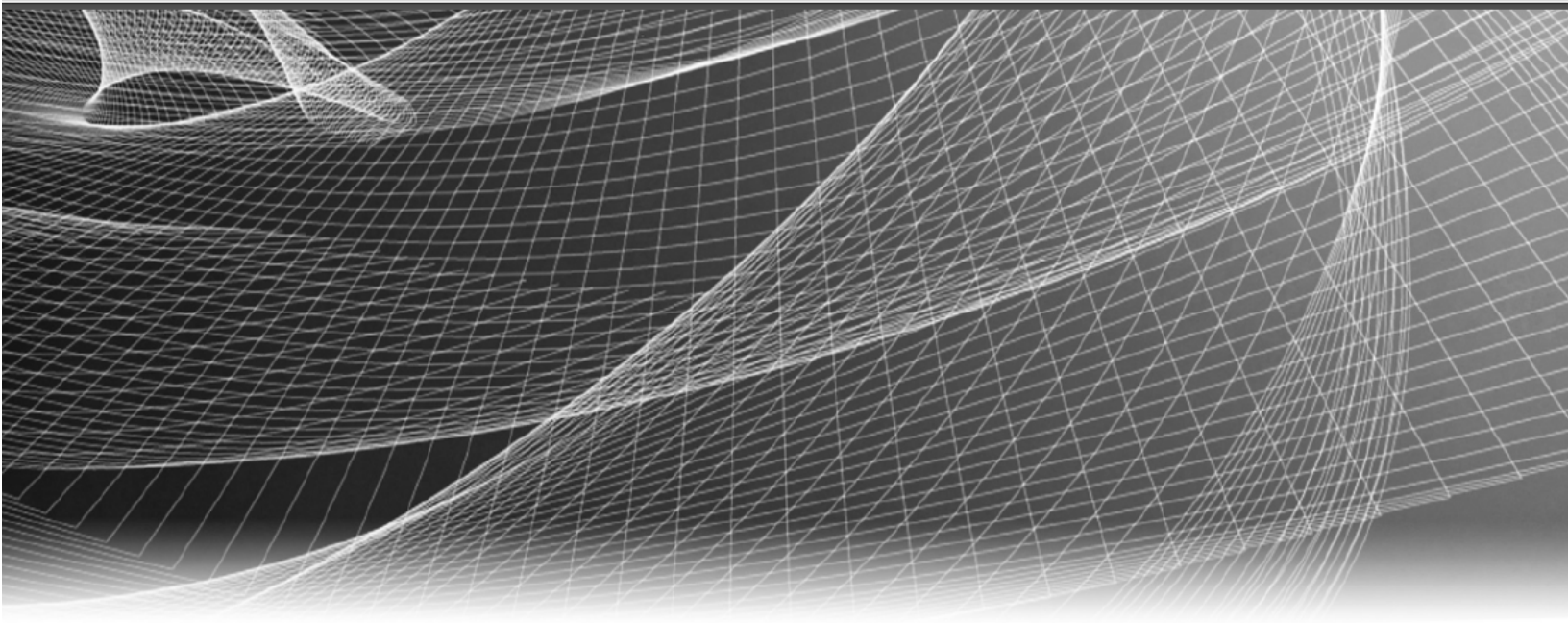


RSA Security Analytics

Guía de Reporting

para la versión 10.6

RSA EMC²

Marcas comerciales

Acuerdo de licencia

Licencias de otros fabricantes

Nota sobre tecnologías de cifrado

Distribución

Contenido

Descripción general **16**

Administrar el acceso para el módulo Reporting 18

Agregar una función y asignar permisos para el módulo Reporting 21

Navegar a la pestaña Funciones 22

Agregar una función y asignar permisos 23

Guías para informes 24

Reglas de NWDB 24

Configuración de tiempo de espera agotado para reglas de NWDB 27

Acción LookupAndAdd Rule 30

Informes de valores de lista 34

Buscar detalles de Reporting 34

Requisitos previos 35

Procedimiento 35

Sintaxis de búsqueda y distintos tipos de búsqueda 36

Solución de problemas 41

Solución de problemas antes de configurar el servidor SFTP. 41

Definiciones: 42

Solución de problemas de la sintaxis de reglas de NWDB en una instalación nueva 43

Solución de problemas de sintaxis de reglas de NWDB en la actualización 43

Solución de problemas de reglas de importación 43

Procedimiento 44

Descripción general de una regla 44

Elementos esenciales de una regla 44

Sintaxis de reglas de IPDB 46

Sintaxis de valores literales (datos) compatible 47

Sintaxis IN no compatible 48

Sintaxis LIKE no compatible 48

Sintaxis LIST compatible 48

Sintaxis LIST no compatible 49

Sintaxis variable compatible 49
Sintaxis variable no compatible 49
Sintaxis de la cláusula select compatible 49
Sintaxis de la cláusula select no compatible 50
Sintaxis de la cláusula where compatible 51
Sintaxis de la cláusula where no compatible 54
Sintaxis de la cláusula order by compatible 54
Sintaxis de la cláusula group by compatible 54
Funciones adicionales compatibles 55
Operadores admitidos 55
Ejemplo de consultas compatibles 56
Ejemplo de consultas no compatibles 56
Sintaxis de reglas de NWDB 57
Regla agregada 59
Agregación de recopilación 60
Agregación de metadatos 61
Funciones agregadas de metadatos compatibles 62
Consulta de agregado para múltiples metadatos 64
dedup (string field) 69
filter_on (string filter, string field, bool matchExact) 72
regex (string regex, string field) 99
sum_values() 103
show_whats_new() 105
Tipos de regla 111
Implementaciones del servicio IPDB Extractor compatibles en ambientes virtuales 112
Plataformas de VMware compatibles 112

Definir reglas y grupos de reglas 116
Agregar un grupo de reglas 116
Definir una regla 117
Requisitos previos 117
Procedimiento 118
Requisitos previos 119
Procedimiento 120
Requisitos previos 124
Procedimiento 124
Probar una regla 126
Ajustar reglas de IPDB 128
Ejemplo del caso 1: Variable indexada con operador AND 130
Ejemplo del caso 5: Variable indexada con función LIKE 133
Ejemplo del caso 3: Variable indexada con operador OR 134
Usar alias de metadatos para Reporting Engine 135
Definiciones de alias que suministra RSA 137
eth.type 138
ip.proto 142
medium 145
Servicio 146
tcp.dstport 148
tcp.srcport 150
udp.dstport 152
Eliminar una regla 153
Eliminar un grupo de reglas 153
Duplicar una regla 154
Editar una regla 154
Exportar una regla 156

Exportar un grupo de reglas 156
Importar reglas y grupos de reglas 157
Ver dependientes de una regla 158
Administrar el acceso para una regla o un grupo de reglas 160
Control de acceso para un grupo de reglas 161
Control de acceso para una regla 164
Lista tabular 167
Establecer el control de acceso para una regla 167
Establecer el control de acceso para un grupo de reglas 169
Crear un gráfico mediante una regla 170
Requisitos previos 170
Procedimiento 171
Crear un informe mediante una regla 171
Requisitos previos 171
Procedimiento 172
Crear una alerta mediante una regla 172
Requisitos previos 172
Procedimiento 173

Descripción general de un informe 174

Definir grupos de informes e informes 175
Agregar un informe 175
Agregar un grupo de informes 176
Eliminar un informe 177
Eliminar un grupo de informes 178
Duplicar un informe 179
Editar un informe 180
Exportar un informe 181
Abrir archivos CSV con caracteres Unicode en MS Excel 181
Exportar un grupo de informes 182
Importar informes y grupos de informes 183
Actualizar una lista de grupos o informes 184
Ver una lista de todos los informes 185
Ver un informe 187
Requisitos previos 188

Procedimiento 189
Los próximos pasos 195
Ejemplos 196
Basada en la duración absoluta: 196
Basada en la duración relativa: 197
Requisitos previos 198
Procedimiento 198
Requisitos previos 198
Procedimiento 199
Los próximos pasos 200
Requisitos previos 200
Procedimiento 200
Requisitos previos 201
Procedimiento 201
Requisitos previos 202
Procedimiento 203
Eliminar un informe programado 203
Editar un informe programado 204
Administrar el acceso para un informe o un grupo de informes 209
Control de acceso para un grupo de informes 210
Control de acceso para un informe 212
Lista tabular 216
Establecer el control de acceso para un informe 217
Establecer el control de acceso para un grupo de informes 219
Investigar un informe 220
Requisitos previos 221
Procedimiento 221
Los próximos pasos 222
Administrar y seleccionar un logotipo de informe 222

Requisitos previos 222
Administrar logotipos de informe 222
Seleccionar un logotipo 223
Usar variables para creación de informes con parámetros 224
Ver las direcciones IP de origen para un país de destino específico 225
Informe con variables dinámicas 226
Ver todas las direcciones IP de destino para una dirección IP de origen 230
Asociar una variable a una lista de valores 231
Regla de IPDB para ver los detalles de un dispositivo de acuerdo con el nombre del dispositivo 232
Informe iterativo 234

Trabajar con gráficos en el módulo Reporting 239

Descripción general de un gráfico 239
Definir grupos de gráficos y gráficos 240
Agregar un gráfico 240
Agregar un grupo de gráficos 242
Eliminar un gráfico 243
Eliminar un grupo de gráficos 244
Desactivar un gráfico 245
Arrastrar y soltar un gráfico en un grupo 245
Duplicar un gráfico 246
Editar un gráfico 246
Activar un gráfico 248
Exportar un gráfico 249
Exportar un grupo de gráficos 249
Importar gráficos y grupos de gráficos 250
Actualizar grupo o lista de gráficos 251
Buscar un gráfico existente 252
Ver la lista de todos los gráficos 253
Ver un gráfico 254
Administrar el acceso para un gráfico o un grupo de gráficos 256
Control de acceso para un grupo de gráficos 257
Control de acceso para un gráfico 260
Control de acceso para un gráfico cuando se seleccionan múltiples gráficos 263
Lista tabular 264
Establecer el control de acceso para un gráfico 265

Establecer el control de acceso para un grupo de gráficos 267
Probar un gráfico 268
Requisitos previos 269
Procedimiento 269
Investigar un gráfico 269
Requisitos previos 270
Procedimiento 270

Trabajar con alertas en el módulo Reporting 272

Descripción general de una alerta 272
Definir alertas 273
Agregar una alerta 273
Eliminar una alerta 277
Desactivar una alerta 278
Editar una alerta 278
Activar una alerta 279
Exportar una alerta 280
Importar una alerta 281
Actualizar una lista de alertas 282
Definir plantillas de alertas 282
Agregar una plantilla 283
Eliminar una plantilla 284
Editar una plantilla 285
Ver todas las plantillas 286
Administrar el acceso para una alerta 287
Control de acceso para una alerta 287
Establecer el control de acceso para una alerta 291
Requisitos previos 291
Procedimiento 292
Configurar Security Analytics para que genere una alerta 293
Procedimiento 293
Desactivar una alerta calendarizada 293
Ver una lista de alertas 294
Ver calendario de alertas 295
Investigar una alerta 296
Requisitos previos 296
Procedimiento 296

Procedimiento 296
Configurar el motor de creación de informes para enviar mensajes de Sylog mediante TCP/TLS para las alertas 297
Requisitos previos 297
Procedimiento 297
Trabajar con listas en el módulo Reporting 300
Descripción general de listas 300
Definir listas y grupos de listas 300
Agregar una lista 301
Agregar un grupo de listas 302
Eliminar una lista 304
Eliminar un grupo de listas 305
Duplicar una lista 306
Editar una lista 306
Exportar una lista 308
Exportar un grupo de listas 309
Importar listas y grupos de listas 310
Administrar el acceso para una lista o un grupo de listas 311
Control de acceso para un grupo de listas 311
Control de acceso para una lista 313
Lista tabular 315
Establecer el control de acceso para una lista 316
Establecer el control de acceso para grupos de listas 317
Referencias del módulo Reporting 319
Referencias de alertas 320
Barra de herramientas de Plantilla 323
Lista de plantillas 323
Cuadro de diálogo Permisos de alerta 323
Vista Alerta 325
Vista Crear o modificar alerta 328
Pestaña Registro 332
Pestaña SMTP 333
Pestaña Syslog 334

Cuadro de diálogo Importar alerta 337
Referencias de plantillas 338
Panel Ver alertas 338
Características 339
Barra de herramientas de Ver alertas 339
Lista Ver alertas 340
Vista Ver calendario de alertas 340
Características 341
Panel de barra de herramientas Calendario de alertas 342
Panel Lista de calendario de alertas 342
Referencias de gráficos 343
Vista Crear gráfico 343
Cuadro de diálogo Permisos de gráficos 344
Vista Gráfico 346
Características 347
Panel Grupos de gráficos 347
Barra de herramientas Gráficos 348
Lista de gráficos 349
Cuadro de diálogo Importar gráfico 350
Panel Ver un gráfico 352
Vista Probar un gráfico 355
Características 356
Barra de herramientas Gráficos 356
Salida del gráfico 357
Opciones de gráficos 357
Referencias de listas 358
Vista Crear lista 359
Cuadro de diálogo Permisos de listas 361
Vista de lista 363

Características 364
Panel Grupos de listas 364
Barra de herramientas Lista 365
Panel de la vista Lista 366
Referencias de informes 366
Características 368
Panel de opciones 368
Panel Salida 369
Características 371
Características 373
Panel Calendarizar informe 373
Panel Acciones de salida 377
Panel Lista dinámica 380
Panel Logotipo 380
Características 382
Barra de herramientas Informes calendarizados 382
Panel Lista de informes calendarizados 383
Características 386
Fair Scheduler 387
Capacity Scheduler 387
Vista Crear informe 387
Cuadro de diálogo Importar informe 391
Cuadro de diálogo Permisos de informes 393
Vista Informe 395
Características 396
Panel Grupos de informes 396

Barra de herramientas Informe 397
Panel Lista de informes 397
Referencias de calendarios 398
Cuadro de diálogo Seleccionar un logotipo 399
Panel Ver todos los informes 400
Características 401
Barra de herramientas Informes 402
Panel Salida de informes 403
Panel Calendario de informes 403
Panel Hora de informes 404
Panel Ver un informe 404
Características 405
Referencias de reglas 407
Sintaxis general de una regla avanzada 408
Informe por hora, diario, semanal y mensual 411
Informes por hora 411
Informe diario 411
Informe semanal 412
Informe mensual 412
Partición de la tabla basada en informe de ubicación 415
Registros de combinación y sesiones basados en informe unique_id 417
Informe de lista 418
Informe con parámetros 419
Tabla basada en partición con varias ubicaciones 420
Partición automatizada mediante función personalizada 423
Sintaxis general 423

Informe Todas las categorías de eventos 426
Informe Categorías de eventos de ataques 428
Fuente: Informe Categorías de eventos de China 429
Informe Categorías de eventos de direcciones IP de origen y destino 431
Informe Categorías de amenazas por tiempo 433
Informe Consulta de arreglo 435
Informe Consulta de registro crudo 437
Vista Crear regla 441
Panel Regla 442
Cuadro de diálogo Probar regla 445
Panel Metadatos 447
Panel Lista 448
Agregados de consulta 449
Count 450
Ejemplo 450
Countdistinct 452
Ejemplo 453
Distinct 454
Ejemplo 454
Primero 456
Ejemplo 456
Última 458
Ejemplo 458
Suma 460
Ejemplo 460

Prom. 462
Ejemplo 462
Max y Min 464
Ejemplo 465
Filtrar resultados de metadatos agregados con Max_threshold 466
Filtrar resultados de metadatos agregados con Min_threshold 468
Longitud 470
Ejemplo 470
Información adicional 472
Cuadro de diálogo Permisos de regla 473
Vista Regla 476
Especificación de orígenes de eventos de IPDB 481
Modos de definición de reglas de la base de datos de Warehouse 482

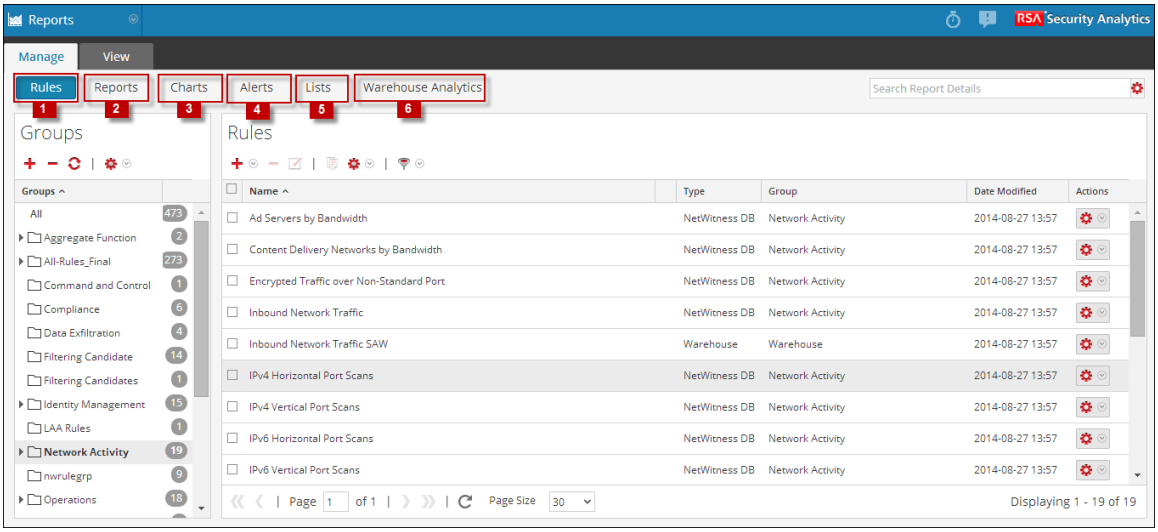
Descripción general

En esta guía se describen las características y las funcionalidades del módulo Reporting de Security Analytics. El módulo Reporting lleva las reglas de Security Analytics a una única vista para definir, programar y ver informes.

El módulo Reporting permite crear, administrar y ver lo siguiente:

- Reglas
- Reports
- Gráficos
- Alertas
- Listas
- Warehouse Analytics

Puede navegar a diferentes secciones (etiquetadas en la siguiente figura) desde la interfaz del usuario de Reporting.



Utiliza el **enfoque de interfaz del usuario con pestañas**, en el cual cuando se hace clic en cada una de las tareas (crear, editar, programar y ver), se carga una nueva pestaña sin tener que abrir varias ventanas para cada una de las distintas tareas. Puede informar y alertar sobre los datos de registros y paquetes recopilados, y personalizar los informes y los gráficos para mejorar la apariencia visual. Puede crear informes en tiempo real para los datos históricos. Puede crear gráficos y dashlets, los cuales también se pueden agregar a los dashlets de gráfico en tiempo real.

El módulo Reporting depende de Reporting Engine para proporcionar datos para los informes, las alertas y los gráficos. Por lo tanto, debe configurar Reporting Engine antes de poder generar los informes. También debe especificar el origen de datos en Reporting Engine desde donde se extraen los datos.

En la siguiente tabla se señalan las tareas que se deben realizar en el módulo Reporting, en el orden en que debe ejecutarlas:

Nota: Asegúrese de tener acceso a los componentes del módulo Reporting. Consulte Agregar una función y asignar permisos para el módulo Reporting.

Paso	Descripción
1	Definir una regla.
2	Probar una regla.
3	Definir reglas y grupos de reglas en función de cómo Crear un informe mediante una regla.
4	Requisitos previos.
5	Requisitos previos.
6	Crear un gráfico mediante una regla.
7	Crear una alerta mediante una regla.
8	Investigar un informe, Investigar un gráfico o Investigar una alerta.
9	Agregar una lista.
10	Definir un trabajo. Para obtener detalles, consulte **Definir un trabajo de Warehouse Analytics** en la *Guía de Warehouse Analytics*.

Los datos que puede informar o alertar dependen de la configuración de Reporting Engine y de los orígenes de datos que especifica como parte de la definición de la regla.

Nota: Asegúrese de tener acceso a los orígenes de datos requeridos. Solo los usuarios con privilegios con acceso a información confidencial tienen permiso para ciertos orígenes de datos. Para administrar el control de acceso a orígenes de datos, consulte el tema **Agregar una función y asignar permisos para Warehouse Analytics** de la *Guía de Warehouse Analytics*. Sin embargo, para los informes, las alertas y los gráficos existentes, si la función o los permisos del usuario se modifican para los orígenes de datos, esto no se aplica a menos que actualice manualmente los permisos.

Reporting Engine es un componente clave que proporciona datos al módulo Reporting. Debe agregar Reporting Engine como un servicio a Security Analytics antes de generar informes o alertas. Cuando ejecuta los informes, los resultados se almacenan en Reporting Engine.

Después de generar un informe, puede realizar lo siguiente:

- Enviar los informes por correo electrónico a otros usuarios mediante la configuración de acciones de salida. Puede configurar las acciones de salida antes de generar un informe.
- Descargar los informes como archivos con formato PDF o de valores separados por comas (CSV).

Una vez creada una alerta, Security Analytics Incident Management recopila estos datos desde Reporting Engine y muestra estas alertas en la interfaz del usuario de Security Analytics.

Nota: De forma predeterminada, esta opción no está activada. Si desea habilitar esta opción, debe hacerlo en la página Configuración de Reporting Engine.

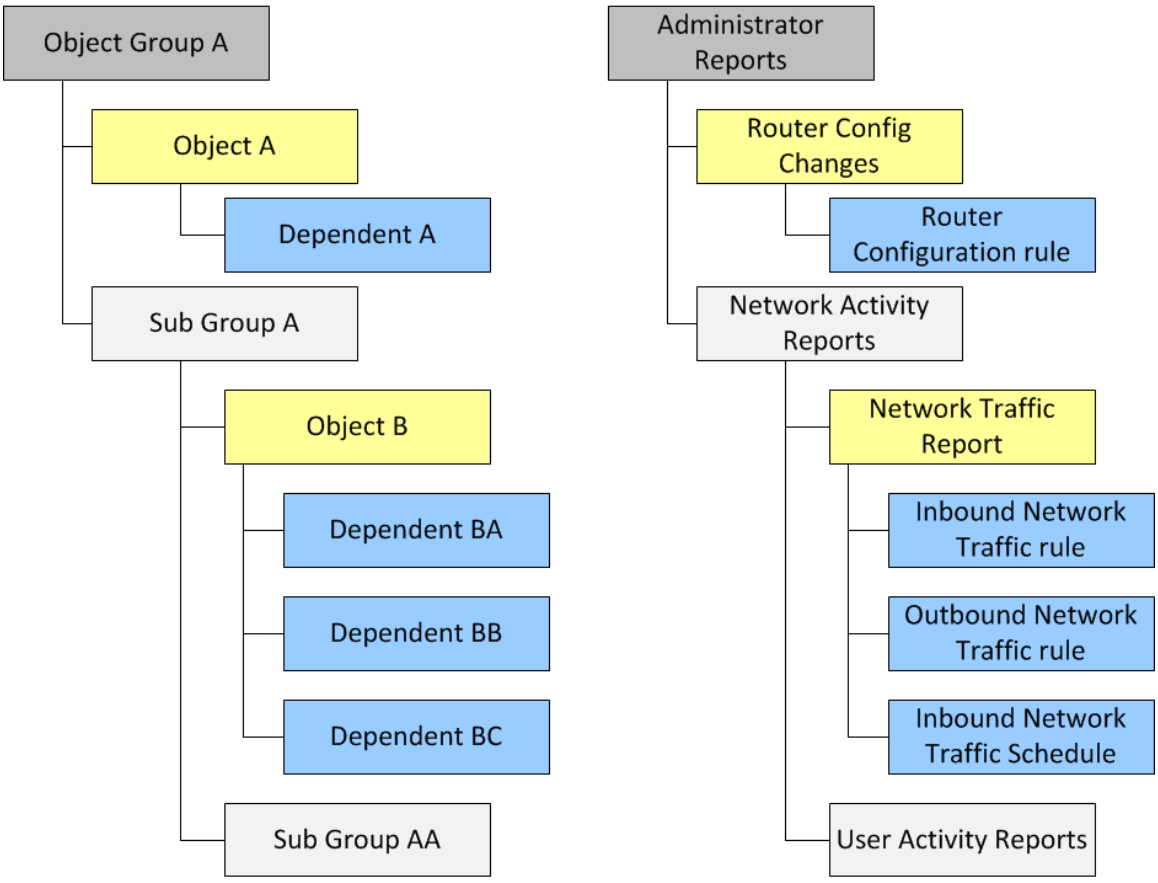
Nota: Se puede acceder a este módulo según el acceso basado en funciones definido para el usuario.

Administrar el acceso para el módulo Reporting

En esta sección se describen los permisos de acceso que puede especificar el usuario para los diversos objetos del módulo Reporting. El módulo Reporting ofrece la opción de configurar el control de acceso para todos sus componentes. En Security Analytics, puede definir distintas funciones y especificar el control de acceso para cada una de ellas desde el módulo Seguridad del sistema. Puede definir el control de acceso que se proporcionará a cada función para el módulo Reporting. Para obtener más información, consulte **Paso 1: Revisar cinco funciones preconfiguradas** y el **Paso 2: (Opcional) Agregar una función y asignar permisos** en la *Guía de administración de usuarios y de la seguridad del sistema*.

El módulo Reports permite modificar los permisos de función o acceder a los siguientes objetos de Reporting:

El siguiente es un ejemplo de la jerarquía de los grupos de objetos, los objetos y los dependientes. Esta es una ilustración de la jerarquía de grupos de informes e informes.



Jerarquía de grupos de informes e informes

Aplicación de permiso para grupos de objetos

- Debe tener permiso de Lectura y escritura para establecer los permisos para el grupo de objetos, los objetos o los dependientes. Los dependientes con el permiso “Sin acceso” aparecen bloqueados en gris y los dependientes con el permiso de “Solo lectura” se indican con un ícono.
- Cuando configura el permiso para el grupo de objetos, los objetos y los dependientes del grupo de objetos no lo heredan automáticamente. Para hacer que lo hereden, debe seleccionar la opción “Aplicar estos permisos a subgrupos y <objetos> en este grupo”. Por ejemplo, si no desea que las funciones Operadores accedan a informes del Grupo de informes A, debe configurar como Sin acceso el permiso del Grupo A para la función Operador y seleccionar la opción “Aplicar estos permisos a subgrupos e informes en este grupo”.
- Cuando configura los permisos para el grupo de objetos y selecciona la opción “Aplicar estos permisos a subgrupos y <objetos> en este grupo”, los dependientes, como reglas o programas,

en los objetos no heredan los permisos automáticamente. Debe usar la opción “Aplicar permisos de solo lectura a las reglas de <objeto>” para aplicar el permiso a las reglas.

- Cuando configura los permisos para los objetos, debe asegurarse de que los objetos de la jerarquía tengan siempre un permiso que sea menor o igual que el superior en la jerarquía de modo que se aplique el permiso. Por ejemplo, si los informes de un grupo de informes tienen permiso de Lectura y escritura, se aplica un permiso de Solo lectura o Sin acceso en el nivel del grupo de informes y se selecciona la opción “Aplicar estos permisos a subgrupos e informes en este grupo”, el permiso en las reglas permanece sin cambios.
- Los permisos se aplican en cascada de arriba abajo en la jerarquía y no viceversa. Por ejemplo, si aplica un permiso a una regla, esto no cambia el permiso del informe que contiene la regla.

Aplicación de permiso para objetos o dependientes

- Debe tener permiso de Lectura y escritura para establecer los permisos para los objetos o los dependientes.
- Puede especificar el permiso para varios objetos simultáneamente en lugar de configurarlo para cada objeto.
- Cuando configura el permiso para el objeto, los dependientes del objeto no lo heredan automáticamente. Para que lo hereden, debe seleccionar la opción “Aplicar permisos de Solo lectura a las reglas de <objeto>”.

Cuando aplica el permiso a los dependientes, se aplica en función del permiso existente para la función. Por ejemplo, considere a un analista y a un operador con los siguientes permisos para los distintos dependientes (el objeto Informe A tiene la Regla AA, la Regla AB y la regla AC como dependientes).

Objeto o dependiente	Analista	Operador
Informe A	Lectura y escritura	Sin acceso
Regla AA	Lectura y escritura	Sin acceso
Regla AB	Lectura y escritura	Lectura y escritura
Regla AC	Solo lectura	Sin acceso

Cuando el analista aplica un permiso de Lectura y escritura a la función Operador y selecciona la opción “Aplicar permisos de solo lectura a las reglas de <objeto>”, los permisos se configuran para los distintos dependientes de la siguiente manera:

Modificación de los permisos

- **En el nivel de grupo:** configure los permisos en el nivel de grupo de objetos y para todos los objetos y las entidades del grupo. Por ejemplo, si tiene 80 informes en el grupo Informes de administradores y no desea que nadie agregue o modifique estos informes, excepto el administrador, puede configurar como Solo lectura el permiso para todas las demás funciones en el nivel de grupo y seleccionar la opción para aplicarla a todos los informes y subgrupos del grupo de informes.
- **Múltiples objetos:** seleccione múltiples objetos y especifique el acceso para todos los objetos seleccionados. Por ejemplo, si tiene 10 informes en el subgrupo Tráfico de red con información confidencial a la cual no desea que nadie acceda, seleccione los 10 informes y, a continuación, configure el permiso para todas las funciones como “Sin acceso”.
- **Un único objeto:** seleccione solo el objeto y especifique el permiso. Por ejemplo, seleccione el Informe de tráfico de red y especifique el permiso de Lectura y escritura para la función Analista de seguridad o seleccione la Alerta de error al iniciar sesión y especifique el permiso de Lectura y escritura para una función Analista de seguridad.

Objeto o dependiente	Operador (antes de la aplicación del permiso)	Operador (después de la aplicación del permiso)
Informe A	Sin acceso	Lectura y escritura
Regla AA	Sin acceso	Solo lectura
Regla AB	Lectura y escritura	Lectura y escritura
Regla AC	Sin acceso	Solo lectura

Temas

Agregar una función y asignar permisos para el módulo Reporting

Agregar una función y asignar permisos para el módulo Reporting

En este tema se explica cómo agregar una función y cómo asignarle permisos. Aunque Security Analytics tiene cinco funciones preconfiguradas, puede agregar funciones personalizadas. Por ejemplo, además de la función Analistas preconfigurada, puede agregar las funciones personalizadas AnalystsEurope y AnalystsAsia.

Role	Permiso
Administradores	Acceso completo al sistema
Operadores	Acceso a configuraciones, pero no a datos
Analistas	Acceso a datos, pero no a configuraciones
SOC_Managers	El mismo acceso que los analistas, además del permiso adicional para manejar incidentes
Malware_Analysts	Acceso solo a eventos de malware

Según la función del usuario, puede establecer los siguientes permisos de acceso para acceder a los componentes del módulo Reporting (reglas, informes, gráficos, alertas, listas):

- Definir
- Delete
- Exportación
- Administrar
- Ver

Nota: Debe habilitar todos estos permisos para una función de usuario con el fin de poder definir, eliminar, administrar y ver cada uno de los módulos Reporting. También debe tener permisos apropiados para que el origen de datos se enumere mientras define los informes, los gráficos o las alertas. Para obtener más información, consulte el tema Configurar permisos para orígenes de datos en la *Guía de configuración de hosts y servicios*.

Para obtener una lista detallada de los permisos, consulte el tema Permisos de funciones de la *Guía de administración de usuarios y de la seguridad del sistema*.

Navegar a la pestaña Funciones

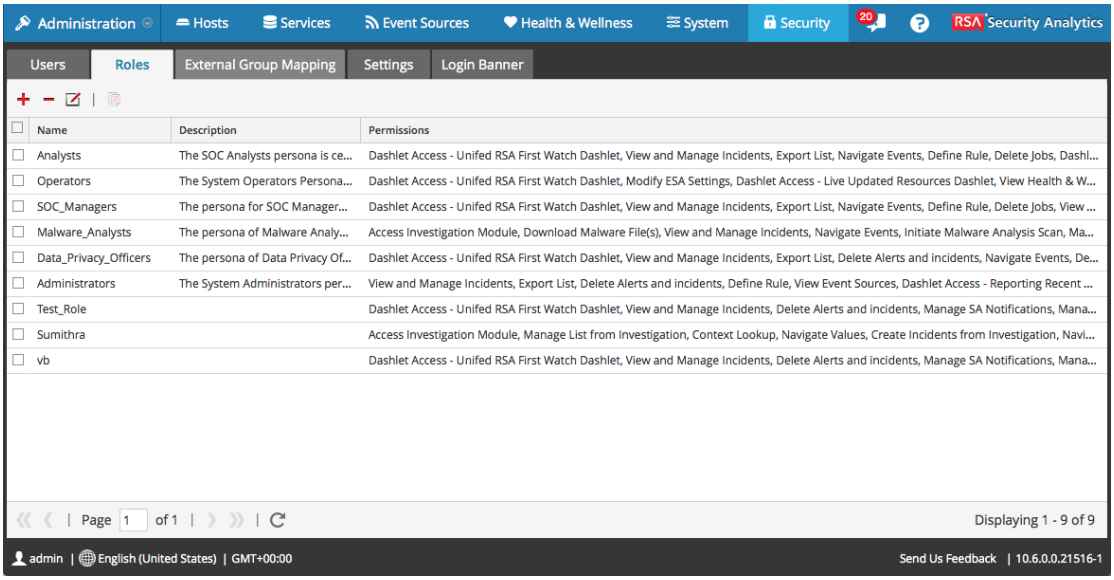
Cada uno de los siguientes procedimientos comienza en la pestaña **Funciones**. Realice los siguientes pasos para navegar a la pestaña **Funciones**:

1. En el menú de **Security Analytics**, seleccione **Administration > Seguridad**.

   El panel Seguridad del sistema se muestra con la pestaña **Usuarios** resaltada.

2. Haga clic en la pestaña **Funciones**.

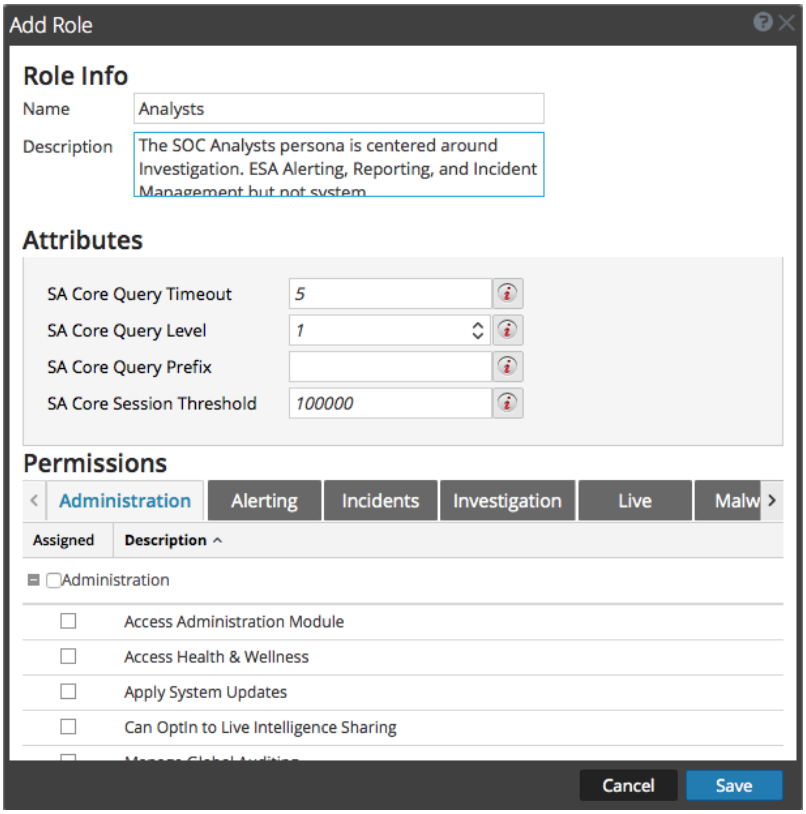
Se muestra el panel Funciones:



Agregar una función y asignar permisos

1. En la pestaña **Funciones**, haga clic en + en la barra de herramientas.

   Se muestra la pantalla **Agregar función**:



2. En la sección **Información de función**, ingrese información de la función para lo siguiente:
   - **Nombre**
   - (Opcional) **Descripción**
3. En la sección **Permisos**:
   - Haga clic en ← y → para desplazarse a través de los módulos.
   - Seleccione el módulo Reports al cual accede la función.
   - Seleccione cada permiso que tiene la función.
4. Repita el paso anterior hasta que seleccione todos los permisos que asignará a la función.
5. Haga clic en **Guardar** para agregar la nueva función, la cual se aplica de inmediato. Ahora puede asignar la nueva función a los usuarios.

Guías para informes

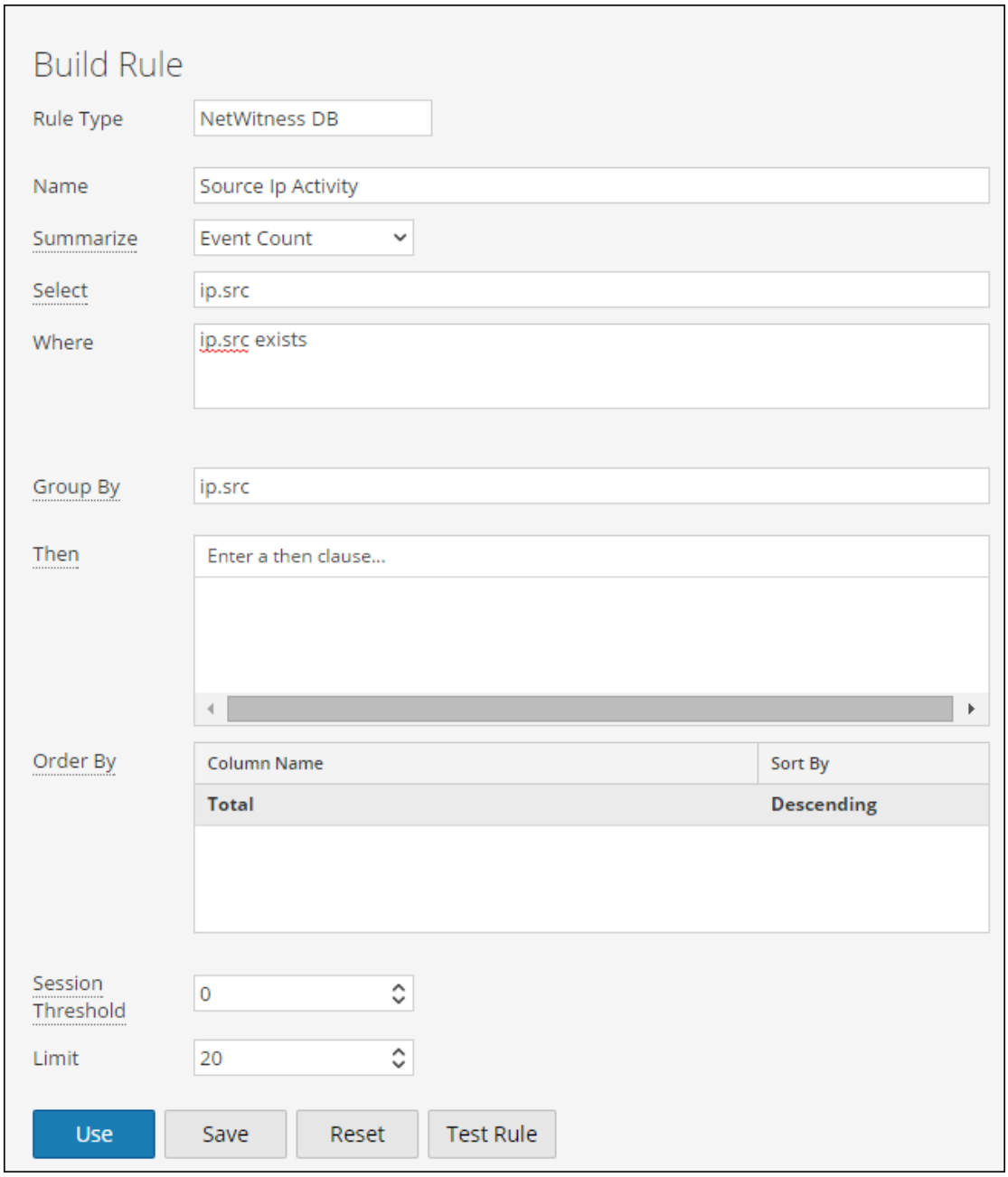
En este tema se enumeran las reglas recomendadas por RSA para mejorar el tiempo de ejecución de las entidades informantes. En este tema se enumeran las reglas recomendadas por RSA para mejorar el tiempo de ejecución de las entidades informantes, como reglas, informes, alertas, gráficos y listas. Las reglas se proporcionan para lo siguiente:

- Reglas de NWDB
- Configuración de tiempo de espera agotado para reglas de NWDB
- Búsqueda y acción Agregar regla
- Informes de valores de lista

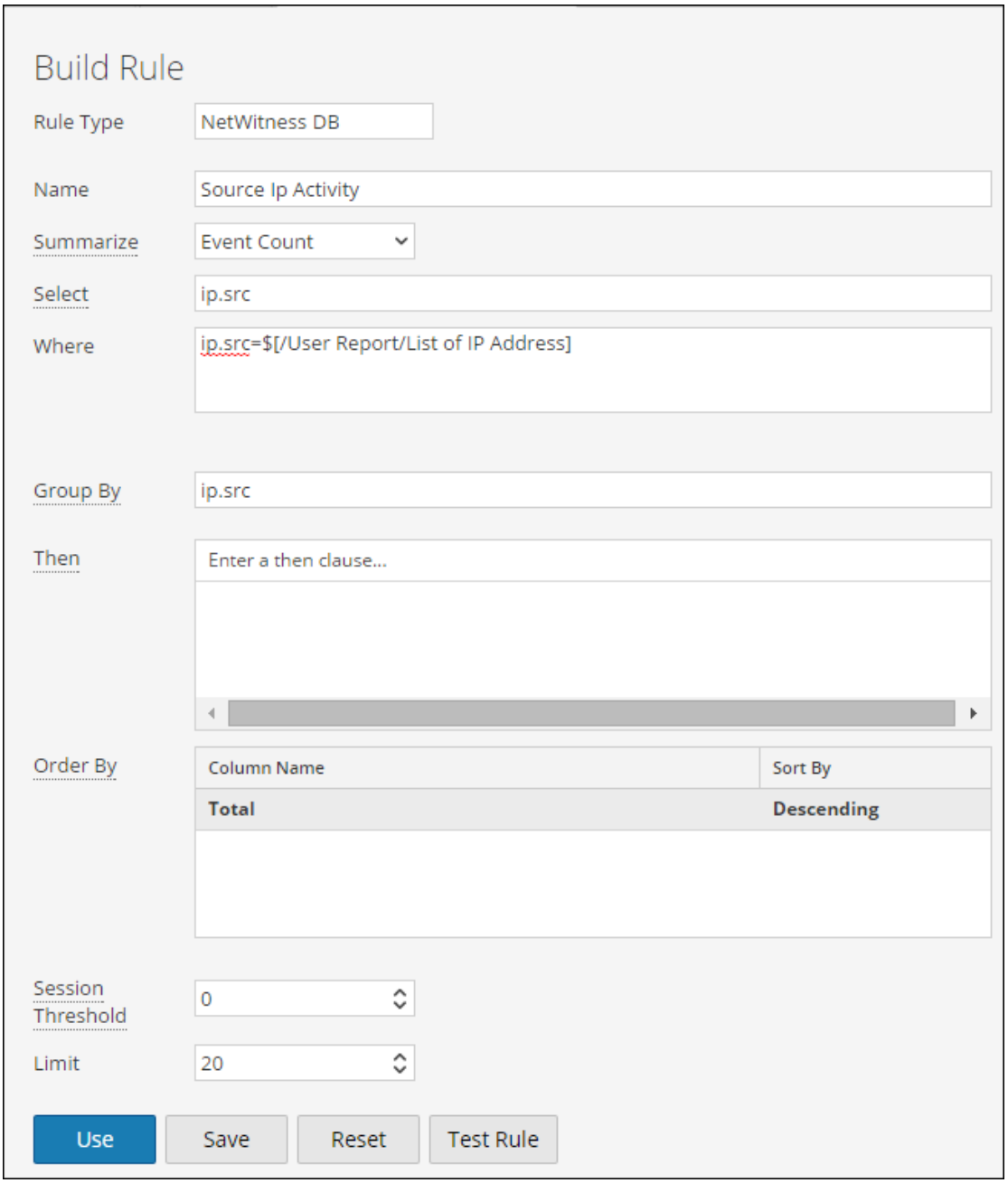
Reglas de NWDB

Si las entidades informantes como informe, alerta, o gráfico contienen reglas NWDB (en la mayoría de los casos cuando se incluye Agrupar por en la consulta) y demoran mucho en ejecutarse, puede hacer lo siguiente:

1. Refinar la cláusula WHERE:
   Puede limitar la cantidad de sesiones escaneadas mediante la utilización o el refinamiento de la cláusula WHERE (especialmente cuando utiliza la opción Agrupar por). Por ejemplo, considere la siguiente regla.

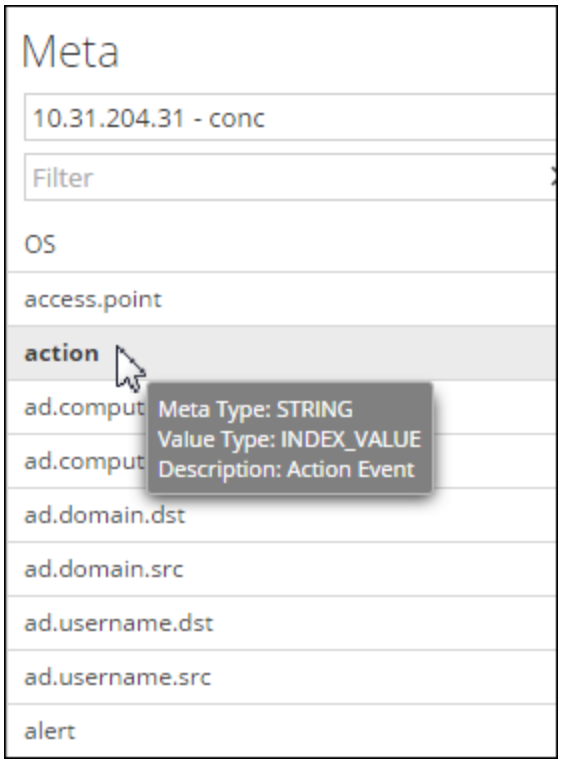


Si usa una cláusula WHERE como se mencionó anteriormente, la cantidad de sesiones agregadas es enorme. Para evitar esto, puede filtrar solo las sesiones requeridas, para lo cual se especifica la lista de direcciones IP o se crea una lista (lista de direcciones IP) que contiene las direcciones IP correspondientes.



2. Usar claves de METADATOS indexadas en la cláusula WHERE:
   Para entender si los METADATOS están indexados, mantenga el mouse sobre la clave de METADATOS. Si el tipo de valor es INDEX_VALUE, significa que los METADATOS están indexados. El tipo de valor es INDEX_KEY o INDEX_NONE si los METADATOS no están indexados.

   A continuación hay un snapshot de una clave de METADATOS que está indexada.



3. Configurar la opción Tiempo de espera agotado:
   Si la consulta está tardando mucho y falla debido a problemas de tiempo de espera agotado, puede configurar el tiempo de espera agotado para las ejecuciones de reglas NWDB. Para obtener más información, consulte la siguiente sección Configuración de tiempo de espera agotado para reglas NWDB.
4. Programar las consultas para su ejecución a horas diferentes:
   Si varios agregados de consultas se ejecutan al mismo tiempo y se produce tiempo de espera agotado, puede programar las consultas para que se ejecuten a horas diferentes sin mucha superposición.

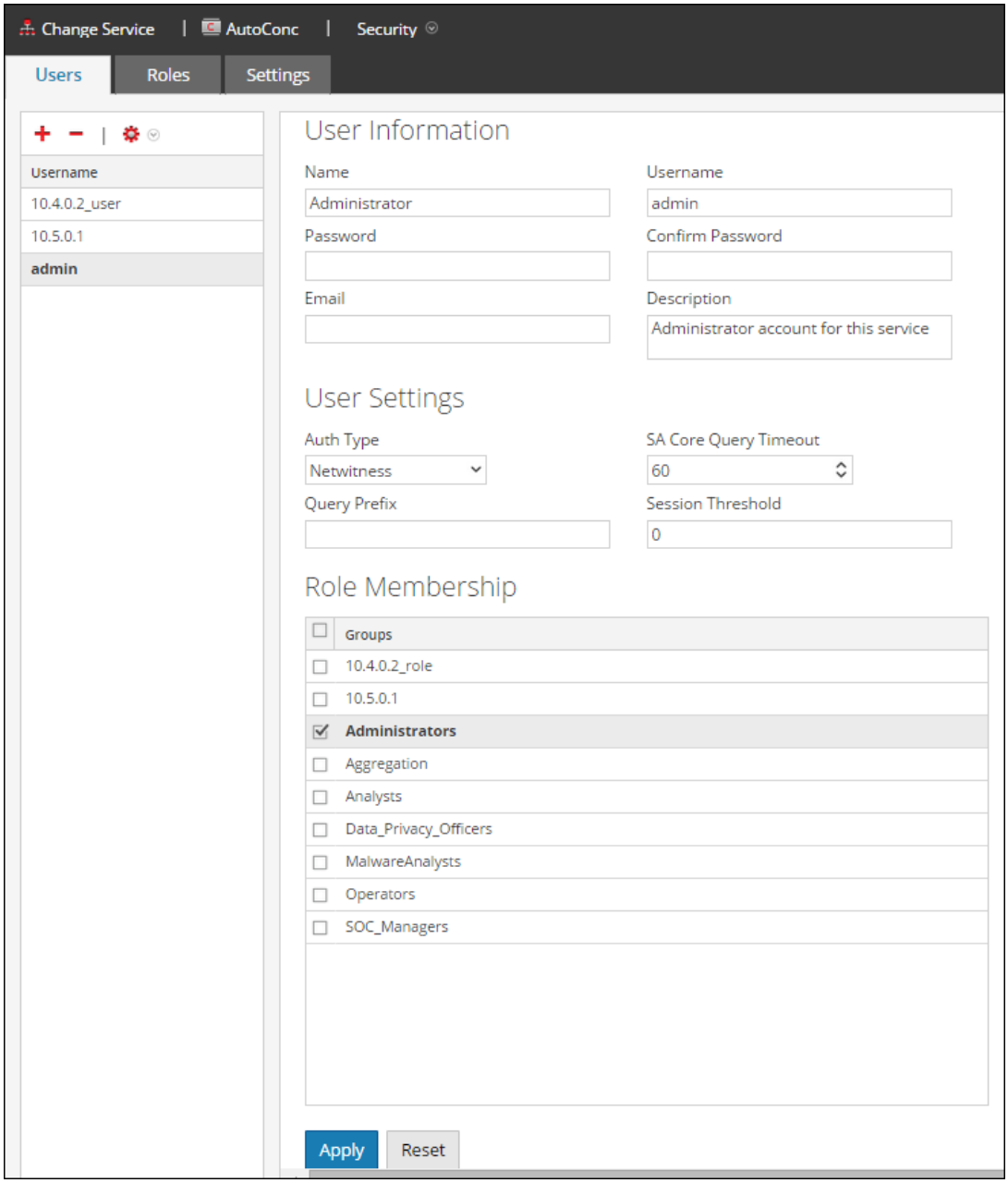
Configuración de tiempo de espera agotado para reglas de NWDB

Nota: Es una buena práctica para comprobar las estadísticas de Reporting Engine y los orígenes de datos de NWDB antes de realizar cualquier cambio en la configuración. Para obtener más información, consulte los temas Monitorear dispositivos y servicios para Reporting Engine y Monitorear estadísticas del sistema de la *Guía de mantenimiento del sistema*.

Si la ejecución de la regla NWDB falla debido a tiempo de espera agotado, puede obtener los siguientes errores en la página Ver un informe:

- Error de tiempo de espera de Reporting Engine
  - «El origen de datos "`10.31.x.x Concentrator`" no respondió dentro del tiempo configurado de `30` minutos para la solicitud "`/sdk/values`"».
- Error de tiempo de espera agotado de NWDB
  - «Se produjo un error al obtener datos del origen "`10.31.x.x Concentrator`". `{Timeout message from NWDB}`».
- En esta situación, puede hacer lo siguiente:
- - Tiempo de espera agotado de Reporting Engine
    En caso de tiempo de espera agotado de Reporting Engine, puede configurar el tiempo de espera en una duración mayor para que se puedan ejecutar las consultas largas. Para obtener más información sobre la configuración de las opciones `NWDB Queries Time Out` y `NWDB Info Queries Time Out` para Reporting Engine, consulte el tema Configurar ajustes de Reporting Engine en la *Guía de configuración de hosts y servicios*. RSA recomienda configurar `NWDB Query Time Out` en cero minutos (implica que no hay tiempo de espera) y `NWDB Info Queries Time Out` en 60 minutos.
  - Tiempo de espera agotado de NWDB
    En caso de tiempo de espera agotado de NWDB, puede ser necesario configurar los parámetros `query.level.timeout` y `max.concurrent.queries` del origen de datos de NWDB en función de las recomendaciones del tema Ajuste de la base de datos de la *Guía de configuración de hosts y servicios* para ajustar las consultas.

    El siguiente es el snapshot de la vista Explorador, donde puede configurar los parámetros para el origen de datos de NWDB.



- Programa informes a distintas horas

  Si los dispositivos principales de NWDB se utilizan mucho, es posible programar los informes para que se ejecuten a diferentes horas sin superposición.

- Dividir el informe

  Si tiene muchas reglas en un informe, divídalo en varios informes, donde cada informe contendrá un conjunto lógico de reglas. Si tiene varias reglas, todas las reglas comenzarán

a ejecutarse al mismo tiempo sobre la base de los hilos de ejecución disponibles, por lo tanto puede agrupar las reglas lógicamente en informes separados.

Acción LookupAndAdd Rule

Si una regla que se compone de acciones de reglas `lookup_and_add` únicas o múltiples tarda mucho en ejecutar el informe, es porque cada acción de regla activa varias consultas de búsqueda en el origen de datos NWDB, lo que da como resultado un tiempo de ejecución mayor.

Para mejorar el tiempo de ejecución del informe, puede hacer lo siguiente:

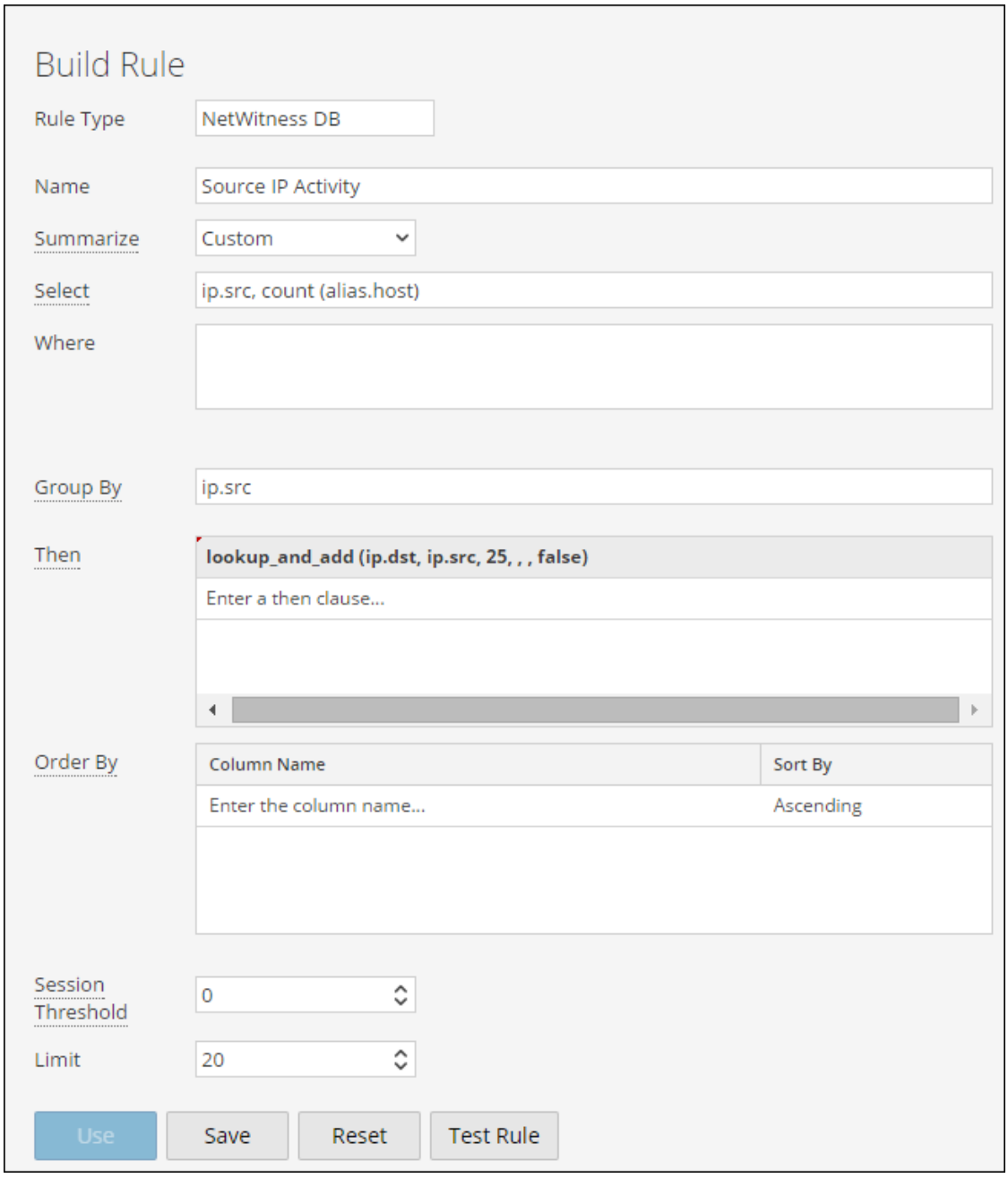
- Refinar la cláusula WHERE en lo siguiente:
  - Regla que contiene la acción de regla `lookup_and_add`
  - Acción de regla `lookup_and_add`
- Establecer límites

  Debe establecer límites adecuados para las acciones de las reglas y las reglas. Si el límite es alto, hará que se activen muchas consultas y por lo tanto la ejecución del informe demorará mucho tiempo.
- Establecer el parámetro de agregación buleano

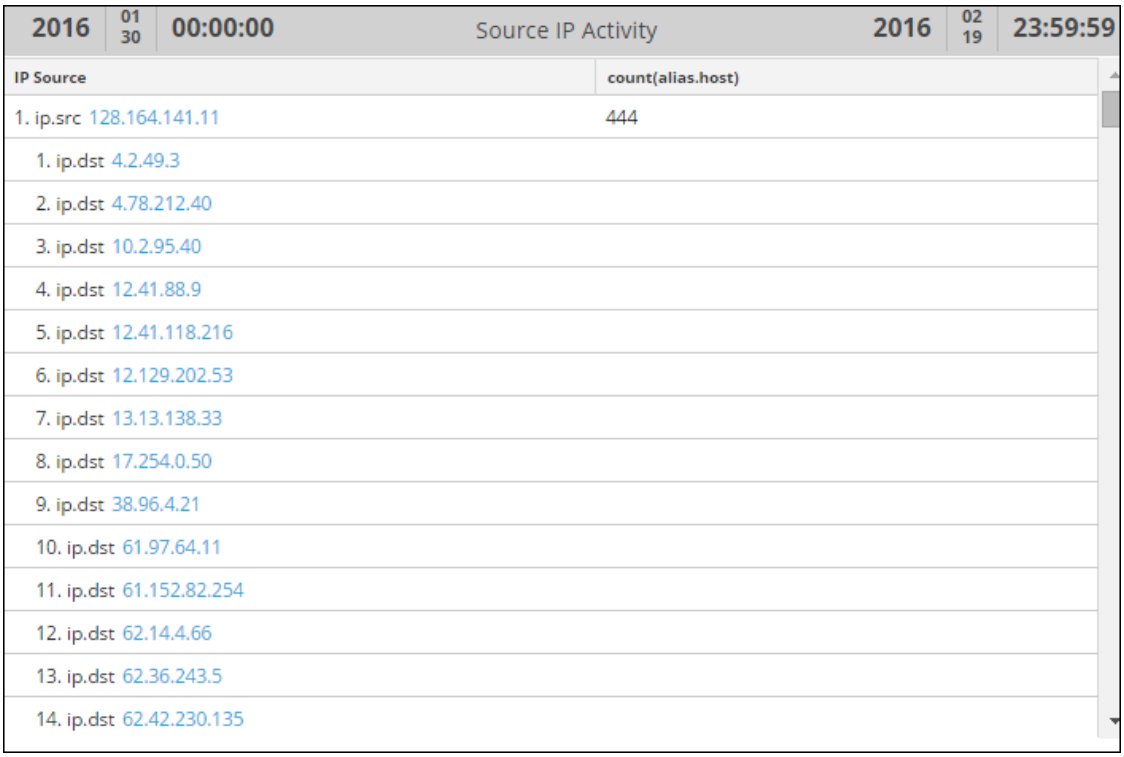
  Si no desea el valor agregado, como `sum(meta), count(meta)`, etc., para los valores de búsqueda, configure el parámetro de agregación buleano en falso en la acción de regla `lookup_and_add`. Para obtener más información, consulte la Sintaxis de reglas de NWDB.

  ```
  lookup_and_add(string select, string field, int limit, boolean
  inherit, string extraWhere, boolean aggregate)
  ```

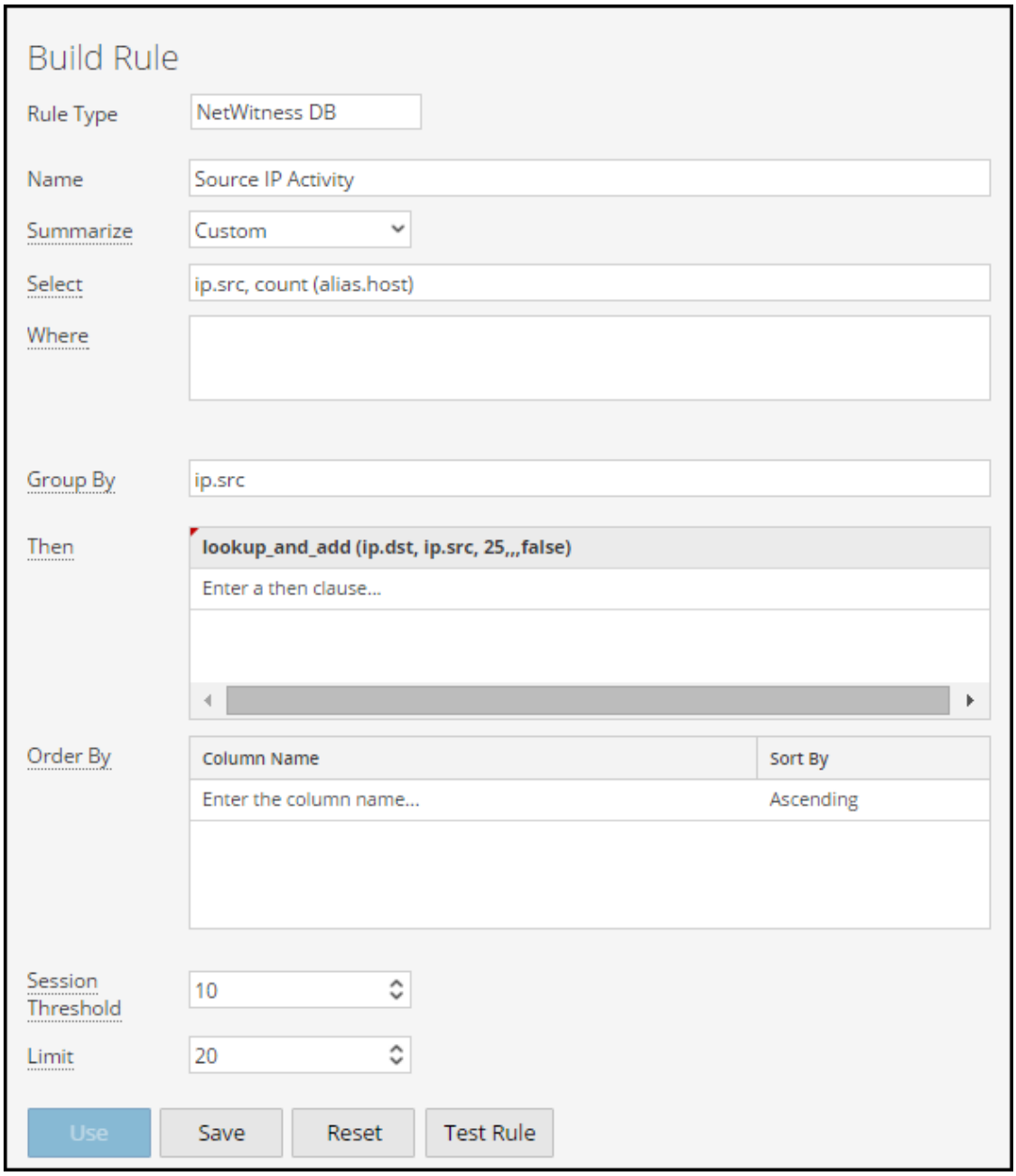
  Considere la regla con la acción de regla lookup_and_add:



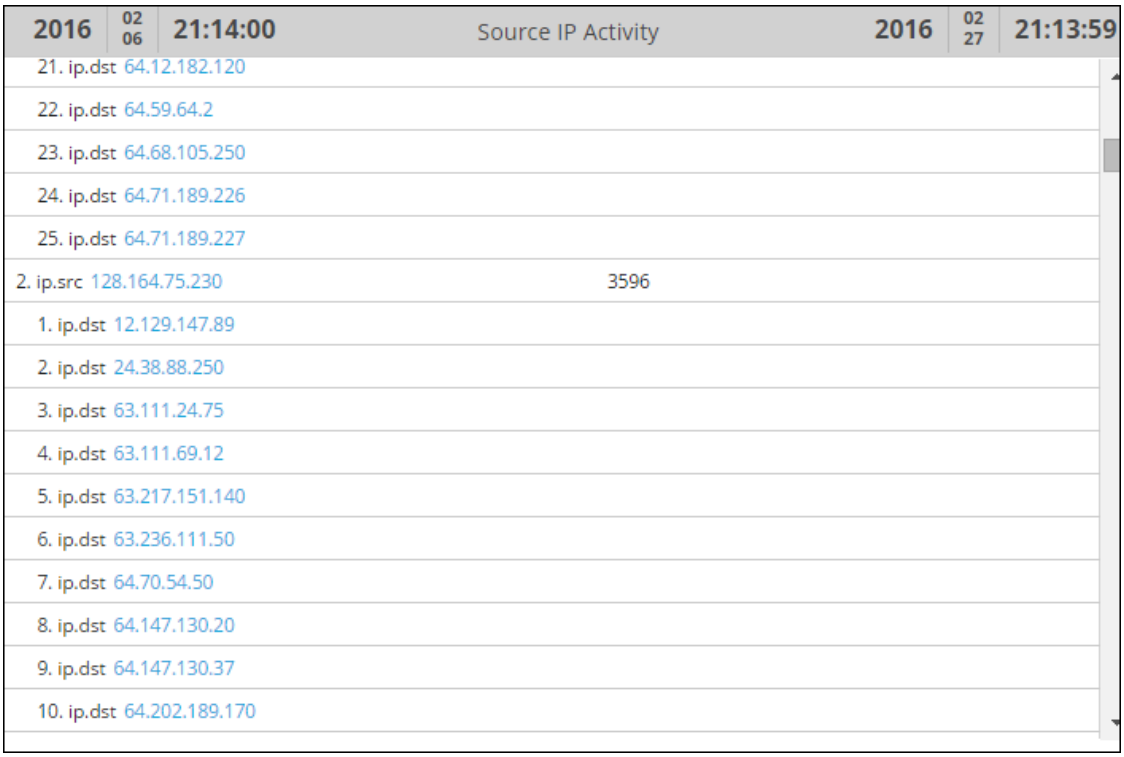
Se muestra la salida:



- Cada acción de regla `lookup_and_add` activa de forma predeterminada dos consultas de búsqueda simultáneas en el origen de datos. RSA recomienda conservar la configuración predeterminada; sin embargo, si desea aumentar el valor, tal vez desee asegurarse de que el valor del parámetro `Max # of Concurrent LookupAndAdd Queries` en Reporting Engine sea menor que el valor `Max Concurrent Queries` en la configuración del origen de datos de NWDB.
  Si el origen de datos de NWDB se comparte en otros servicios, puede conservar un valor bajo para el parámetro `Max # of Concurrent LookupAndAdd Queries` en Reporting Engine, puesto que aumentarlo afectará las consultas desde otros servicios. Para obtener más información, consulte el tema Pestaña General de Reporting Engine de la *Guía de configuración de hosts y servicios*.
- Si está interesado solo en valores únicos y no en agregados precisos, establezca `Session Threshold` en un valor distinto de cero para la regla NWDB. Para obtener más información, consulte Requisitos previos. Cuanto más alto sea el valor, más demorará la ejecución de la regla. Si el valor se configura en cero, demorará más, pero proporcionará agregados precisos.
  Considere una regla con la acción de regla lookup_and_add y el umbral de sesión configurado en 10.



Se muestra la salida:



Informes de valores de lista

Usar una lista refinada:

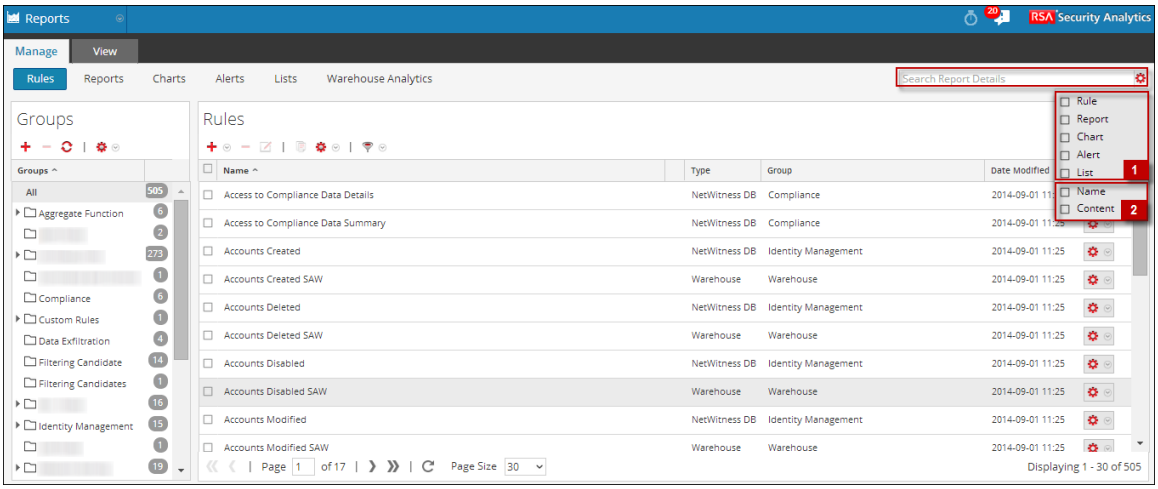
En el caso de los informes de valor de lista (para cualquier tipo de origen de datos), se generan informes individuales para cada valor de la lista. Por lo tanto, mientras mayor sea el número de valores en la lista, más demorará la ejecución de los informes. Por lo tanto, debe utilizar una lista refinada para generar dichos informes.

Buscar detalles de Reporting

En este tema se proporcionan instrucciones para realizar una búsqueda de palabras clave de nombre y contenido para cada uno de los componentes de Reporting. Puede realizar una búsqueda de palabras clave de nombre y contenido para cada uno de los componentes de Reporting (regla/informe/gráfico/alerta/lista) en la interfaz del usuario de Reporting.

Nota: No puede buscar en función de valores de fecha y numéricos.

En la siguiente figura se muestran los parámetros de búsqueda disponibles en el módulo Reporting:



Los siguientes son los parámetros de búsqueda disponibles en la interfaz del usuario de Reporting:

1. Buscar entidades (regla, informe, gráfico, alerta, lista).
2. Buscar entidades en función del nombre o contenido.

Nota: Las búsquedas no distinguen mayúsculas de minúsculas. Por ejemplo, Completado equivale a completado.

Requisitos previos

En el módulo Reporting, puede realizar una búsqueda de palabra clave en función del nombre y contenido (definición). En este contexto, el contenido implica la definición de cada uno de los componentes de Reporting. Por ejemplo, el valor definido en la regla, informe, calendario de informes, gráfico y panel de alerta. También puede priorizar la búsqueda mediante la selección de uno o todos los componentes: regla, informe, gráfico, alerta o lista.

Nota: No puede buscar en función de los valores de lista y la ruta de lista almacenados en el panel de definición de calendario.

Por ejemplo, para buscar el nombre de la regla (ExpertRule), debe seleccionar **regla, nombre y contenido** en la lista desplegable **Opciones de filtrado** para ver todos los nombres de reglas que coinciden con la búsqueda. De forma similar, puede buscar un informe, un gráfico, una alerta o una definición de lista.

Procedimiento

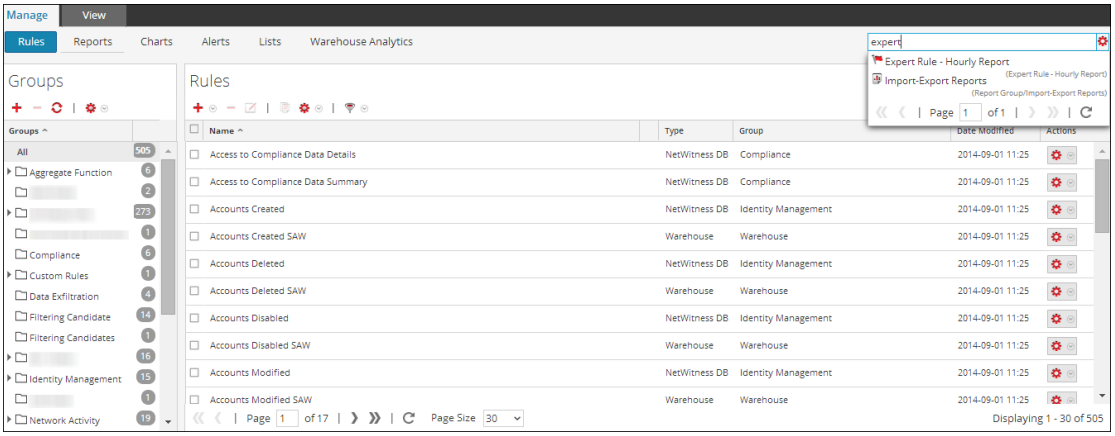
Realice los siguientes pasos para buscar detalles de creación de informes en la pestaña Administrar:

1. En el menú de Security Analytics, haga clic en **Administration > Informes**.

   Se muestra la pestaña **Administrar**.

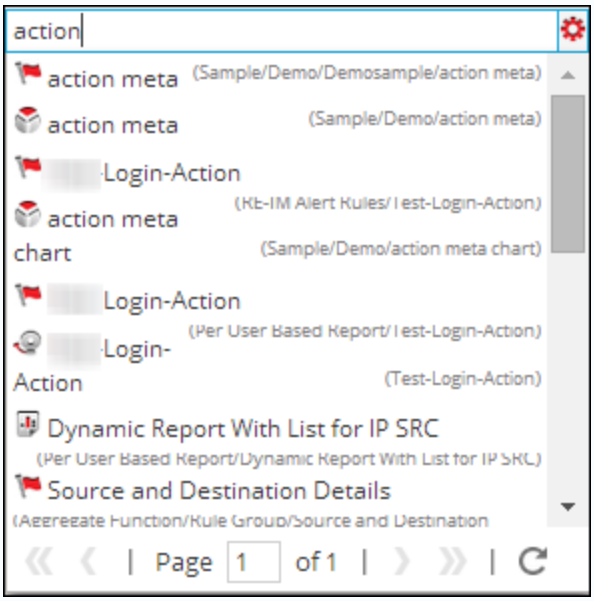
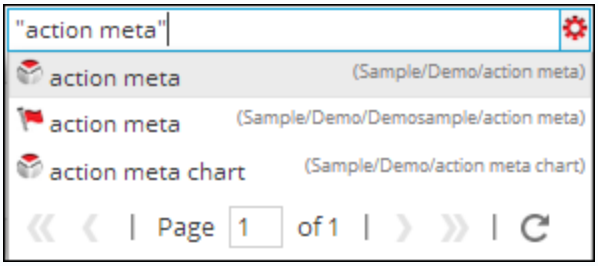
2. Haga clic en y seleccione los criterios apropiados para buscar.

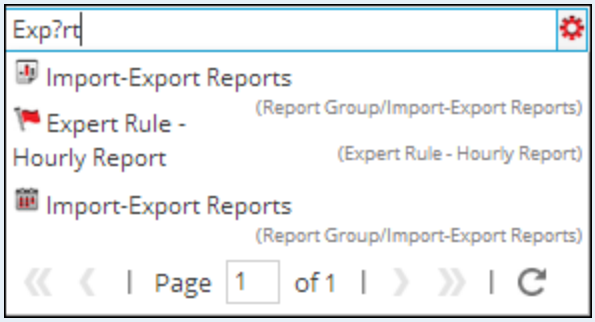
3. En el campo **Buscar**, ingrese el texto que desea buscar.
   Aparece la lista desplegable de búsqueda:

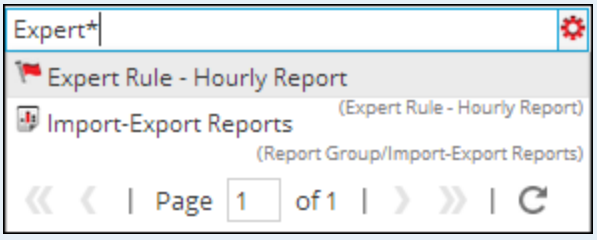
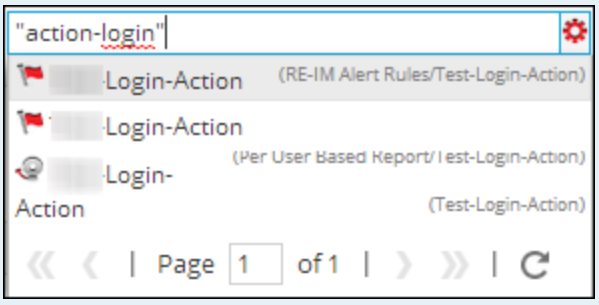


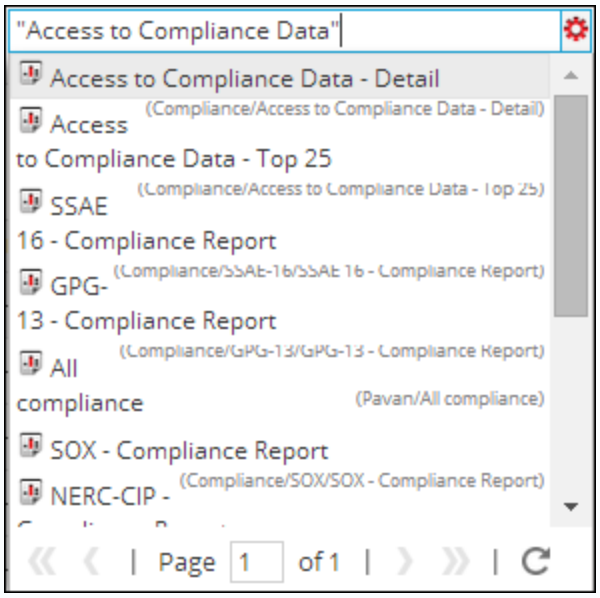
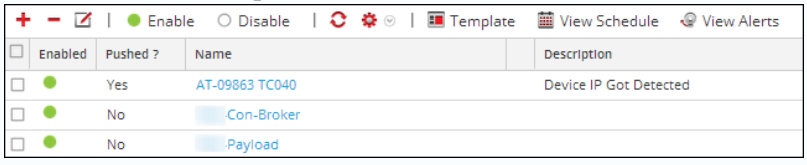
Sintaxis de búsqueda y distintos tipos de búsqueda

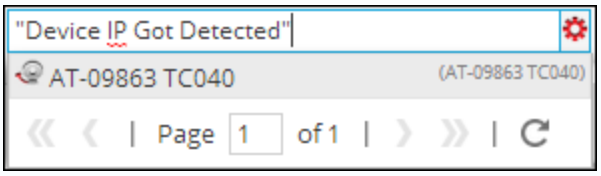
En la siguiente tabla se explica la sintaxis de búsqueda y las posibles búsquedas que se pueden realizar en la interfaz del usuario de Reporting.

Tipos de búsqueda	Descripción
Búsqueda basada en palabra o frase	**Búsqueda basada en palabra**: Para buscar una palabra como “action” o “meta”, debe ingresarla en el cuadro de búsqueda. En la siguiente figura se muestran los resultados de búsqueda del texto **action**.  **Búsqueda basada en frase:** Una frase es un grupo de palabras entre comillas dobles, como “action meta”. Para buscar una frase, debe ingresarla entre comillas dobles en el cuadro de búsqueda. En la siguiente figura se muestran los resultados de búsqueda de la frase “action meta”. 

Tipos de búsqueda	Descripción
Búsqueda con comodín (búsqueda de carácter único/múltiple/especial) El signo de interrogación "**?**" se usa para realizar una búsqueda con comodín de un único carácter, y el símbolo asterisco "*", para realizar una búsqueda con comodín de múltiples caracteres.	**Búsqueda de carácter único:** La búsqueda de comodín de carácter único busca términos que coincidan con el carácter único reemplazado. Por ejemplo, para la búsqueda de "Expert" o "Export", puede usar la sintaxis de búsqueda: Exp?rt En la siguiente figura se muestran los resultados de búsqueda del carácter comodín **Exp?rt**.  **Búsqueda de carácter múltiple:** La búsqueda de comodín de carácter múltiple busca 0 o más caracteres. Por ejemplo, para la búsqueda de Expert o Experts, puede usar la sintaxis de búsqueda: Expert* En la siguiente figura se muestran los resultados de búsqueda del comodín de múltiples caracteres **Expert***.

Tipos de búsqueda	Descripción
	 **Búsqueda de carácter especial:** Ciertos caracteres de puntuación y especiales se omiten durante la búsqueda (@#$%^&*(){}"~=+-[]\?|!:,.). Por ejemplo, una búsqueda de action-login se interpretará durante la búsqueda como “action” “login”, es decir, si existen reglas con nombre “action-login” y “action@login” y la cadena de búsqueda es “action-login”, el resultado de la búsqueda devolverá ambas reglas. 

Tipos de búsqueda	Descripción
Búsqueda basada en nombre o contenido	**Búsqueda basada en nombre:** Cuando desee buscar en función del nombre de un informe, seleccione la casilla **Informe** y **nombre** en el menú desplegable de opciones de filtrado. Por ejemplo, para buscar el nombre de informe “Acceso a los datos de cumplimiento de normas”, puede usar la sintaxis de búsqueda: “Acceso a los datos de cumplimiento de normas” **Nota:** Cuando busca un informe, implica que también puede buscar los calendarios del informe. Los resultados de la búsqueda devolverán el informe que contiene el nombre específico.  **Búsqueda basada en contenido:** Cuando desea buscar contenido dentro de una alerta, por ejemplo, la descripción de la alerta, seleccione la casilla **Alerta** y **contenido** en el menú desplegable de opciones de filtrado. Por ejemplo, para buscar la descripción de la alerta “Se detectó IP de dispositivo”, puede usar la sintaxis de búsqueda: “Se detectó IP de dispositivo” 

Tipos de búsqueda	Descripción
	La búsqueda devolverá el resultado con el contenido específico. 

Próximos pasos

Realice una de las siguientes tareas:

1. Puede editar una regla, un informe, un gráfico, una alerta y una lista en los paneles correspondientes.
2. Puede programar un informe en la vista Requisitos previos .
3. Puede probar un gráfico en la vista Probar un gráfico .

Solución de problemas

En este tema se proporcionan instrucciones de solución de problemas que se presentan cuando se usa el módulo Reporting en Security Analytics.

Solución de problemas antes de configurar el servidor SFTP.

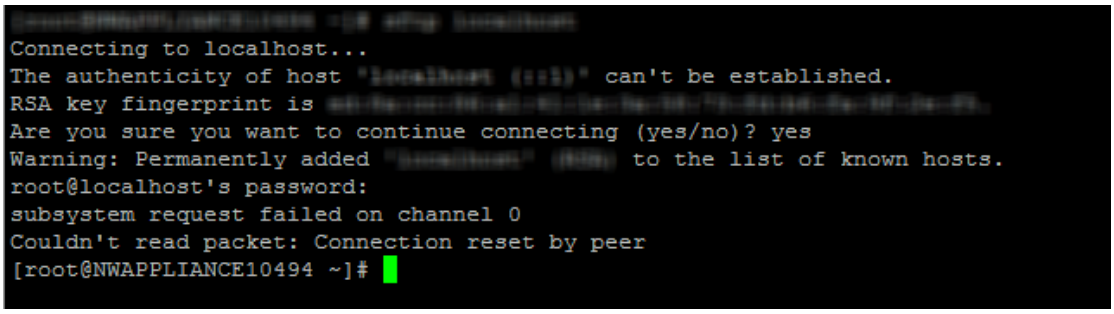
En esta sección se proporcionan instrucciones de solución de problemas que se presentan antes de la configuración del servidor SFTP.

Procedimiento

Intente los siguientes pasos si experimenta problemas relacionados con el servidor SFTP de Linux configurado:

1. Si la Acción de salida del informe para el SFTP configurado falla, debe obtener acceso al servidor SFTP mediante el protocolo SSH e intentar una conexión local para comprobar si SFTP funciona correctamente.

   Conéctese al servidor SFTP:



2. Si la conexión local falla, abra el archivo **sshd_config> vi /etc/ssh/sshd_config.**
3. Busque esta entrada en el archivo:

   ```
   # override default of no subsystems
   Subsystem sftp /usr/libexec/openssh/sftp-server
   ```

4. Si esta entrada no existe, agregue las dos líneas mencionadas en el Paso 3 en la parte inferior del archivo y **guárdelo**.
5. Reinicie el servicio desde **SSH > service sshd restart**.
6. Reintente ahora la conexión a SFTP.
7. Asegúrese de que el firewall del dispositivo del servidor de SA no esté bloqueando el puerto SFTP. Actualice las reglas iptables para permitir el puerto SFTP

Definiciones:

Analizador estricto: El analizador estricto (no obsoleto) espera que la sintaxis de consulta sea del tipo correcto.
Para todos los tipos de metadatos de texto, use comillas; por ejemplo, username = ‘user1’.
No use comillas para las direcciones IP, las direcciones de Ethernet y los tipos de metadatos numéricos, por ejemplo, service = 80 &&
ip.src = 192.168.1.1.
Para los tipos de metadatos de fecha y hora,
Si el formato de fecha y hora es “AAAA-MM-DD HH:MM:SS”, use comillas.
Si el formato de fecha y hora es 1448034064 (número de segundos transcurridos desde EPOCH (1 de enero de 1970), no use comillas.
Las consultas de creación de informes se analizarán con el analizador estricto cuando el valor de configuración de /sdk/config/query.parse sea **strict** en los servicios principales de NWDB.

Analizador no estricto: El analizador no estricto (obsoleto) no espera que la sintaxis de consulta sea de tipo correcto, es decir, los valores de tipos de metadatos de texto y numéricos pueden ir entre comillas o sin ellas independientemente del tipo de metadatos.

Por ejemplo, username es un tipo de metadatos de cadena y, por lo tanto, sus valores pueden ir entre comillas o sin ellas. De esta forma, es válida la sintaxis username = ‘user1’ y username = user.

Las consultas de creación de informes se analizarán con el analizador no estricto cuando el valor de configuración de /sdk/config/query.parse sea **deprecated** en los servicios principales de NWDB.

Nota: El procedimiento de solución de problemas para el modo de analizador estricto se aplica a Reporting Engine 10.6 y superior.

Solución de problemas de la sintaxis de reglas de NWDB en una instalación nueva

En una instalación nueva de Security Analytics 10.6, los servicios principales de NWDB utilizan el analizador estricto (modo no obsoleto) de forma predeterminada para consultas de creación de informes. Por lo tanto, RSA recomienda crear reglas que cumplan con la sintaxis del analizador estricto (modo no obsoleto). Para obtener más información sobre la sintaxis de la consulta de NWDB, consulte Sintaxis de reglas de NWDB.

Solución de problemas de sintaxis de reglas de NWDB en la actualización

En caso de una actualización de Security Analytics 10.4.x o 10.5.x a Security Analytics 10.6.x, los servicios principales de NWDB continuarán utilizando un analizador no estricto (modo obsoleto) para las consultas de Reporting Engine. Por lo tanto, las consultas existentes continuarán ejecutándose correctamente incluso si no cumplen con la sintaxis del analizador estricto y proporcionarán resultados similares a las versiones anteriores. RSA recomienda crear reglas que cumplan con la sintaxis del analizador estricto.

El uso de un analizador estricto (modo no obsoleto) o no estricto (modo obsoleto) por parte de los servicios principales de NWDB para las consultas de creación de informes lo controla /sdk/config/query.parse (Administration > Servicios > Seleccione un servicio (servicio principal de NWDB) y en el menú Acciones, seleccione Ver > Explorar).

Si va a agregar un nuevo dispositivo principal de NWDB, en el cual se ejecuta la consulta de Reporting Engine, a una infraestructura existente que se ejecuta en modo no estricto (modo obsoleto), puede actualizar la configuración /sdk/config/query.parse (Administration > Servicios > Seleccione un servicio [servicio principal de NWDB] y en el menú Acciones, seleccione Ver > Explorar) al modo no estricto (modo obsoleto) para el dispositivo nuevo, hasta que la instancia completa de Security Analytics y los servicios asociados se hayan trasladado al modo estricto.

Solución de problemas de reglas de importación

En esta sección se proporcionan instrucciones de solución de problemas que se presentan cuando se importan reglas, informes, gráficos y alertas que se exportan desde 10.4.x o 10.5.x y se importan a 10.6.

Procedimiento

1. Inicie sesión en Security Analytics.
2. Vaya a **Administration** >**Informes** > **Administrar** > **Reglas**
3. Haga clic en **Operaciones de regla** > **Importar**
   Aparece la ventana Importar regla.

Cuando se importan reglas de Reporting Engine 10.4.x o 10.5.x a Reporting Engine 10.6.x, o cuando se implementan reglas de Live, estas pueden contener errores de sintaxis. La ejecución de estas reglas falla con un mensaje de error, por ejemplo, "**Error occured while fetching data from source "Concentrator - Concentrator [10.0.0.0]". Error details: rule syntax error: expecting <IPv4 address> here: "'172.15.0.0'|| eth.src=00:13:C3:3B:BE:00)"**.
Se debe corregir la sintaxis de la regla según el mensaje de error que se muestra o cambiar el dispositivo principal para que funcione en modo no estricto (modo obsoleto).
Por ejemplo,
Para todos los tipos de metadatos de texto, use comillas; por ejemplo, username = 'user1'.

Descripción general de una regla

En este tema se proporciona una descripción breve de una regla. Una regla es el elemento esencial y básico del módulo Reporting. Se debe crear una regla que se pueda usar en informes, gráficos o alertas.

Elementos esenciales de una regla

Una regla representa una consulta única que detecta y resume la información solicitada dentro de una recopilación de datos de red. Por ejemplo, puede escribir una regla para ver las 20 direcciones web principales que sus usuarios visitan diariamente o una regla para detectar la presencia de autenticación de texto sin cifrar en sus activos de alto valor.

La sintaxis de una regla es muy similar a la del lenguaje de consulta estándar (SQL) donde puede usar la cláusula SELECT, la cláusula WHERE, clasificar y agrupar opciones y límites para el conjunto de resultados. Una regla consta de lo siguiente:

Propiedad	Descripción	Ejemplo
Nombre	El nombre de la regla.	Actividad de cuenta del sistema Windows

Propiedad	Descripción	Ejemplo
Seleccionar	Lista de los tipos de metadatos que se devuelven en el conjunto de resultados. La lista de los tipos de metadatos se proporciona en la biblioteca de metadatos. La biblioteca de metadatos en el generador de reglas está constantemente sincronizada con la configuración de índices del host de Security Analytics al cual está conectada esta aplicación. La cantidad de tipos de metadatos que esta propiedad puede representar depende de cómo se clasifica la regla. Si la propiedad Ordenar por es “Ninguno” o no agregado, una regla puede tener más de un campo de selección, por ejemplo, para cada coincidencia, incluir el ip.src, ip.dst, el tamaño, la hora en el resultado de la regla. Si una regla está establecida para clasificarse, por conteo de sesiones, tamaño de sesión, o tamaño de paquete, puede haber solo un campo en el cual seleccionar.	
Donde	Una cláusula que constituye la consulta base de la regla.	`alert='cleartext_ftp_passwords'`

Propiedad	Descripción	Ejemplo
Then (acciones de la regla)	Una serie de funciones que manipulan el conjunto de resultados original de una regla para lograr que la salida en un informe sea más concreta o agregar una funcionalidad adicional distinta a la consulta de datos y su visualización.	`lookup_and_add ('username','ip.src',10);`
Ordenar por	Determina cómo se ordenan los datos del conjunto de resultados. Las diversas posibilidades son: • Total • Valor	Total
Límite	Designa el tamaño máximo de un conjunto de resultados para la regla determinada. Los usuarios deben tener en cuenta que si un conjunto de resultados se clasifica por conteo o tamaño, el límite representa los N valores superiores (o inferiores) que se devolverán. Si el conjunto de resultados no se ordena, se devuelven los primeros valores N.	20

Nota: En la interfaz del usuario, la fecha o la hora mostradas dependen de la zona horaria que seleccionó el usuario.

Sintaxis de reglas de IPDB

En este tema se describe la sintaxis soportada de reglas del servicio IPDB Extractor mediante descripciones y ejemplos de las sintaxis compatibles y no compatibles. Existe un conjunto limitado de sintaxis que puede usar para crear las reglas de los informes utilizando el servicio IPDB Extractor de esta versión. En este tema se incluye:

- Descripciones de las sintaxis compatibles y no compatibles con ejemplos.
- Funciones adicionales compatibles.
- Operadores compatibles.
- Ejemplos de consultas compatibles.

Sintaxis compatible y no compatible

Cuando cree reglas que contengan consultas SQL contra la base de datos IPDB de esta versión, debe adherirse a las descripciones y ejemplos de sintaxis descritos en las tablas siguientes.

Sintaxis de valores literales (datos) compatible

Descripción	Ejemplos de sintaxis compatible
Para los datos de tipo texto o cadena, ingrese la cadena o el texto entre comillas simples. Si hay un carácter especial, como un apóstrofo (por ejemplo '*data*'), use dos comillas simples, "*data*", para encerrar el valor de los datos.	select msg.id where msg='(Primary) Link status "Down" on interface INTNAME.'
Para la fecha y la hora (columnas del tipo de datos fecha/registro de fecha y hora), use la sintaxis "*aaaa-mmm-dd hh:mm:ss*".	select time where time = '2012-sep-04 13:09:03'
El sistema es compatible con direcciones IP literales. Considera las columnas que contienen direcciones IP como cadenas/texto, de forma que utiliza el operador de comparación de cadenas para evaluar las expresiones. Use los siguientes operadores para garantizar un procesamiento preciso: • = (es igual a) • != (no es igual a) • in (está contenido en) • not in (no está contenido en)	

Sintaxis IN no compatible

Descripción	Ejemplos de sintaxis no compatible
Security Analytics no es compatible con el uso de *in* en las direcciones IP	select ip.src where ip.src in between '*n.n.n.*n' and '*n.n.n.*n'

Sintaxis LIKE no compatible

Descripción	Ejemplos de sintaxis no compatible
Security Analytics no es compatible con () for like	user.dst not like ('%')

Sintaxis LIST compatible

Descripción	Ejemplos de sintaxis compatible
Coloque una lista entre paréntesis en el campo de la cláusula **where**. Use el operador IN. Debe encerrar los valores en una lista en comillas simples, excepto lossiguientes valores: • caracteres alfanuméricos • : (dos puntos) • _ (guion bajo) • . (punto)	select ip.src,ip.dst where ip.dst IN ($[LIST])

Sintaxis LIST no compatible

Descripción	Ejemplos de sintaxis no compatible
No omita los paréntesis.	select ip.src,ip.dst where ip.dst IN $[LIST]
No omita el operador IN.	select ip.src,ip.dst where ip.dst =($[LIST])

Sintaxis variable compatible

Cuando asigna el valor de la variable en una configuración de ejecución, debe ingresar el valor entre comillas simples: '*value*'.

Descripción	Ejemplos de sintaxis compatible
Inserte $ antes de una variable. Encierre una variable en llaves.	columnname=${*variable*}

Sintaxis variable no compatible

Descripción	Ejemplos de sintaxis no compatible
No omita el símbolo $.	columnname={variable}
No omita las llaves.	columnname=$variable
No sustituya las llaves con paréntesis.	columnname=$[variable]

Sintaxis de la cláusula select compatible

Debe incluir las columnas **order by** y **group by** en las cláusulas **select**.

Descripción	Ejemplos de sintaxis compatible
Seleccione todas las columnas de un origen de datos de IPDB.	select *

Descripción	Ejemplos de sintaxis compatible
Seleccione columnas específicas de un origen de datos de IPDB (debe separar cada columna con una coma).	select *column1* , *column2* , *column3* ,...,*columnN*
Use distinct en una cláusula select. Debe encerrar la columna en paréntesis cuando use distinct.	select distinct (*column1*)
Use funciones de agregación en la cláusula select. Consulte “Funciones de agregación compatibles”, a continuación, para conocer una completa lista de las funciones de agregación compatibles en esta versión que contiene este artículo.	select count (msg.id) select count (distinct (msg.id))

Sintaxis de la cláusula select no compatible

Descripción	Ejemplos de sintaxis no compatible
No encierre los nombres de las columnas en paréntesis a menos que desee especificar un agregado. En el siguiente ejemplo se representa un uso no compatible de los paréntesis.	select (msg.id), (ip.src)
No use columnas calculadas. En el siguiente ejemplo se representa un uso no compatible de columnas calculadas.	select msg.id+100, ip.src

Descripción	Ejemplos de sintaxis no compatible
No use alias de columnas (con o sin AS). El siguiente ejemplo representa un uso no compatible de los alias de columnas.	select msg.id as ID, ip.src SRC
Security Analytics no es compatible con la función Lower de las cláusulas select.	

Sintaxis de la cláusula where compatible

Debe incluir las columnas **ordenar por** y **agrupar por** en las cláusulas **where**.

Descripción	Ejemplos de sintaxis compatible
Encierre un valor comillas simples si el valor incluye un espacio. La siguiente sintaxis está incorrecta: where msg = Auth start for user USERNAME from 20.20.20.2/20 to 10.10.10.1/10.	where msg = 'Auth start for user USERNAME from 20.20.20.2/20 to 10.10.10.1/10'

Descripción	Ejemplos de sintaxis compatible
Ingrese un valor entre comillas simples si el valor incluye caracteres especiales. No debe encerrar los siguientes caracteres en comillas simples: • caracteres alfanuméricos • : (dos puntos) • _ (guion bajo) • . (punto) La siguiente sintaxis no funciona: select url,size device spec: ***device-specifications*** where url = http://1.1.1.1//tsweb/images/clear.gif La siguiente sintaxis no funciona: where url = some/urls/string La siguiente sintaxis no funciona: where msg = Failover cable OK.	La siguiente sintaxis funciona: where msg.id = 101001:10 La siguiente sintaxis funciona: select url,size device spec: *device-specifications* where url = 'http://1.1.1.1//-tsweb/images/clear.gif' La siguiente sintaxis funciona: where url = 'some/urls/string' La siguiente sintaxis funciona: where msg = ‘Failover cable OK.’
Use esta sintaxis para expresar una condición de filtro.	*column1 <operator>* '*value*'
Use esta sintaxis para los operadores y/o buleanos, o buleanos. Consulte “Operadores compatibles” a continuación, para obtener una lista completa de los operadores compatibles con esta versión.	*column1 <operator>* 'value' and column2< *operator> 'value'* or *column1 <operator>* 'value'
Use esta sintaxis para comprobar valores nulos.	*column1* is null *column1* is not null

Descripción	Ejemplos de sintaxis compatible
Use esta comprobación de sintaxis para la membresía que utiliza el operador in.	*column1* in ('*value1*','*value2*',...,'*valueN*') *column1* not in ('*value1*','*value2*',...,'*valueN*')
Use esta sintaxis para especificar un rango mediante el uso del operador between.	*column1* between '*value1*' and '*value2*' *column1* not between '*value1*' and '*value2*'
Use esta sintaxis para comparar una cadena utilizando el operador like.	*column1* like '*value*' *column1* not like '*value*'
Use esta sintaxis para buscar patrones utilizando el comodín % con el operador like.	select msg.id where msg like 'ip%'
Use la función Lower para omitir las mayúsculas y minúsculas en las búsquedas de la cláusula where. Puede asociar la función Lower en una cláusula where con el tipo de columna TEXTO de manera exclusiva. Si especifica Lower con un tipo de columna distinto de TEXTO, Security Analytics muestra un mensaje de error. Security Analytics no es compatible con la función para los operadores BETWEEN, IN y NOT NULL.	Lower(columnName) like ‘some%’ Lower(columnName) like lower (‘some%’)

Sintaxis de la cláusula where no compatible

Descripción	Ejemplos de sintaxis no compatible
No use consultas anidadas.	select msg.id where msg.id in (select msg.id from table where ip.src = '1.1.1.1')
No use la función Lower para los operadores BETWEEN, IN y NOT NULL.	

Sintaxis de la cláusula order by compatible

La función order by no distingue mayúsculas de minúsculas.

Descripción	Ejemplos de sintaxis compatible
Use esta sintaxis para ejecutar clasificaciones ascendentes (asc) y descendentes (desc) con order by.	• order by size asc • order by msg desc • order by size asc, msg desc • order by count(size) asc
Solo encierre los nombres de columnas en paréntesis si desea aplicar una función adicional a la columna. El siguiente ejemplo representa un uso no válido de los paréntesis en una cláusula order by: order by (count(size)) asc	order by count(size) asc

Sintaxis de la cláusula group by compatible

Descripción	Ejemplos de sintaxis compatible
Use esta sintaxis para agrupar una o más columnas. No ingrese los nombres de columnas entre paréntesis. La función group by no distingue mayúsculas de minúsculas.	• group by size • group by msg

Funciones adicionales compatibles

El servicio IPDB Extractor es compatible con las siguientes funciones y sintaxis de agregación en esta versión.

- count
- máx.
- min
- sum
- avg

Puede usar distinct con funciones de agregación, como se muestra en la siguiente sintaxis:

- count(distinct)
- max(distinct)
- min(distinct)
- sum(distinct)
- avg(distinct)

Operadores admitidos

Operador	Sintaxis
= (es igual a)	*column1* = '*value*'
!= (no es igual a)	*column1* != '*value*'
<= (menor que o igual que)	*column1* <= '*value*'
>= (mayor que o igual que)	*column1* >= '*value*'
<(menor que)	*column1* < '*value*'
>(mayor que)	*column1* > '*value*'
IN	*column1* NOT ('*value1*','*value2*',...,'*valueN*') *column1* not in ('*value1*','*value2*',...,'*valueN*')

Operador	Sintaxis
between (rango entre dos valores)	*column1* between '*value1*' and '*value2*' *column1* NOT between '*value1*' and '*value2*'
and, or, NOT (buleano)	*condition1* and *condition2* *condition1* or *condition2* *condition1* not in ('*value1*','*value2*',...,'*valueN*')
like	*column1* like '*value*' *column1* not like '*value*'

Ejemplo de consultas compatibles

select msg.id, ip.src, ip.dst, user.dst where size is not null

select msg.id, size, ip.srcport where msg.id='109007' and size not between '10' and '20'

select max(distinct(size)) where msg.id in ('109007','109001')

select * where size != '99' and ip.src = '20.20.20.2'

select ip.srcport,ip.dstport where ip.dst != '225.31.125.90' order by ip.dstport asc

select ip.srcport,ip.dstport where ip.dst != '225.31.125.90' order by ip.dstport asc,ip.srcport desc

select ip.srcport,ip.dstport where ip.dst != '225.31.125.90' group by ip.srcport,ip.dstport order by min(distinct(ip.dstport)) asc, sum(distinct(ip.srcport)) desc

select time where time = ‘2012-sep-04 13:09:03’

select * where ip.src = '20.20.20.2' and ip.dst != '10.31.125.90' or ip.dst!= '225.31.125.90'

Ejemplo de consultas no compatibles

Consulta no compatible	Motivo
select (msg.id), (ip.src), ip.dst, user.dst where size is not null.	No puede encerrar columnas en paréntesis.

Consulta no compatible	Motivo
select msg.id where msg.id IN (select msg.id from table where ip.src = ‘1.1.1.1’)	No puede usar una selección anidada (subconsulta) para obtener el campo msg.id en otra condición.
select ip.src where ip.src in between ’10.10.10.1’ and ’10.10.9.1’	Puede usar el operador between solamente con tipos de datos numéricos y de fecha y hora.
select ip.srcport,ip.dstport where ip.dst != '225.31.125.90' order by count(distinct ip.dstport) asc	Cuando usa distinct o cualquier otra función de agregación, debe encerrar el nombre de la columna en paréntesis.
select ip.srcport,ip.dstport where ip.dst != '225.31.125.90' order by (ip.dstport) asc,(ip.srcport) desc	No puede encerrar los nombres de columna en paréntesis.
select ip.srcport,ip.dstport where ip.dst != '225.31.125.90' group by ip.srcport,ip.dstport order by COUNT((ipsrcport))	Solo puede usar un par de paréntesis para encerrar los nombres de columna. El sistema trata varios conjuntos de paréntesis como expresiones anidadas, las cuales no son compatibles.
select time where time = ‘1999-NOVEMBER-01 10:10:10’	El formato de registro de fecha y hora es incorrecto.
select time where time = ‘2012-11-11 10:10:10’	El formato de registro de fecha y hora es incorrecto.

Sintaxis de reglas de NWDB

En este tema se describe la sintaxis de reglas compatible con la sintaxis de reglas de NWDB en Reporting Engine. Para mejorar el tiempo de ejecución de las entidades informantes, consulte Guías para informes.

Una regla es una función que manipula el conjunto de resultados de una regla para lograr que la salida de un informe sea más concreta o para agregar una funcionalidad adicional distinta a la consulta de datos y su visualización. Se puede utilizar cualquier combinación de estas acciones de regla para crear representaciones únicas e interesantes de la información que recopila Security Analytics.

El Reporting Engine es compatible con las siguientes categorías de sintaxis de reglas de orígenes de datos de NWDB:

- Cláusula **Select**
  - Regla no agregada
  - Regla agregada
- Cláusula **Where**
- Operadores de la cláusula **Where**
- Cláusula **Then**
- Campo **Límite**
- Acciones de regla
- Operadores de regla

Cláusula Select

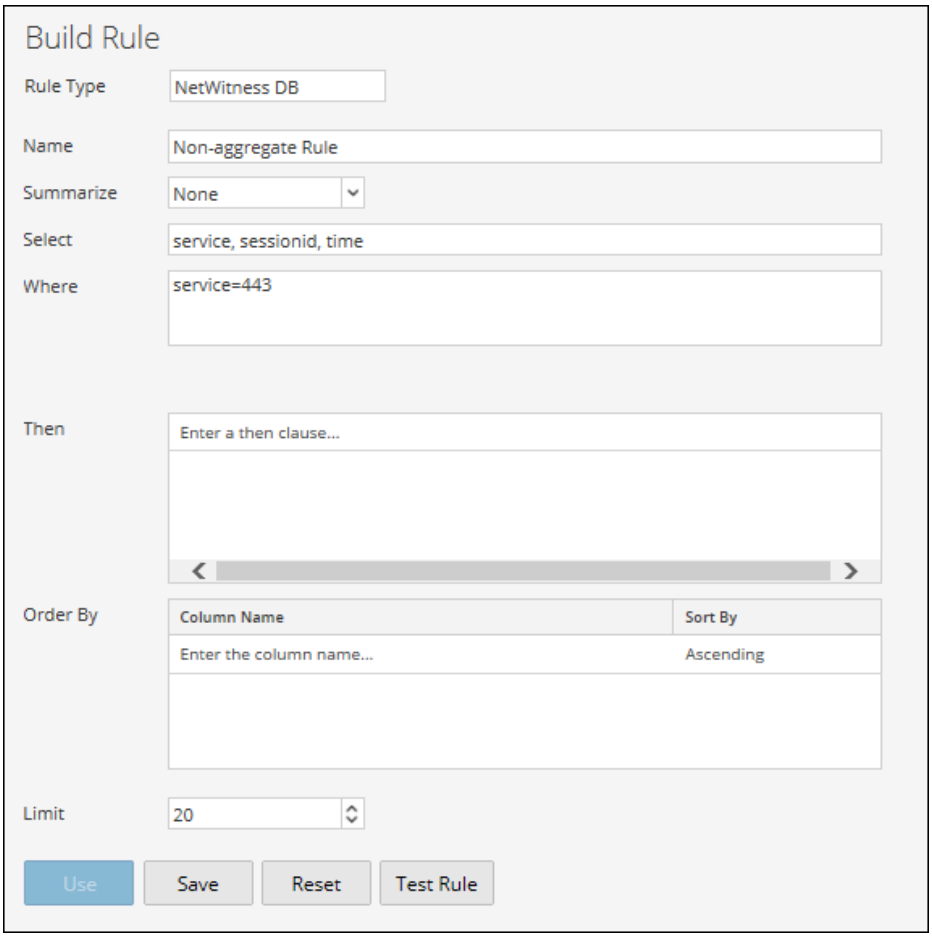
La cláusula Select es una lista de valores separados por comas. Por ejemplo: select sessionid,time,service.

Hay dos tipos de cláusulas Select para la regla NWDB:

- Regla no agregada
- Regla agregada

Regla no agregada

Cuando desee definir una regla sin agrupación, elija “Ninguno” en el campo Resumen. En una regla no agregada, puede seleccionar una cantidad indefinida de metadatos en la cláusula *Select*. Por ejemplo, select service, sessionid, time.

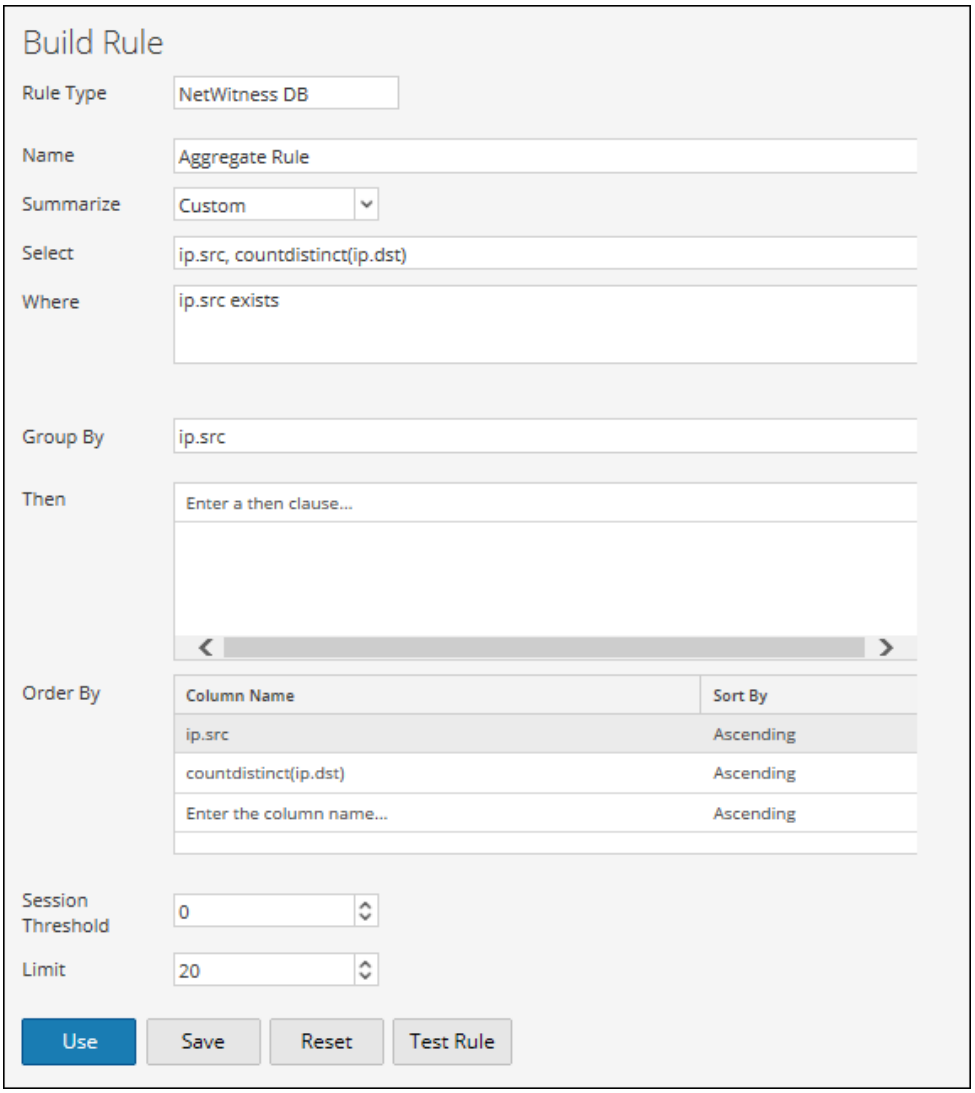


Regla agregada

Cuando desea consultar por metadatos específicos y su valor agregado asociado, debe usar la regla agregada. Para obtener un agregado, debe elegir cualquiera de los tres metadatos (Conteo de eventos, Conteo de paquetes o Tamaño de sesión) o seleccionar “Personalizado” en el campo **Resumen** para incluir una función de agregado en la cláusula *Select*. Por ejemplo, select ip.src, sum (ip.dst). Cuando se habilita la regla agregada Personalizado, se completan los siguientes campos en la interfaz del usuario:

- Agrupar por
- Ordenar por
- Umbral de sesión

En la siguiente figura se muestra la vista Crear regla para una regla agregada.



Existen dos tipos de valores de agregados que se pueden consultar:

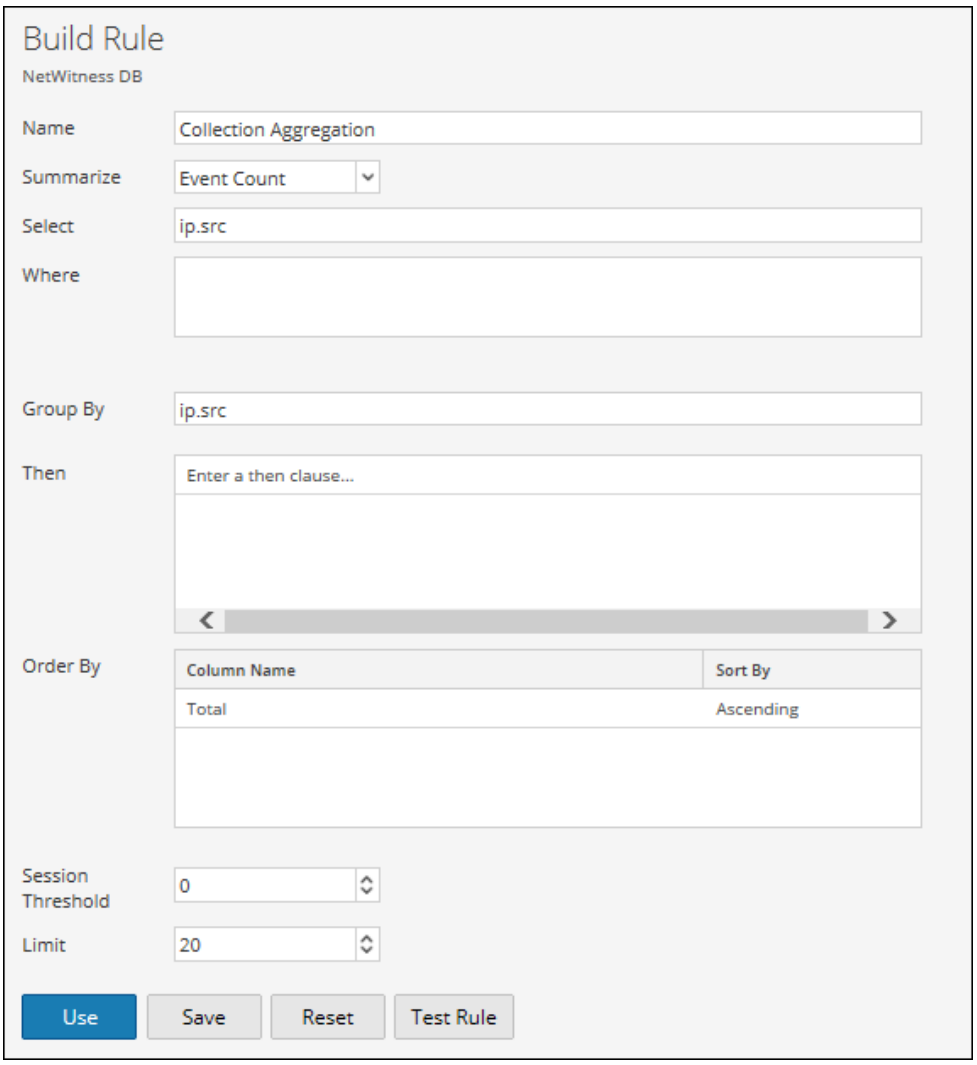
- Agregación de recopilados
- Agregación de metadatos

Agregación de recopilación

Con la agregación de recopilación, puede obtener agregados relacionados con eventos, sesiones o paquetes. Los siguientes valores se pueden solicitar en una agregación de recopilación:

- **Conteo de eventos**: El conteo total de eventos.
- **Conteo de paquetes**: El conteo total de paquetes.
- **Tamaño de sesión**: El tamaño total de la sesión.

Estas opciones se indican en el campo “Resumen ejecutivo” y cualquiera de ellas se puede seleccionar en una regla.
Por ejemplo, elija cualquiera de los agregados de Recopilación (Conteo de eventos, Conteo de paquetes o Tamaño de sesión) en el campo “Resumen” y seleccione ip.src.



Agregación de metadatos

Con la agregación de metadatos, puede obtener agregados de valores de metadatos. Las siguientes son las funciones de agregado de metadatos compatibles:

- sum(meta)
- count(meta)
- countdistinct(meta)
- min(meta)

- max(meta)
- avg(meta)
- first(meta)
- last(meta)
- len(meta)
- distinct(meta)

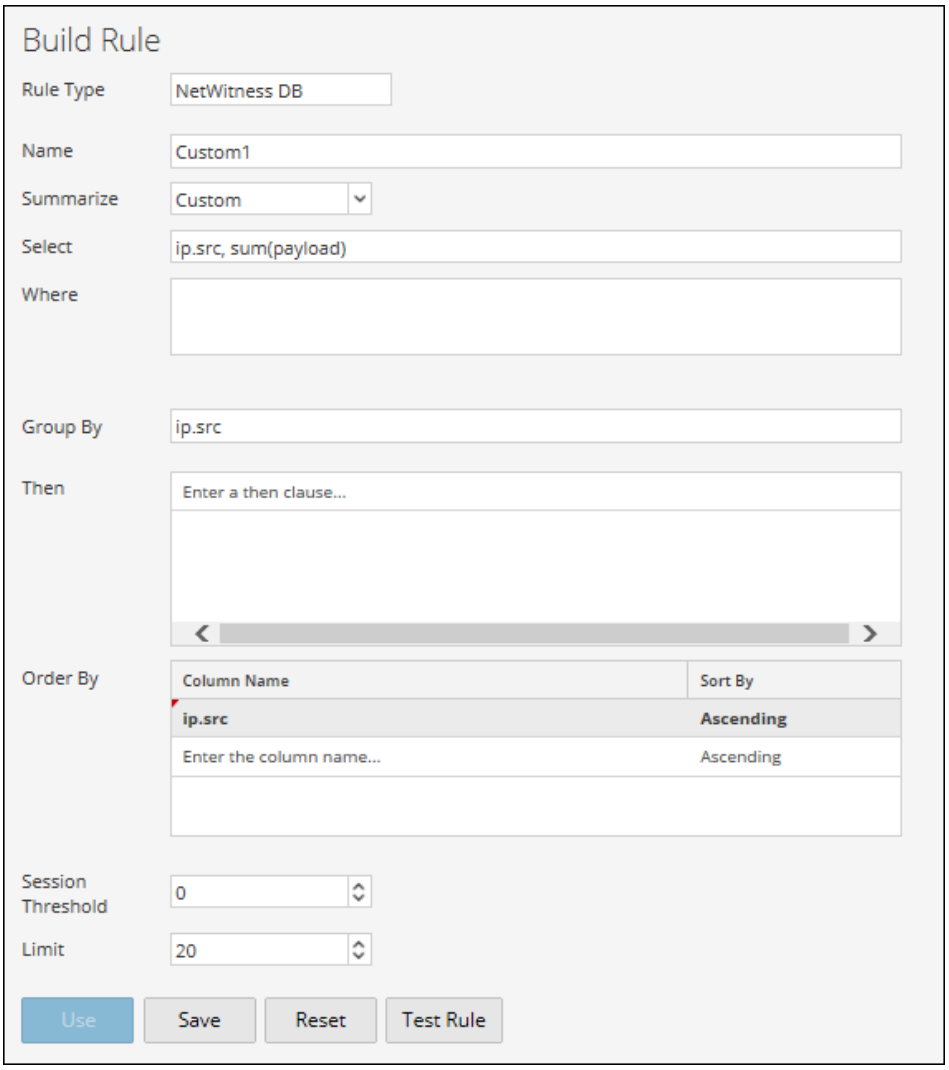
Funciones agregadas de metadatos compatibles

El servicio NWDB es compatible con las siguientes funciones agregadas y sintaxis en esta versión.

Sintaxis	Función
sum (<meta>)	La suma de todos los valores de metadatos. Por ejemplo, si proporciona el campo sum(payload) en la cláusula Select, el conjunto de resultados es la suma del tamaño de la carga útil. **Nota:** El campo de metadatos escogido para la función de suma de agregados debe ser del tipo de datos numéricos.
count (<meta>)	La cantidad total de campos de metadatos que se deberían devolver. Por ejemplo, si proporciona el campo count(ip.dst) en la cláusula Select, el conjunto de resultados es la cantidad de veces que se devuelve un valor ip.dst.
countdistinct (<meta>)	La cantidad total de campos de metadatos distintos que se devolverían. Por ejemplo, si proporciona el campo countdistinct(ip.dst) en la cláusula Select, el conjunto de resultados es la cantidad de veces que se devuelve un valor distinct ip.dst.
min (<meta>)	El mínimo de todos los valores de metadatos. Por ejemplo, si proporciona el campo min(payload) en la cláusula Select, el conjunto de resultados es el mínimo del tamaño de la carga útil.
max (<meta>)	El máximo de todos los valores de metadatos. Por ejemplo, si proporciona el campo max(payload) en la cláusula Select, el conjunto de resultados es el máximo del tamaño de la carga útil.

Sintaxis	Función
avg (<meta>)	El promedio de todos los valores de metadatos. Por ejemplo, si proporciona el campo avg(payload) en la cláusula Select, el conjunto de resultados es el promedio del tamaño de la carga útil. **Nota:** El campo de metadatos que se eligió para la función de promedio de agregados debe ser del tipo de datos numéricos.
first (<meta>)	La primera aparición del valor de metadatos. Por ejemplo, si proporciona el campo first(ip.src) en la cláusula Select, el conjunto de resultados es la primera aparición de ip.src para ese grupo.
last (<meta>)	La última aparición del valor de metadatos. Por ejemplo, si proporciona el campo last(ip.src) en la cláusula Select, el conjunto de resultados es la última aparición de ip.src para ese grupo.
len(<meta>)	Convierte todos los valores de campo a una longitud UInt32 en lugar de devolver el valor real. Esta longitud es el número de bytes para almacenar el valor real, no la longitud de la estructura almacenada en la base de datos de metadatos. Por ejemplo, el valor de metadatos “NetWitness” devuelve una longitud de 10. Todos los campos IPv4, como ip.src, devuelven 4 bytes.
distinct (<meta>)	Los valores distintos de los metadatos. Por ejemplo, si proporciona el campo distinct(ip.src) en la cláusula Select, el conjunto de resultados corresponde a todos los ip.src distintos para ese grupo.

Debe seleccionar “Personalizado” en el campo “Resumen” y proporcionar los metadatos y las funciones de agregado de metadatos en la cláusula Select.



Nota: Las funciones de agregado de metadatos no se pueden usar en una cláusula WHERE y las acciones de regla como min_threshold/max_threshold se pueden usar para filtrar funciones de agregado. Se recomienda usar una cláusula WHERE más refinada para obtener un mejor rendimiento de la regla cuando se usa "group by".

Consulta de agregado para múltiples metadatos

Para ejecutar una consulta de agregado para múltiples metadatos, siga estos pasos:

1. En el menú de Security Analytics, haga clic en **Administration > Informes**.

   Se resalta la pestaña Administrar y se muestra la vista **Reglas**.

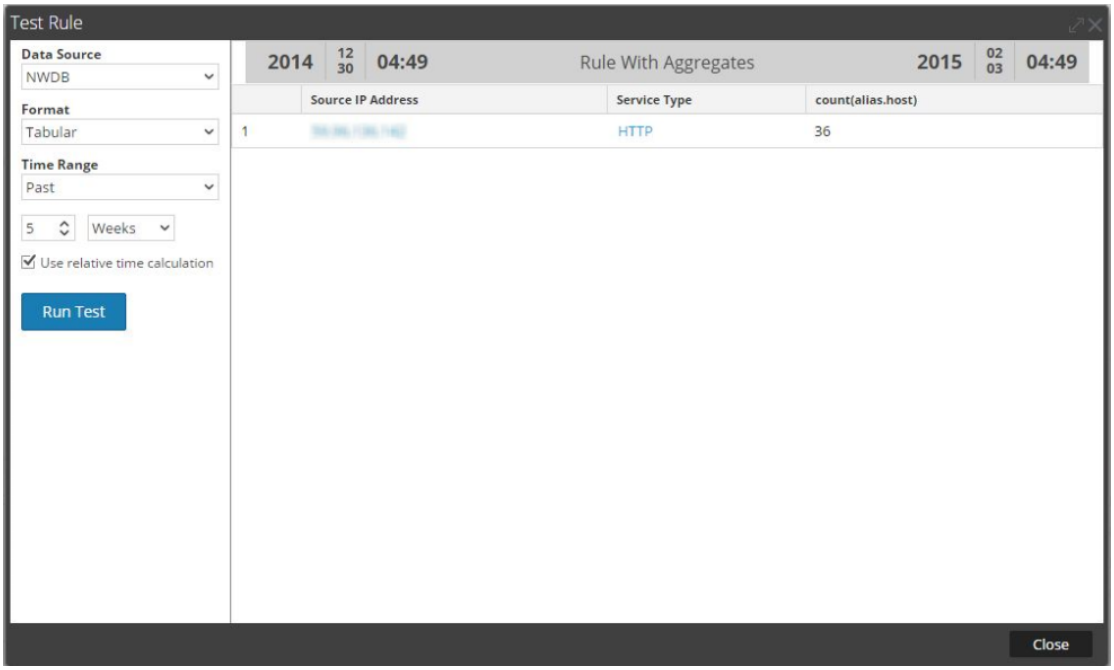
2. En la barra de herramientas Regla, haga clic en  > **Base de datos de NetWitness**.

   Por ejemplo, ingrese los siguientes metadatos en los campos que se resaltan a continuación:

SELECT: ip.src, service, count(alias.host)
WHERE: ip.src = 59.96.136.142

3. Haga clic en el botón **Probar regla** de la parte inferior de la pantalla.

   Aparecerá la página Probar regla.



Resumen

Resumen determina el tipo de resumen o agregación para la regla.

Nombre	Valor de configuración
Resumen	Para consultar metadatos sin ninguna agrupación personalizada, seleccione: • **Ninguno**: los datos se agrupan por sesión en este caso. Para obtener agregados relacionados con la recopilación (sesiones/eventos/paquetes), seleccione una de las siguientes opciones: • **Conteo de eventos**: El conteo total de eventos. • **Conteo de paquetes**: El conteo total de paquetes. • **Tamaño de sesión**: El tamaño total de la sesión. Para obtener agregados basados en metadatos, seleccione: • **Personalizada**: Esto indica que la función agregada de metadatos esperados se define en la cláusula Select de la regla.

Ordenar por

Ordenar por determina cómo se ordena el conjunto de resultados.

Nombre	Valor de configuración
Nombre de la columna	El **Nombre de la columna** es el nombre de las columnas según las cuales desea ordenar los resultados. El valor está vacío de forma predeterminada. Cuando hace clic en una columna, el valor se completa de acuerdo con el campo Resumen. • Para “Ninguno” y “Personalizado”, el valor se completa de acuerdo con las entradas hechas en el campo Select. Puede seleccionar un valor de esta lista o agregar un nombre personalizado. • Para Conteo de eventos, Conteo de paquetes y Tamaño de sesión, los valores aceptados son Total y Valor. • Total: se ordena por valor agregado • Valor: se ordena por grupo por metadatos
Ordenar por	**Ordenar por** determina el orden en el cual desea clasificar los resultados. Los valores son los siguientes: • Orden ascendente • Orden descendente

Umbral de sesión

El umbral de sesión es la configuración de optimización para detener el escaneo de las sesiones coincidentes para cada valor único posible
para los metadatos seleccionados. El umbral es un número entero entre 0 (predeterminado) y 2,147,483,647. El umbral 0 escanea todas las sesiones coincidentes.

Nota: Si proporciona un valor distinto de cero (un valor mayor que cero), los resultados del agregado son inexactos. Esto puede utilizarse únicamente cuando está interesado en valores únicos y no en valores agregados.

Cláusula Where compatible

Sintaxis	Descripción
where <field1> [<field-operator>] <value1>,<value2>,<value3-value4> <logic-operator> <field2>, etc.	La cláusula Where es una lista separada por comas de los valores y rangos de campos de idiomas que utiliza la función NwValues. En la cláusula Where, los valores de cadena deben estar encerrados en comillas simples. Por ejemplo, where username = 'admin' && service = 22.
where <field1> [<field-operator>] <List1>	Puede usar una lista en la cláusula Where si tiene múltiples valores que informar. Por ejemplo, where ip.src exists && alias.host exists && alias.host contains $[User Reports/List of Alias Host]. Cuando utiliza la lista, debe especificar en el formato $[<path>/<List name>].

En la cláusula Where, asegúrese de que la sintaxis esté correcta según el tipo de metadatos.
Por ejemplo,
Para todos los tipos de metadatos de texto, use comillas; por ejemplo, username = 'user1'.
Para todas las direcciones IP, las direcciones de Ethernet y los tipos de metadatos numéricos, no utilice comillas; por ejemplo, service = 80 && ip.src = 192.168.1.1.
Para los tipos de metadatos de fecha y hora, si el formato de fecha y hora es "AAAA-MM-DD HH:MM:SS", utilice comillas.
Si el formato de fecha y hora es 1448034064 (número de segundos transcurridos desde EPOCH (1 de enero de 1970), no use comillas.

Nota: Si se utiliza una lista en la regla, asegúrese de que los valores de la lista estén entre comillas o sin comillas en función del tipo de metadatos que se utiliza. Si marca la casilla de verificación **Se insertarán comillas para todos los valores** en la página de definición de lista (para obtener más información, consulte la sección Agregar una lista), se agregarán comillas a todos los valores de la lista.

Operadores de cláusula Where compatibles

Sintaxis	Descripción
=	Devuelve los resultados donde el campo es igual a cualquier valor proporcionado. Por ejemplo, tcp.dstport = 21-25,110 devuelve la sesión con puertos de destino TCP de 21, 22, 23, 24, 25 o 110.

Sintaxis	Descripción
!=	Devuelve resultados para los campos que no coinciden con los valores especificados. Por ejemplo, eth.type !=0x0800 devuelve sesiones fuera del valor hexadecimal (valor decimal de 2048), que son todos los protocolos que no se basan en IP.
begins	Verifica un valor en el comienzo de un texto o campo binario.
contains	Busca un textoo valor binario para una coincidencia parcial.
ends	Verifica un valor al final de un texto o campo binario.
exists	Si el valor de campo existe, independientemente del valor, la operación se evalúa como verdadera.
!exists	Si el valor de campo no existe, la operación se evalúa como verdadera.
length	Evalúa la longitud del campo. Por ejemplo, username length 20-u devuelve todos los nombres de usuario que tienen 20 o más caracteres de longitud.
regex	Ejecuta una búsqueda de expresión regular contra el texto o los valores binarios.

Cláusula Then compatible

Sintaxis	Descripción
then <rule action>	La cláusula Then contiene una acción de regla que manipula el conjunto de resultados original de una regla para lograr que la salida en un informe sea más concreta o agregar una funcionalidad adicional distinta de la consulta de datos y su visualización. Por ejemplo, dedup (nombre de archivo).

Campo Límite

Indica el límite que se introducirá en la consulta mientras se obtienen los datos de la base de datos. Si un conjunto de resultados se ordena por conteo de
eventos, conteo de paquetes o tamaño de sesión, el límite representa los N valores superiores (o inferiores) que se devolverán. Si el conjunto de resultados no
se ordena, se devuelven los primeros N valores.

Acciones de regla

La sintaxis de regla de orígenes de datos de NWDB es compatible con las siguientes acciones de regla:

- dedup
- filter_on
- filter_out
- lookup_and_add
- max_threshold
- min_threshold
- regex
- sum_count
- sum_values
- show_whats_new

dedup (string field)

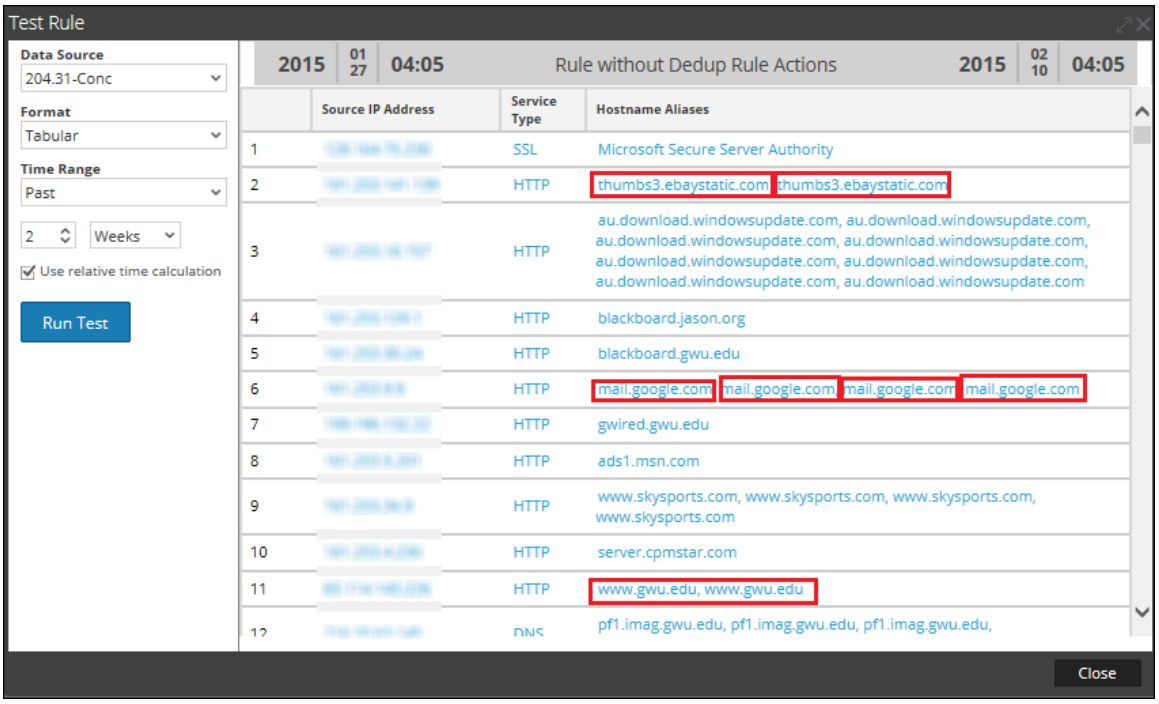
Dedup elimina las entradas duplicadas en un conjunto de resultados desordenado y solo muestra datos pertinentes. La acción de regla dedup elimina entradas duplicadas de un campo específico del informe, de modo que solo se incluye la primera aparición de ese valor en el informe.

Nota: La acción de regla dedup no se puede usar con una regla agregada.

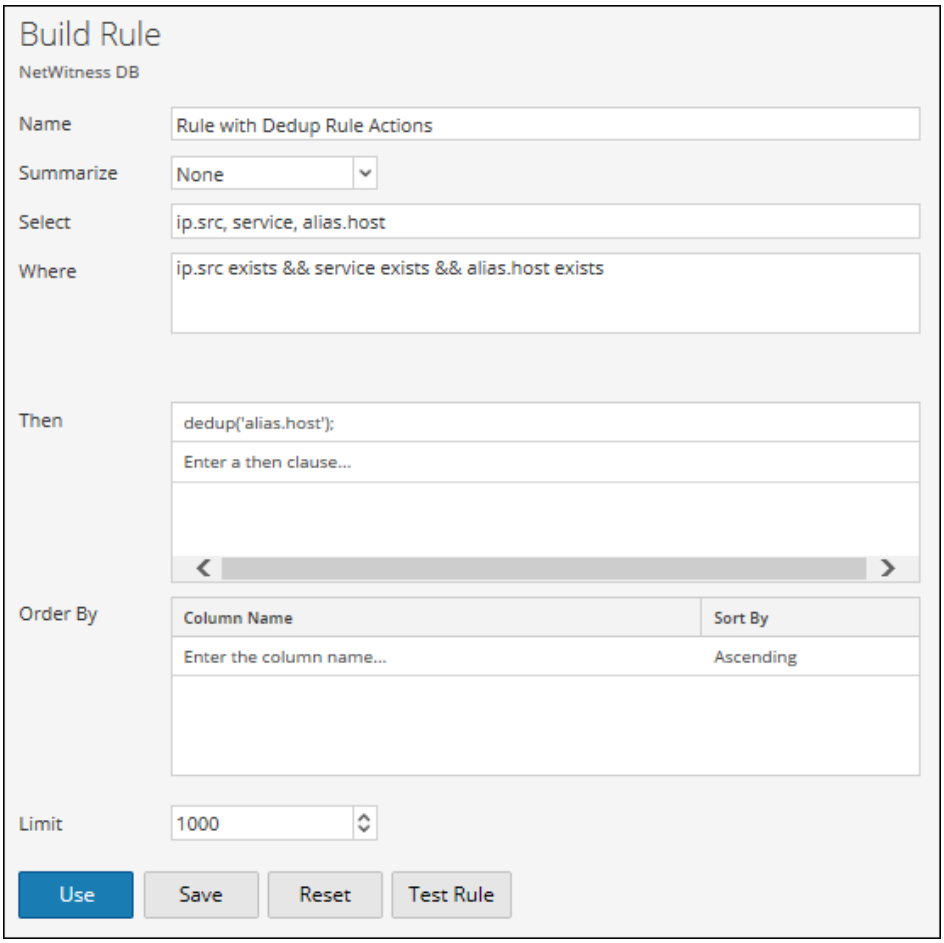
Por ejemplo, los metadatos que genera una sesión individual son generalmente repetitivos, en especial cuando tiene sesiones con muchas búsquedas de DNS o sesiones web que acceden al mismo host en múltiples ocasiones para varios recursos (como javascript, css). Para quitar las entradas duplicadas del host, puede usar la acción de regla dedup.

Ejemplo:

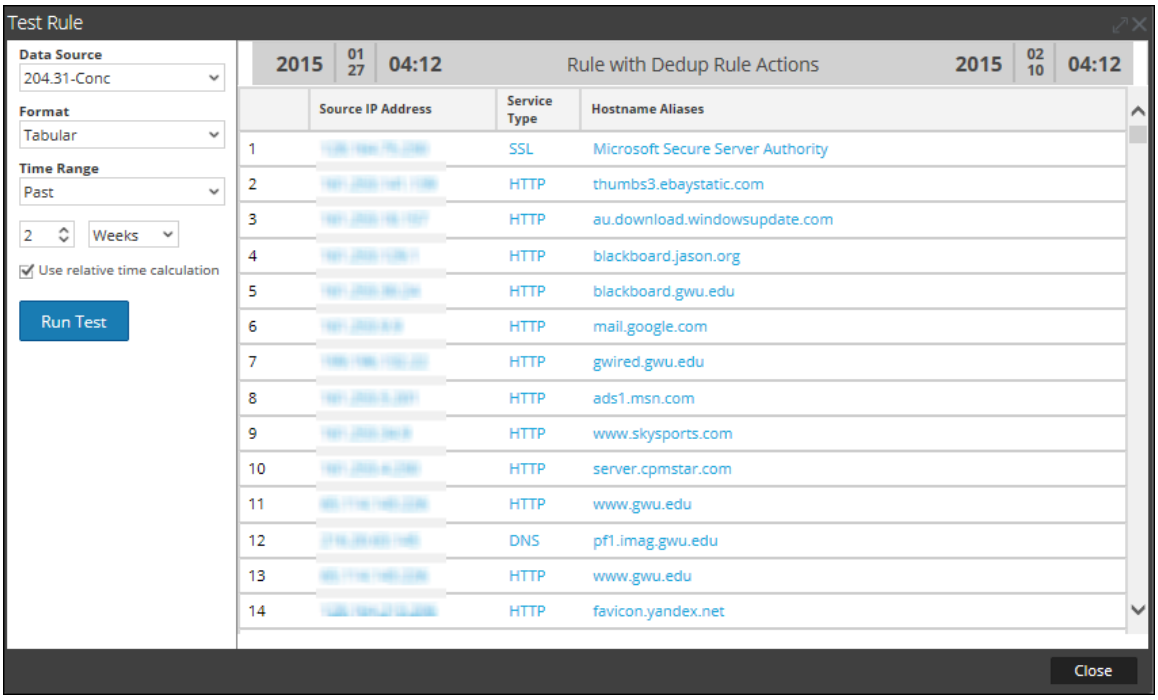
El siguiente ejemplo es un conjunto de resultados extenso que se puede acortar eliminando los valores duplicados en la misma sesión.



Las siguientes figuras muestran la acción de regla dedup para eliminar las entradas duplicadas del conjunto de resultados.



El valor duplicado de cada entrada en el conjunto de resultados de la regla se reduce a un valor.



filter_on (string filter, string field, bool matchExact)

`filter_on` quita valores que no contienen el criterio `filter` del conjunto de resultados. Si el conjunto de resultados contiene múltiples campos, debe seleccionar un campo específico al cual se aplica el filtro. Para agregar resultados adicionales a un único conjunto de resultados, incluya una función como lookup_and_add.

El parámetro matchExact determina si la coincidencia es una coincidencia exacta o si contiene una coincidencia.

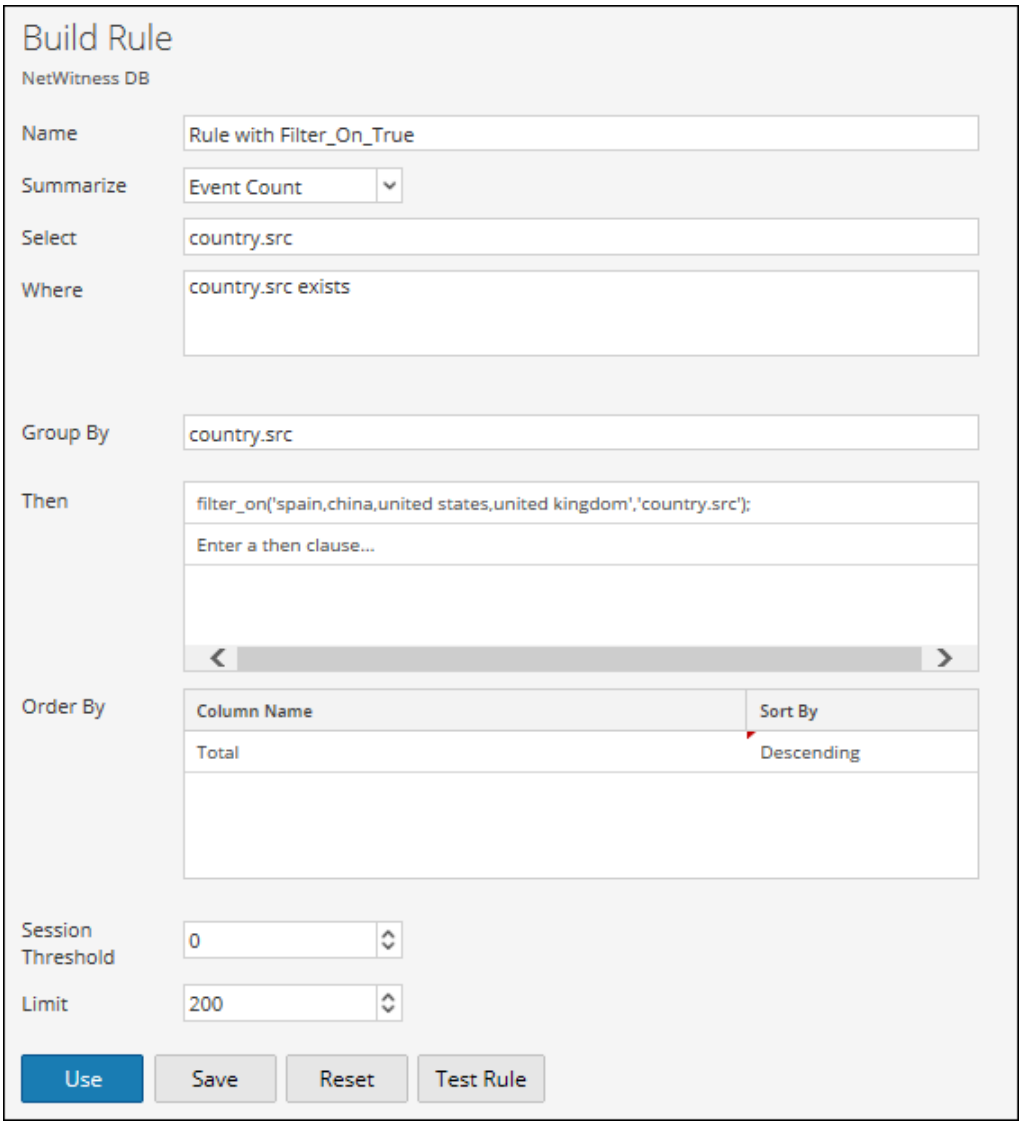
- Si matchExact se configura en `false`,, cualquier valor que contiene el texto de filtro se considera una coincidencia.
- Si matchExact se configura en `true`, solamente los valores que coinciden con el texto de filtro proporcionado se incluyen en el conjunto de resultados.

Nota: A menos que se especifique el parámetro matchExact, el comportamiento predeterminado de la acción de regla será coincidir exactamente con el texto especificado en el parámetro de filtro. Para especificar que los resultados que contienen el texto de filtro se mantengan en el conjunto de resultados, los usuarios deben configurar el parámetro matchExact en falso.

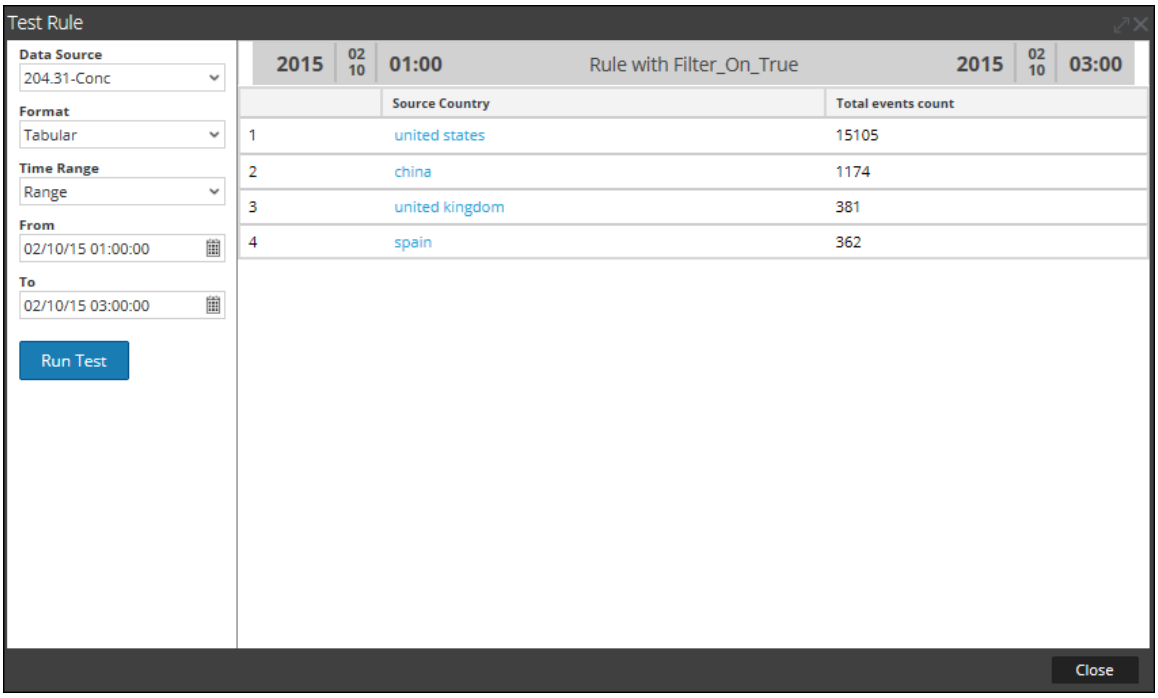
Ejemplo:

La siguiente figura muestra la lista de países y su conteo de eventos.

En la siguiente figura se muestra una acción de regla filter_on para excluir países del conjunto de resultados, con excepción de España, China, Estados Unidos y Reino Unido.



En la siguiente figura se muestra la salida con la acción de regla filter_on:



Otra forma de filtrar las salidas de cada conjunto de resultados es crear una lista de variables que desea filtrar. Por ejemplo, puede crear una lista con Reino Unido, Francia y Alemania como valores de la lista. Puede utilizar esta lista en la acción de regla para obtener el mismo conjunto de resultados. Por ejemplo, si crea una lista denominada COUNTRY_LIST, puede utilizar la lista de la siguiente manera:

```
filter_on ('$COUNTRY_LIST', 'country.src', 'false');
```

```
filter_out (string filter, string field)
```

```
filter_out (string filter, string field, bool matchExact)
```

filter_out elimina los valores que contienen el criterio *filtro* del conjunto de resultados. Si el conjunto de resultados contiene múltiples campos, debe seleccionar un campo específico al cual se aplica el filtro (por ejemplo, puede utilizar lookup_and_add para agregar resultados a un único conjunto de resultados).

El parámetro matchExact determina si la coincidencia es una coincidencia exacta o si contiene una coincidencia.

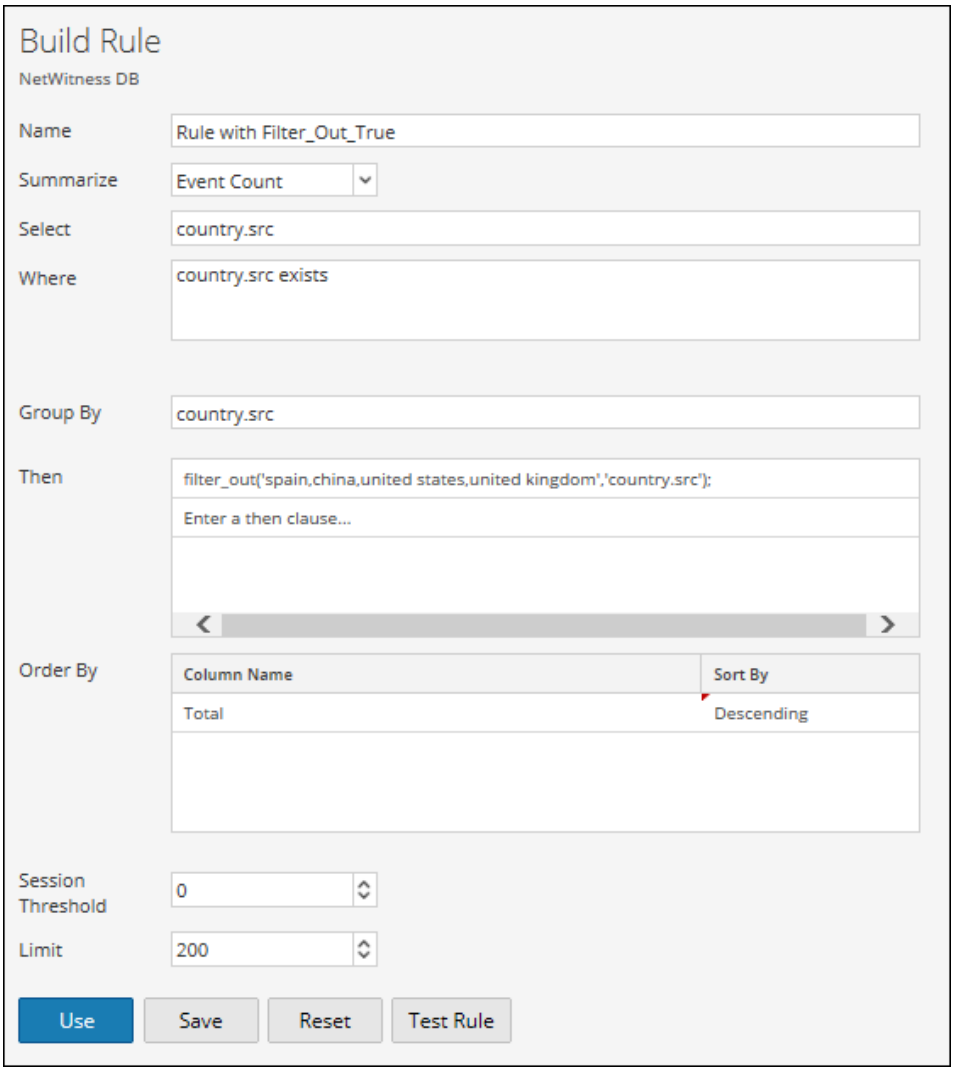
- Si matchExact se configura en falso, cualquier valor que contiene el texto de filtro se considera una coincidencia.
- Si matchExact se configura en verdadero, solamente los valores que coinciden con el texto de filtro proporcionado se excluyen del conjunto de resultados.

Nota: A menos que se especifique el parámetro `matchExact`, el comportamiento predeterminado de la acción de regla es buscar una coincidencia exacta para el texto especificado en el parámetro de filtro. Para especificar que los resultados que contienen el texto de filtro se quiten del conjunto de resultados, los usuarios deben configurar el parámetro `matchExact` en falso.

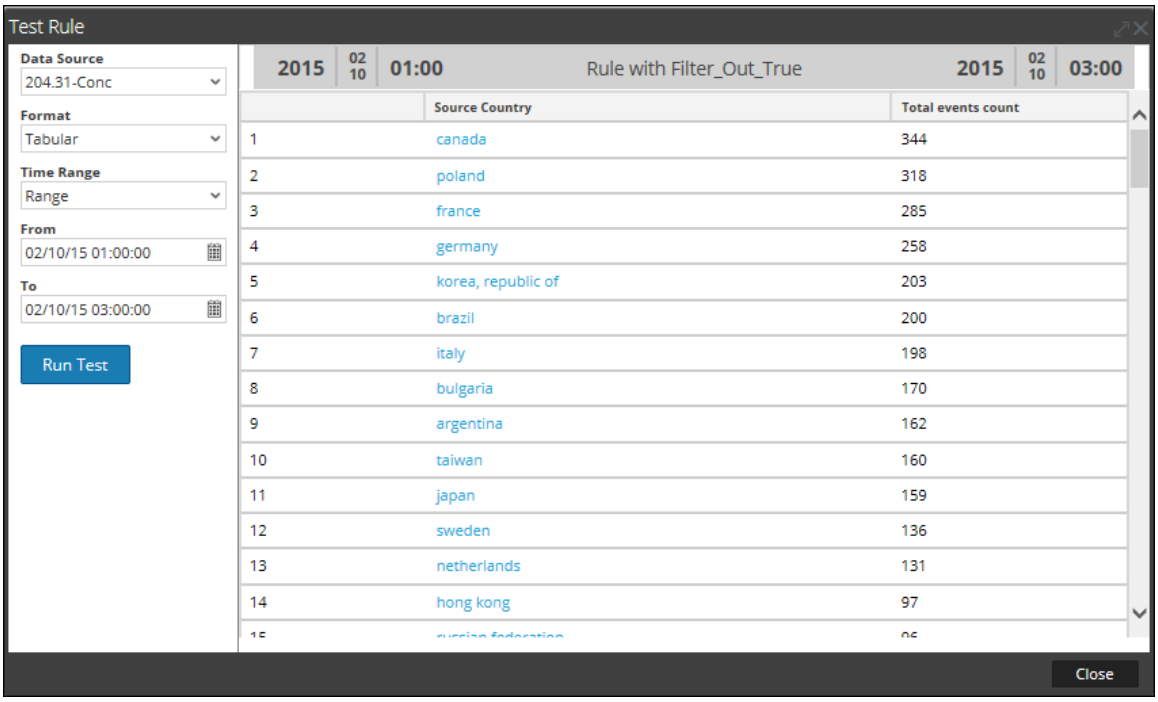
Ejemplo:

La siguiente figura muestra la lista de países y su conteo de eventos.

En la siguiente figura se muestra la acción de regla filter_out para eliminar el conteo de eventos de España, China, Estados Unidos y Reino Unido del conjunto de resultados.



En la siguiente figura se muestra la salida con la acción de regla filter_out.




```
lookup_and_add (string select, string field)
```

```
lookup_and_add (string select, string field, int limit)
```

```
lookup_and_add (string select, string field, int limit, boolean inherit)
```

```
lookup_and_add (string select, string field, int limit, boolean inherit,
string extraWhere)
```

```
lookup_and_add(string select, string field, int limit, boolean inherit,
string extraWhere, boolean aggregate)
```

Esta acción de regla realiza una iteración mediante una lista de valores en un conjunto de resultados y busca metadatos adicionales para describir con más detalles las relaciones entre diversos elementos dentro de un conjunto de resultados.

Nota: La acción de regla lookup_and_add se puede usar solo con una regla agregada.

El primer parámetro, select, designa el tipo de metadatos que se debe agregar a los elementos del conjunto de resultados. El segundo parámetro, field, especifica en qué parte del conjunto de resultados se debe aplicar el adjunto. Además, se puede aplicar un límite para evitar la sobrecarga del conjunto de resultados con un gran conjunto de resultados.

De manera predeterminada, las consultas posteriores que se realicen a SDK heredan la cláusula Where de la regla principal. Para usar una cláusula Where única, puede especificar un valor booleano en el cuarto parámetro como false y, en el quinto parámetro, especificar una cláusula Where diferente.

Nota: Si está utilizando una cláusula where única en su consulta, asegúrese de utilizar una comilla simple (') para encerrar argumentos y comillas dobles (") para los valores de cadena.

Ahora, con la adición del resumen **Personalizado** y la función **Group By**, el resultado se puede lograr incluso sin tener una acción de regla lookup_and_add. La sintaxis de la nueva regla con groupby muestra el resultado en una estructura plana que es mejor que la sintaxis de regla anterior sin groupby. Por lo tanto, se recomienda editar/actualizar manualmente las reglas con la acción de regla lookup_and_add y usar la cláusula groupby dondequiera que pueda aplicarse.

Nota: La acción de regla Lookup_And_Add solo es compatible si la cláusula SELECT tiene un metadato y una función de agregado.

Por ejemplo, consulte los siguientes escenarios: En el ejemplo **2a**, se usa la acción de regla lookup_and_add. En lugar de usar la acción de regla lookup_and_add, se puede lograr el mismo resultado si se usa el resumen **Personalizado** y la función **Group By**. Consulte el ejemplo **2b** más adelante.

Sin embargo, la acción de regla lookup_and_add es compatible con las reglas de NWDB en las siguientes condiciones:

- Todas las versiones de reglas de NWDB en las cuales Resumen está configurado en Conteo de eventos, Conteo de paquetes o Tamaño de sesión.
- En el caso del resumen Personalizado, la regla lookup_and_add debe tener solo un metadato group by con solo una función de agregado, y esta debe ser sum() o count().

Nota: No es compatible con “Resumen: Ninguno”.

Por ejemplo, la acción de regla lookup_and_add se puede usar para las siguientes reglas:

- select ip.src, sum(size) group by ip.src
- select ip.src, count(filename) group by ip.src

No se puede usar para las siguientes reglas:

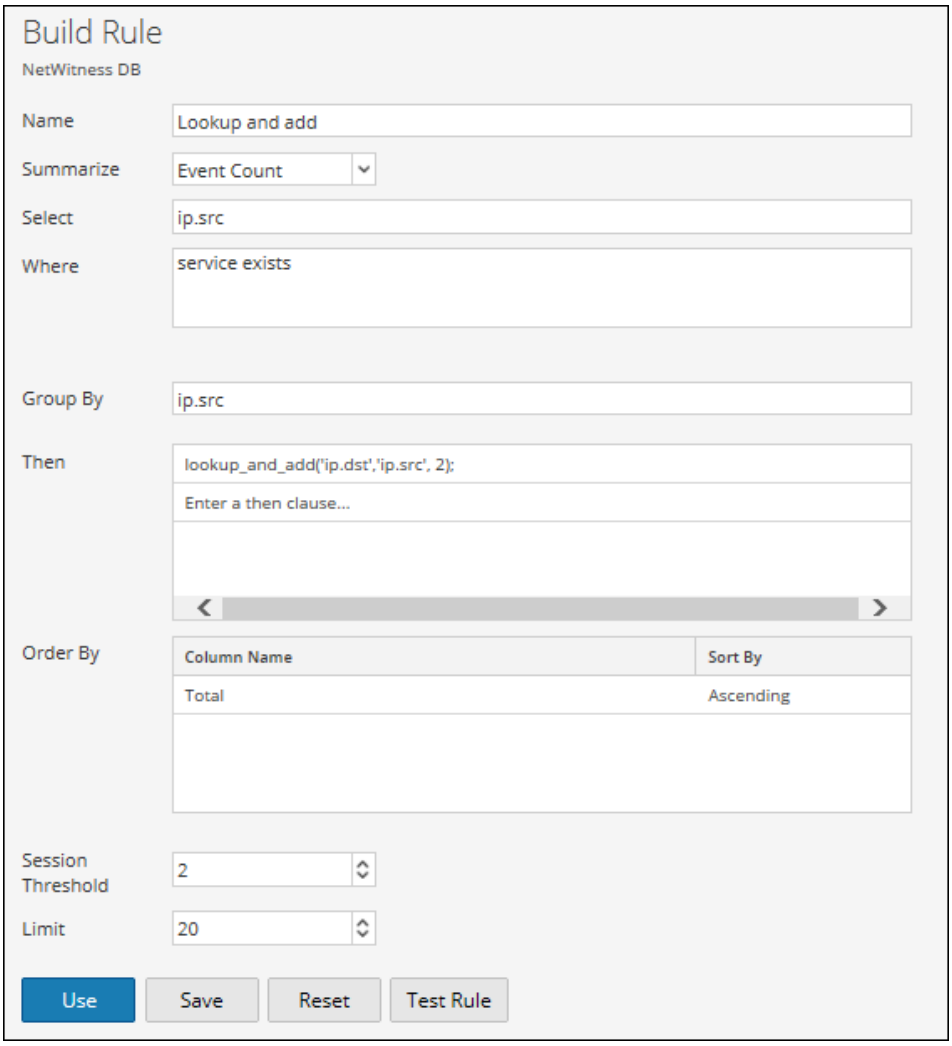
- select ip.src, sum(size),count(filename) group by ip.src
- select ip.src, sum(size),avg(size) group by ip.src
- select ip.src,ip.dst count(filename) group by ip.src,ip.dst

Ejemplos:

1. lookup_and_add('ip.dst','ip.src', 2);

Esta acción de regla se repetirá a través de cada ip.src en el conjunto de resultados inicial y buscará las dos direcciones IP de destino principales con cada ip.src.

La siguiente figura muestra la definición de la regla.

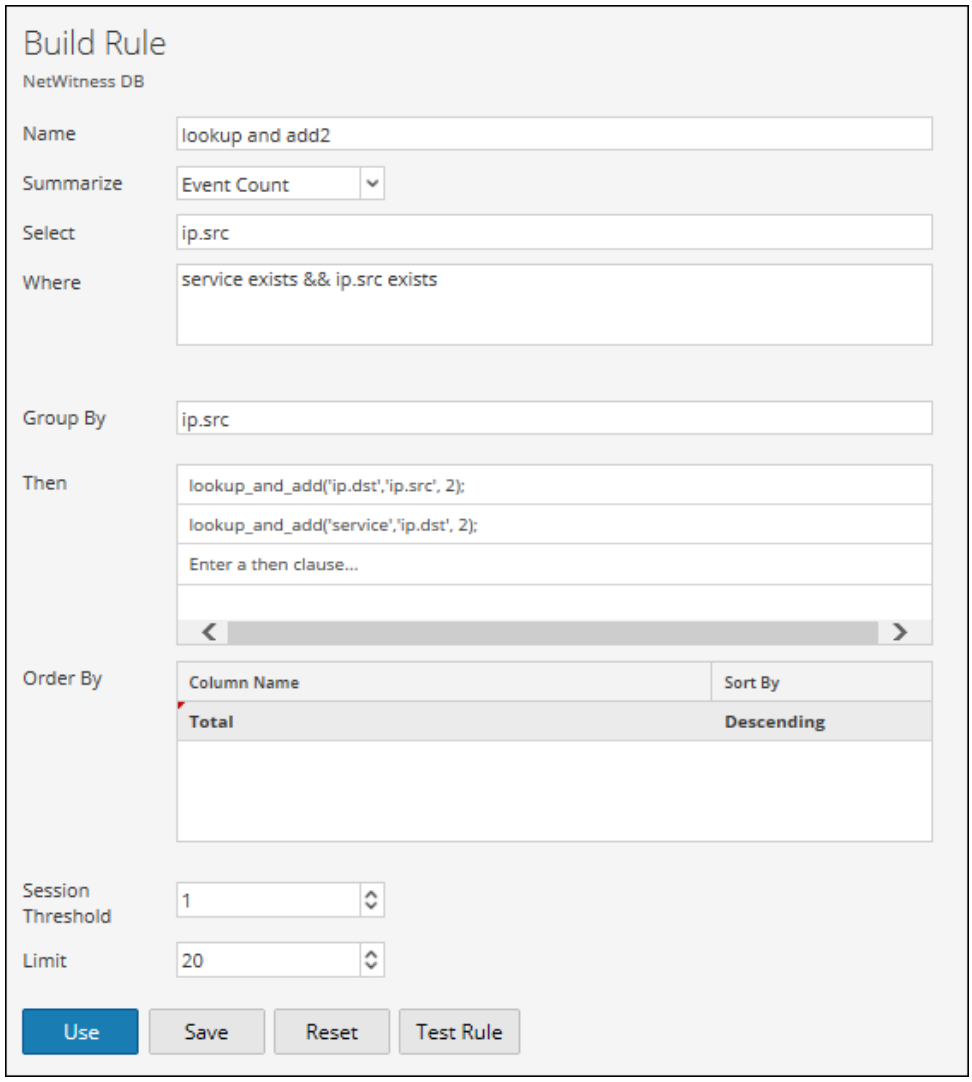


En la siguiente figura se muestra el conjunto de resultados que contienen las direcciones IP de origen y las dos direcciones IP principales de destino con cada ip.src.

2a. lookup_and_add('ip.dst','ip.src', 2); lookup_and_add('service','ip.src', 3);

Esta acción de regla realizará la iteración a través de cada ip.src en el conjunto de resultados inicial y buscará las dos direcciones IP de destino principales con cada ip.src y los tres puertos principales utilizados por ip.src.

La siguiente figura muestra la definición de la regla.



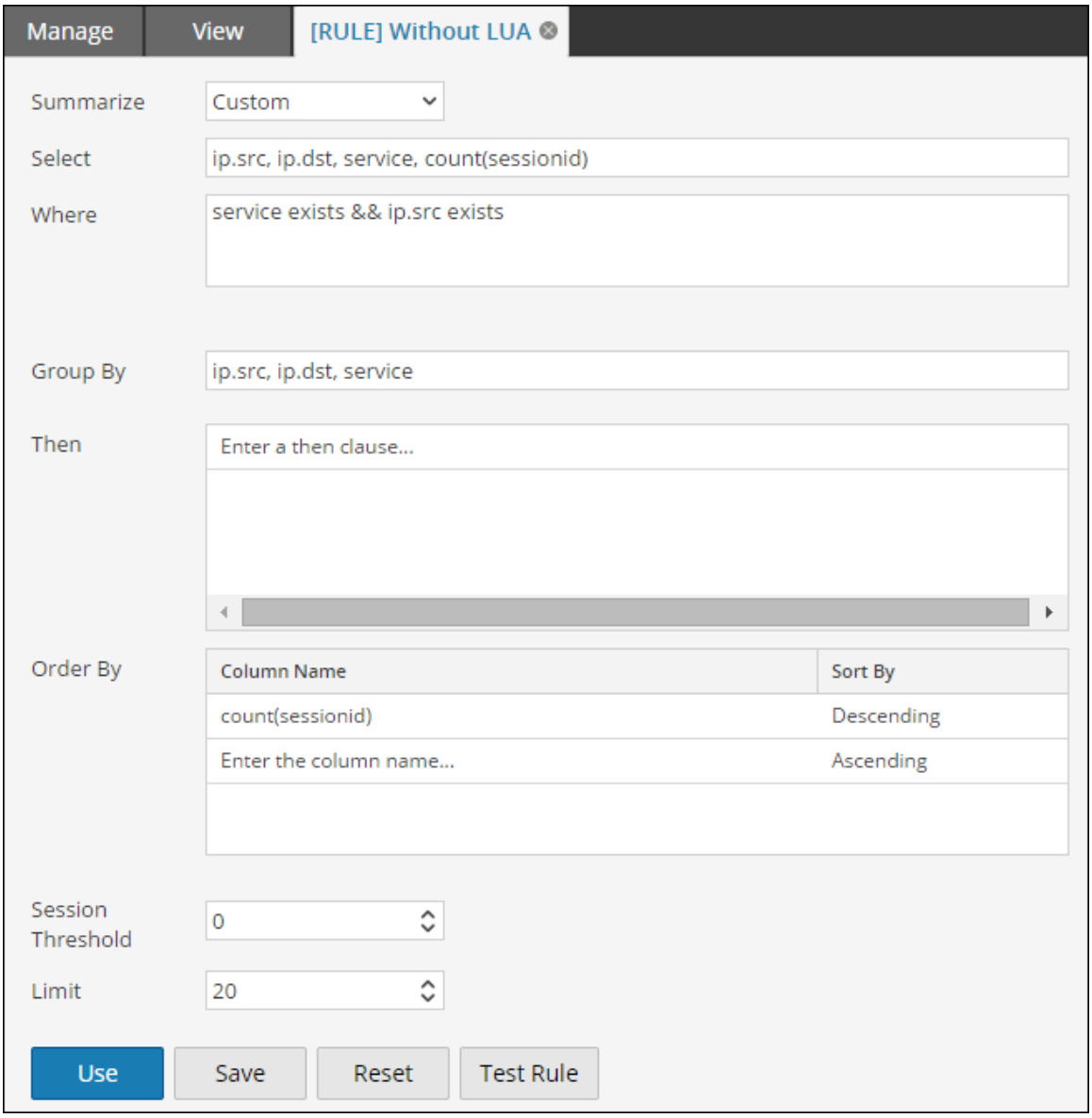
La siguiente captura de pantalla muestra el conjunto de resultados que contienen las direcciones IP de origen y las dos direcciones IP principales de destino con cada ip.src y los tres puertos principales utilizados por cada ip.src:

Puede hacer la consulta con el grado de complejidad que desee mediante la selección de diferentes campos en el conjunto de resultados y la adición a diferentes partes. Por ejemplo, puede que desee saber qué archivos ha tocado cada IP de origen. Sin embargo, debido a que la regla principal tiene una cláusula WHERE service = 6667 y a que el comportamiento predeterminado de esta acción de regla es anexarse a la cláusula WHERE original, será necesario reemplazar la cláusula WHERE primaria. La manera más fácil de comprender este concepto es buscar en la llamada lookup_and_add anterior: lookup_and_add('ip.dst','ip.src',2). La consulta real que se envía al servidor es SELECT ip.dst WHERE service = 6667 &&ip.src = 206.42.199.194. Para forzar que la cláusula WHERE reemplace la parte de service = 6667 de la cláusula WHERE (heredada de la regla primaria), el usuario puede especificar un cuarto parámetro false, como se muestra en el ejemplo 3.

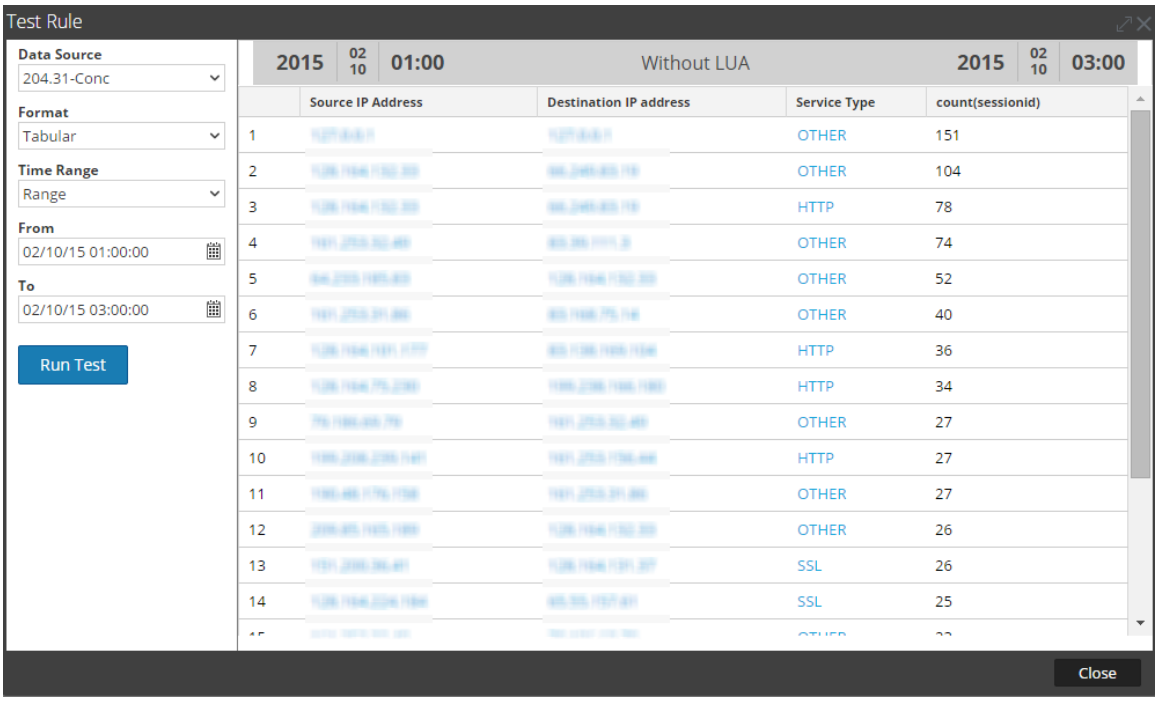
2b. Sin la regla lookup_and_add

Esta regla usa el resumen Personalizado y la función Group By para ordenar los resultados.

La siguiente figura muestra la definición de la regla.



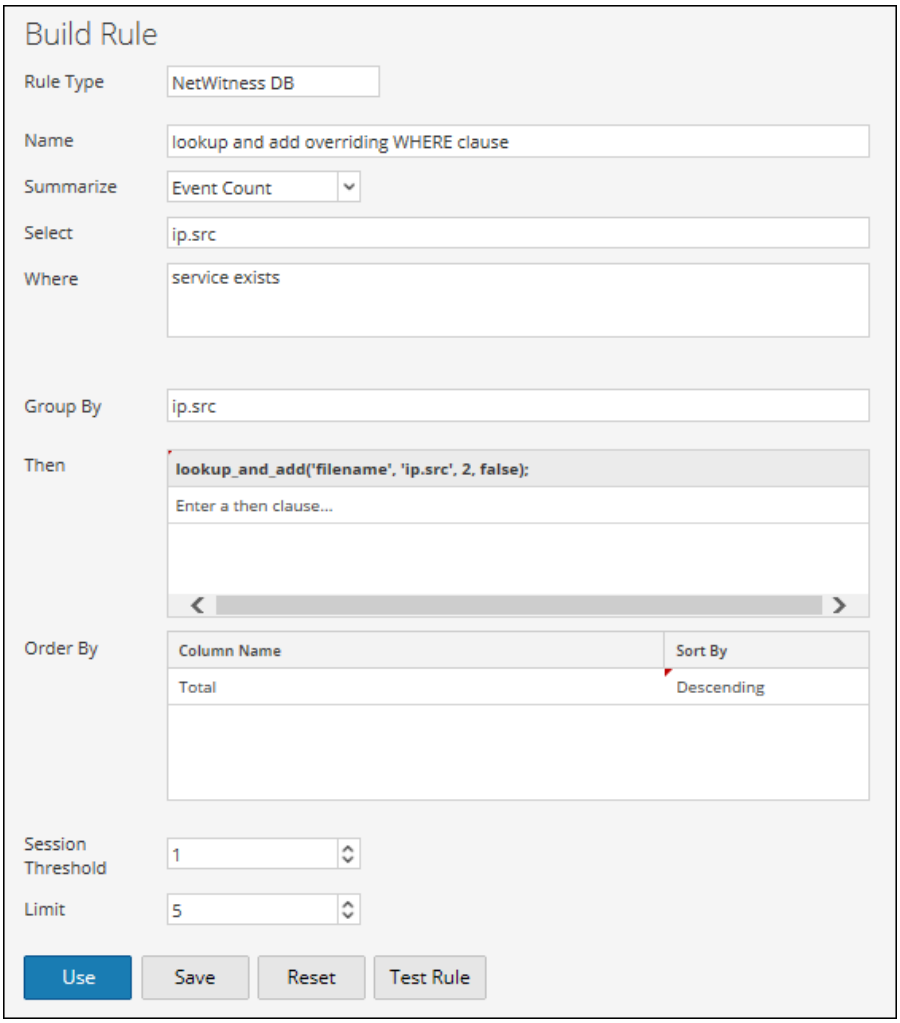
La siguiente captura de pantalla muestra el conjunto de resultados que contienen las direcciones IP de origen y las dos direcciones IP principales de destino con cada ip.src y los tres puertos principales utilizados por cada ip.src:



3. lookup_and_add('filename', 'ip.src', 2, false);

Esta llamada enviaría una consulta al servidor, como `SELECT filename WHERE ip.src = 90.0.0.142` en lugar de `SELECT filename WHERE service = 6667' && ip.src = 90.0.0.142`, porque se especificó la acción de regla para omitir la cláusula `WHERE` inicial de la regla primaria.

La siguiente figura muestra la definición de la regla.



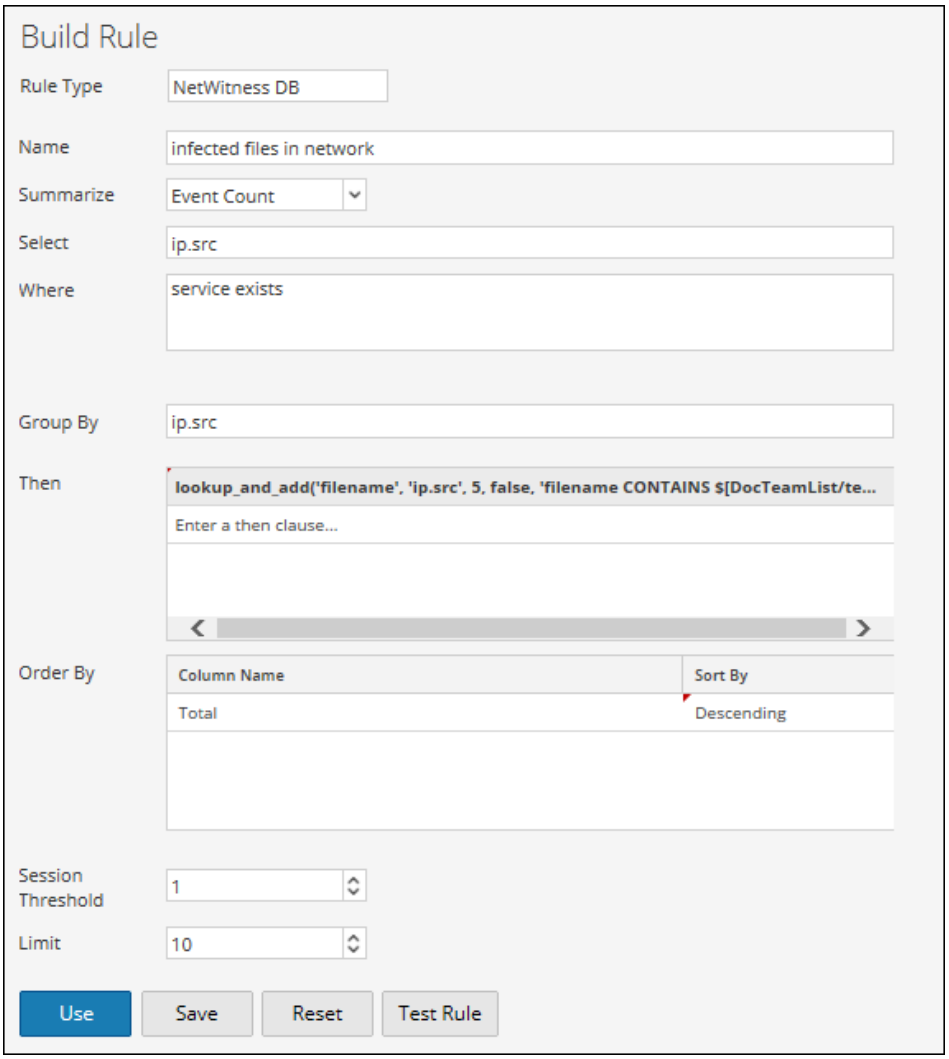
La siguiente figura muestra el conjunto de resultados.

La lista test está en un grupo llamado netwitness, puede acceder a esa lista con la siguiente sintaxis.

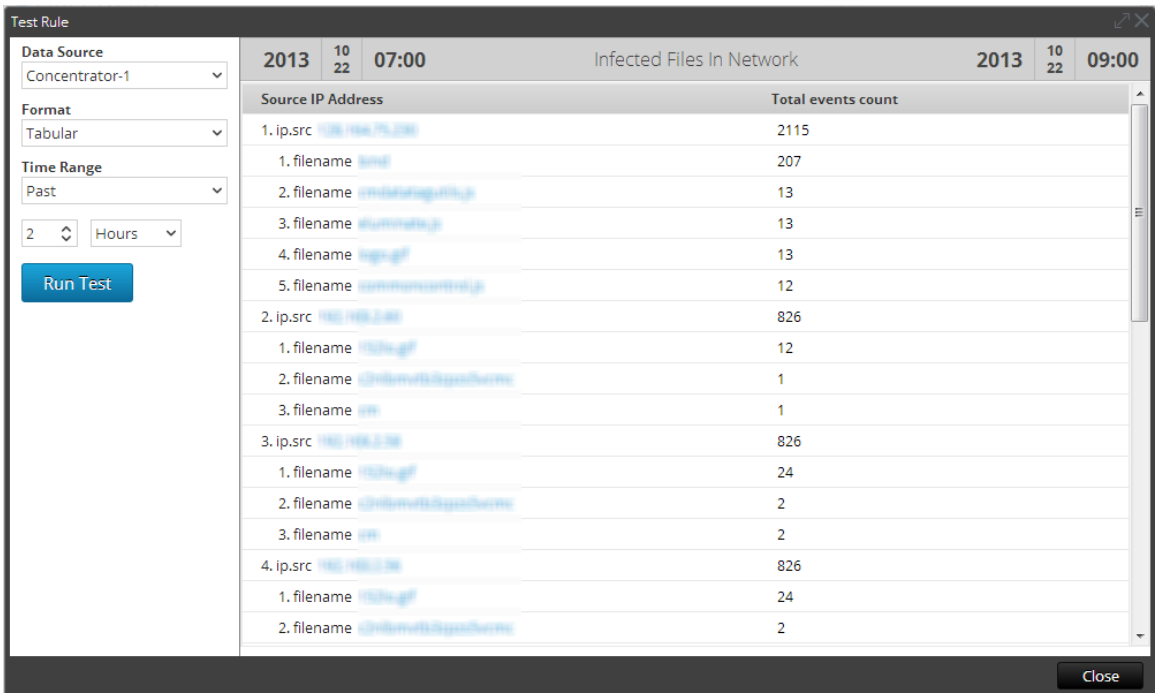
Incluso puede acotar aún más estos resultados anexados para incluir solamente nombres de archivos que tengan .gif como la extensión del nombre de archivo utilizando el quinto parámetro en la acción de regla. El quinto parámetro le permite especificar criterios adicionales de la cláusula WHERE. Los archivos con extensión de nombre de archivo .gif se almacenarían en la lista **test** dentro de un grupo llamado **DocTeamList**. Puede acceder a esta lista con la siguiente sintaxis: threat.source = $[DocTeamList/test]
Puede hacer referencia a ella en el parámetro de la cláusula Where adicional de la siguiente forma:

4. lookup_and_add('filename', 'ip.src', 5, false, 'filename CONTAINS $[DocTeamList/test] ');

La siguiente figura muestra la definición de la regla.



La siguiente figura muestra el conjunto de resultados.

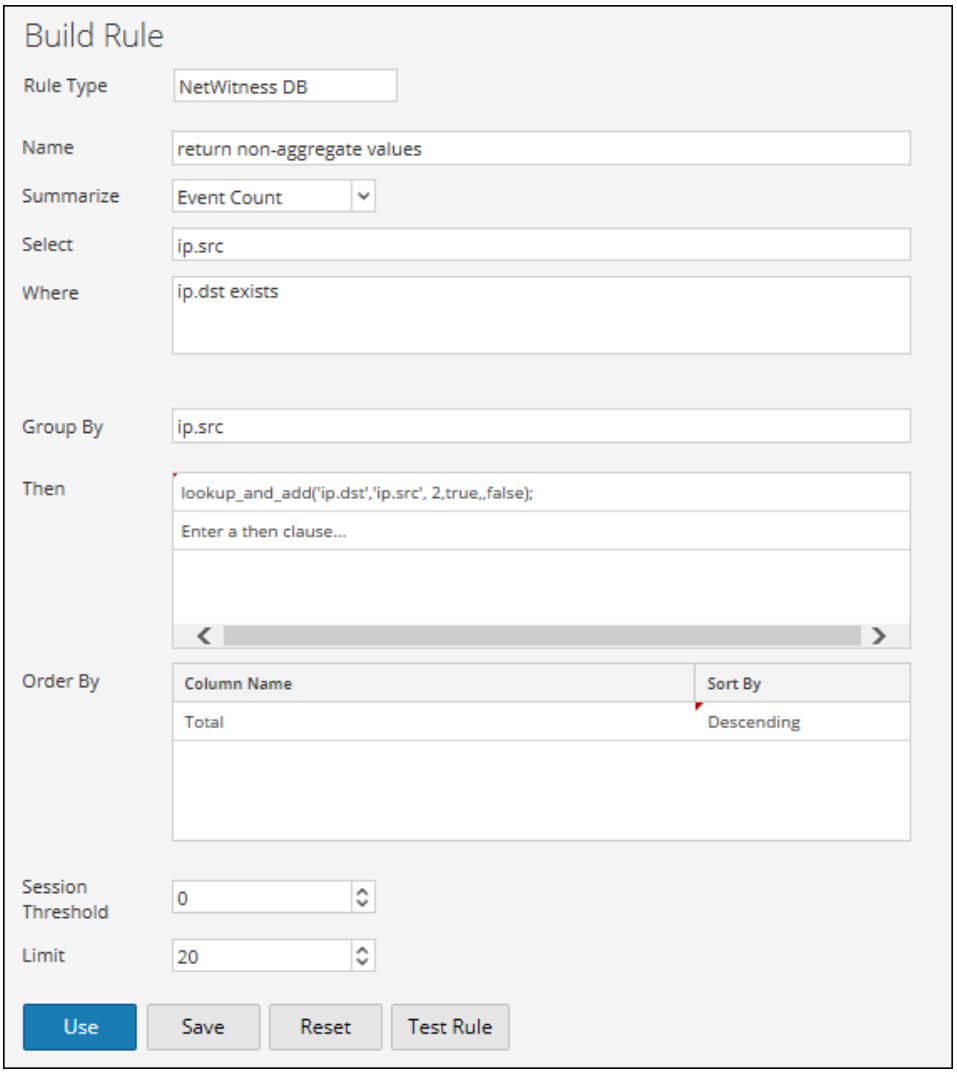


5. lookup_and_add('ip.dst','ip.src', 2,true,,false);

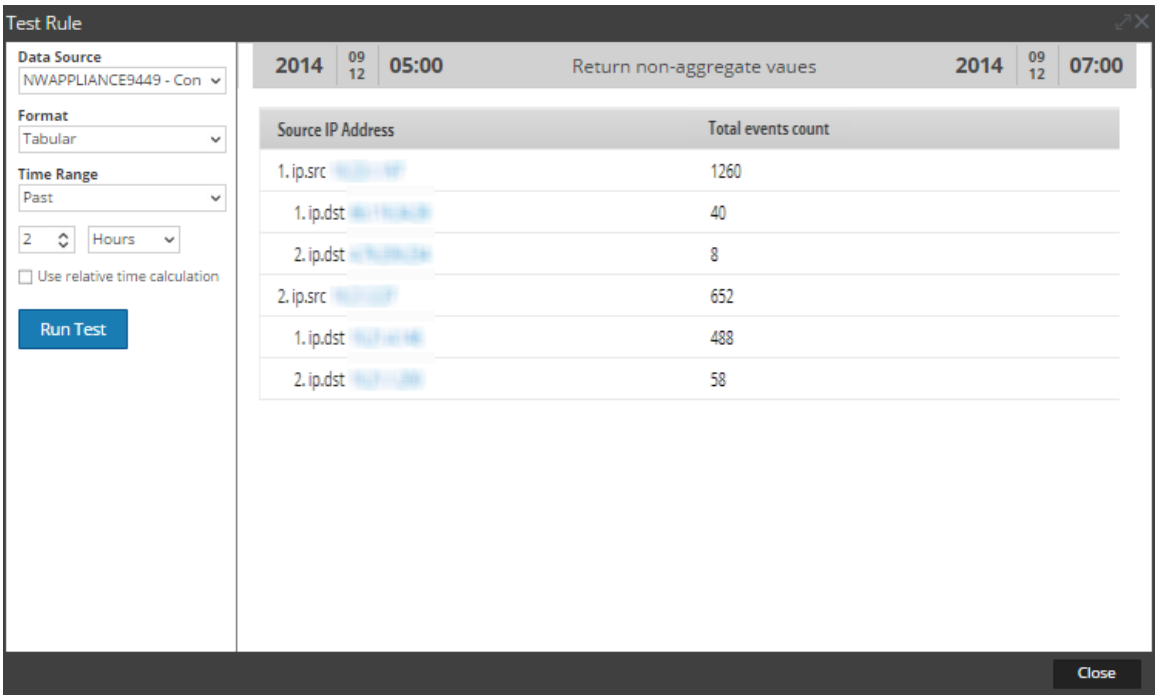
Esta acción de regla se repetirá a través de cada ip.src en el conjunto de resultados inicial y buscará las dos direcciones IP de destino principales con cada ip.src. El parámetro “aggregate” está configurado en “false”, lo cual implica que los agregados se omitirán en los valores de búsqueda y, por lo tanto, las ejecuciones de consulta de búsqueda se completarán más rápidamente.

Nota:
El valor predeterminado para “aggregate” es “true”. Cuando “aggregate” está configurado en “false”, Reporting Engine transmite threshold=1, Sort by='value' y Order=Ascending a NWDB para acelerar las consultas de búsqueda.
. Debe configurar “aggregate” en false cuando la regla contenga funciones de agregado o cuando se ejecute contra un rango de tiempo amplio. Esto ayuda a la regla a completar la ejecución con mayor rapidez.

La siguiente figura muestra la definición de la regla.



La siguiente figura muestra el conjunto de resultados.




```
max_threshold (string quantity)
```

```
max_threshold (string quantity, string field)
```

max_threshold elimina cualquier resultado con una cantidad que es mayor a la cantidad del umbral máximo de un conjunto de resultados. Se puede especificar la cantidad en términos de conteo o de tamaño y es relativa a las opciones de orden de la regla principal. Esto significa que si clasifica una regla por tamaño, la acción de la regla espera que especifique el parámetro en bytes (puede agregar KB, MB, GB o TB al parámetro para facilitar la conversión del tamaño).

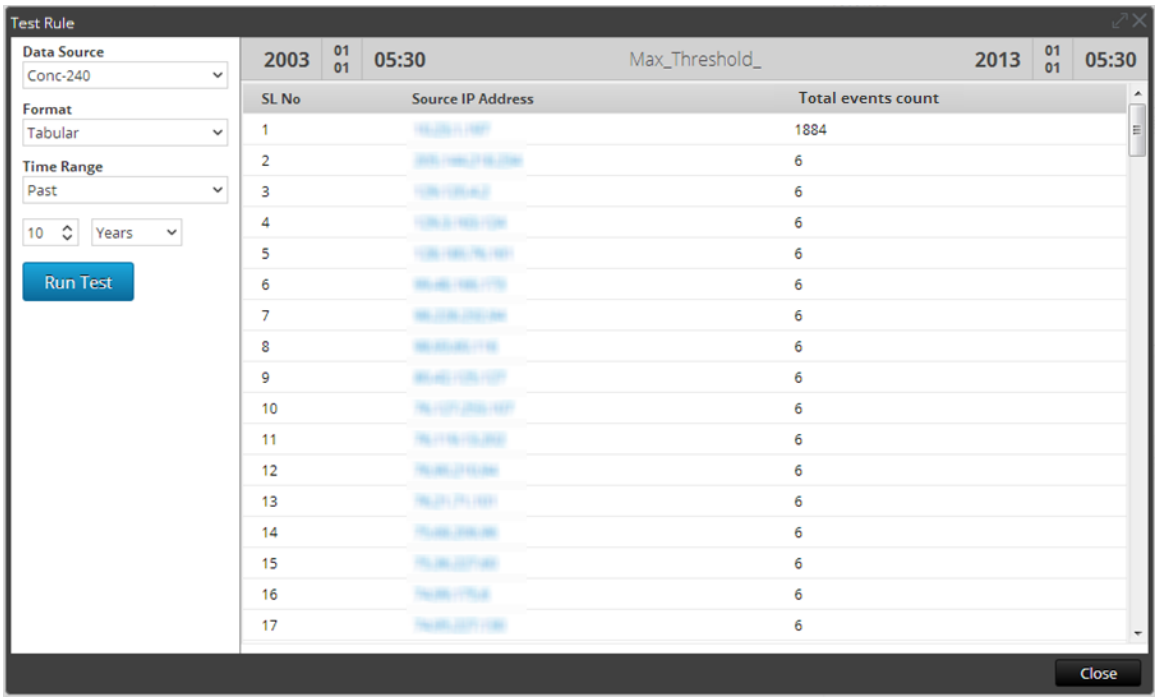
La regla max_threshold también se puede usar para filtrar valores de acuerdo con los valores de la función de agregado. Use la sintaxis según el tipo de resumen que se utiliza en la regla que se muestra a continuación:

- max_threshold(String quantity): se puede usar para filtrar Conteo de eventos, Conteo de paquetes y Tamaño de sesión.
- max_threshold(String quantity, String field): se puede usar para filtrar valores de agregados personalizados o cualquier metadato.

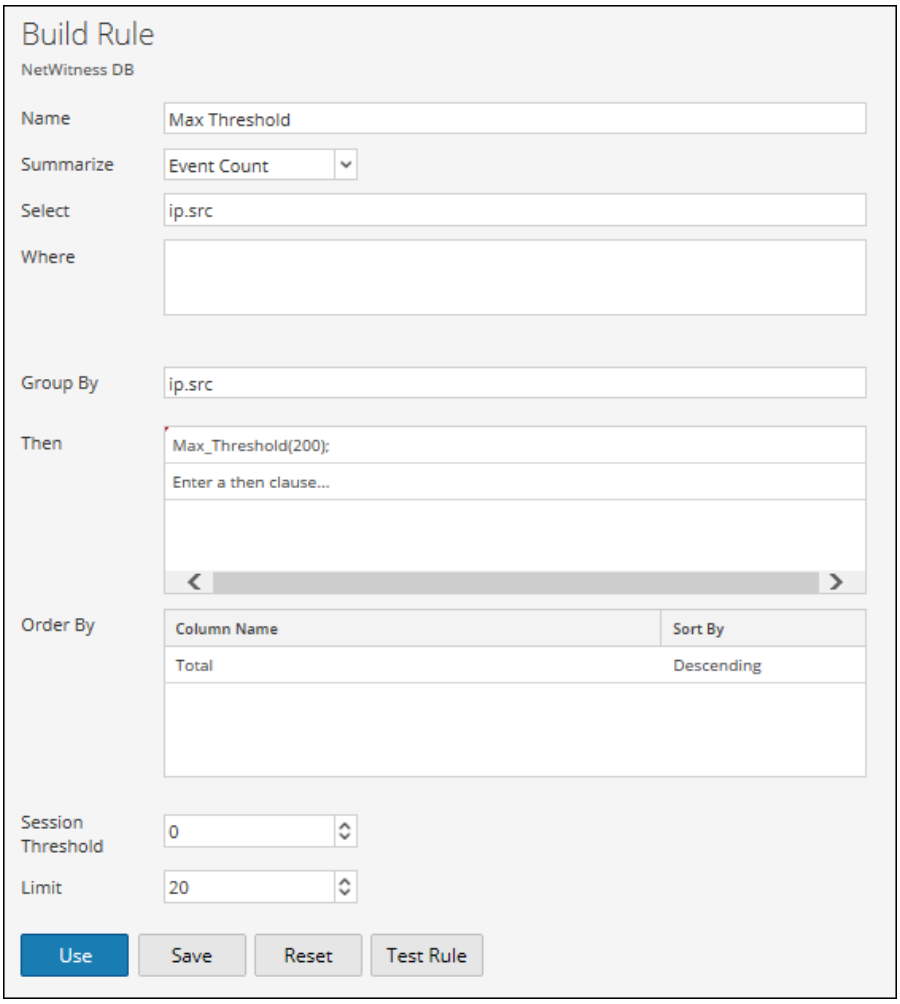
Ejemplos:

1. max_threshold(200);

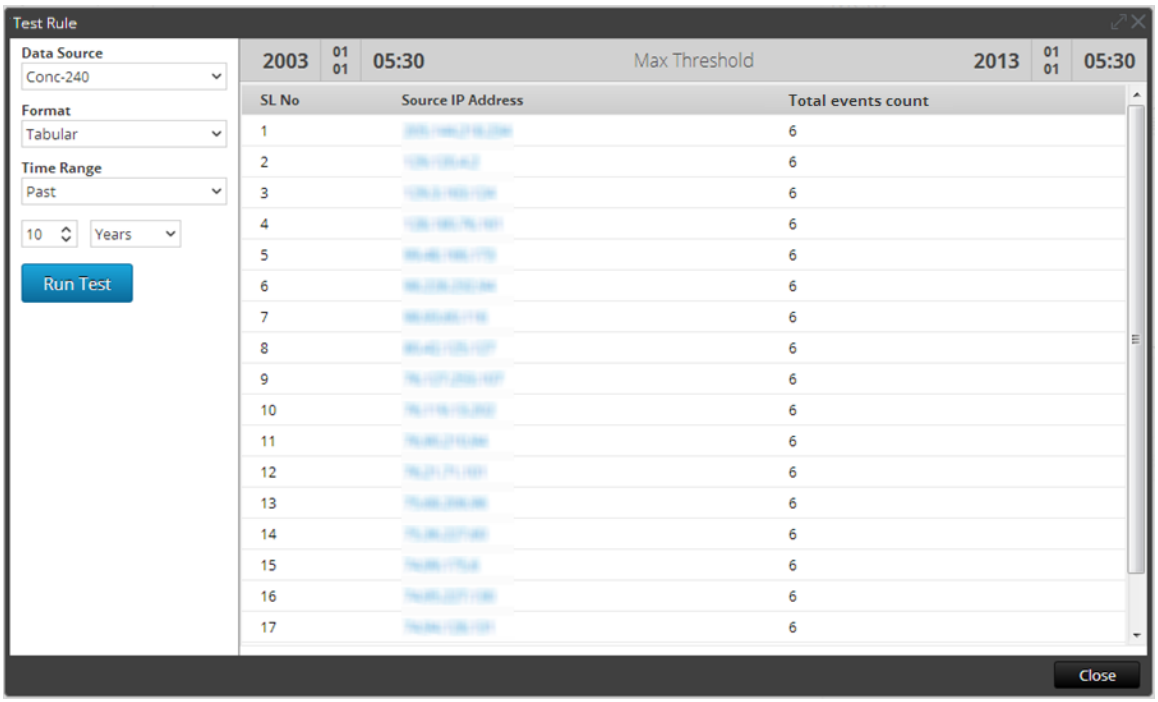
En la siguiente figura se muestra el resultado sin el argumento max_threshold. Los resultados de salida tienen conteos de eventos que exceden los 200.



En la siguiente figura se muestra la acción de regla max_threshold que pone un límite de 200 bytes en la salida. No se enumera ninguna salida que tenga más de 200 bytes de datos.

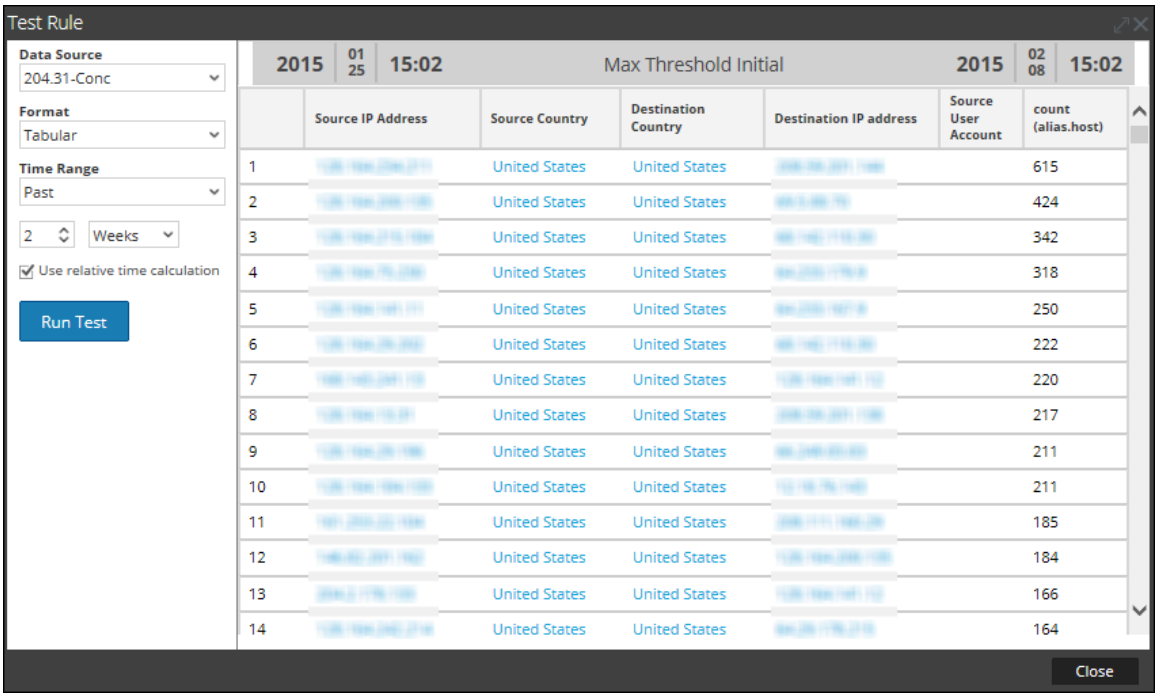


En la siguiente figura se muestra el resultado cuando se aplica la acción de regla max_threshold. Los resultados enumerados 1 en la captura de pantalla anterior se quitan del resultado.

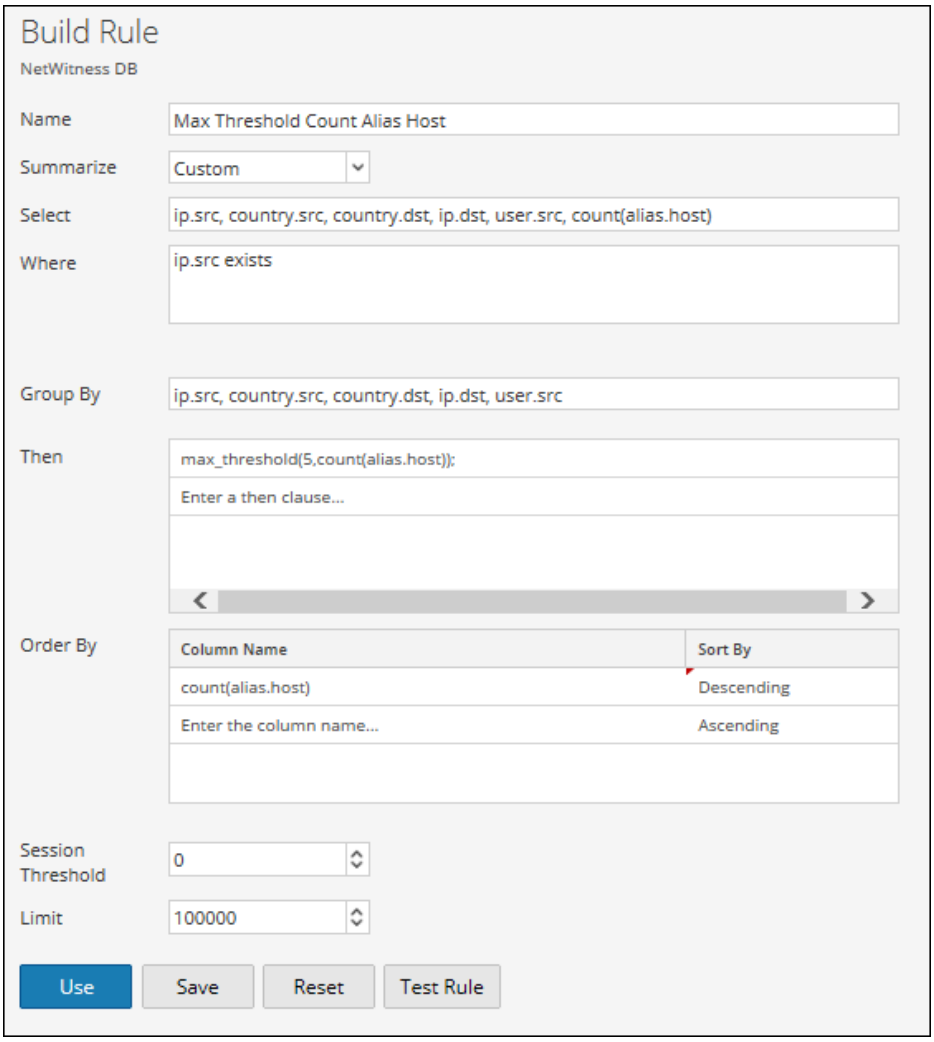


2. max_threshold(5,count(alias.host));

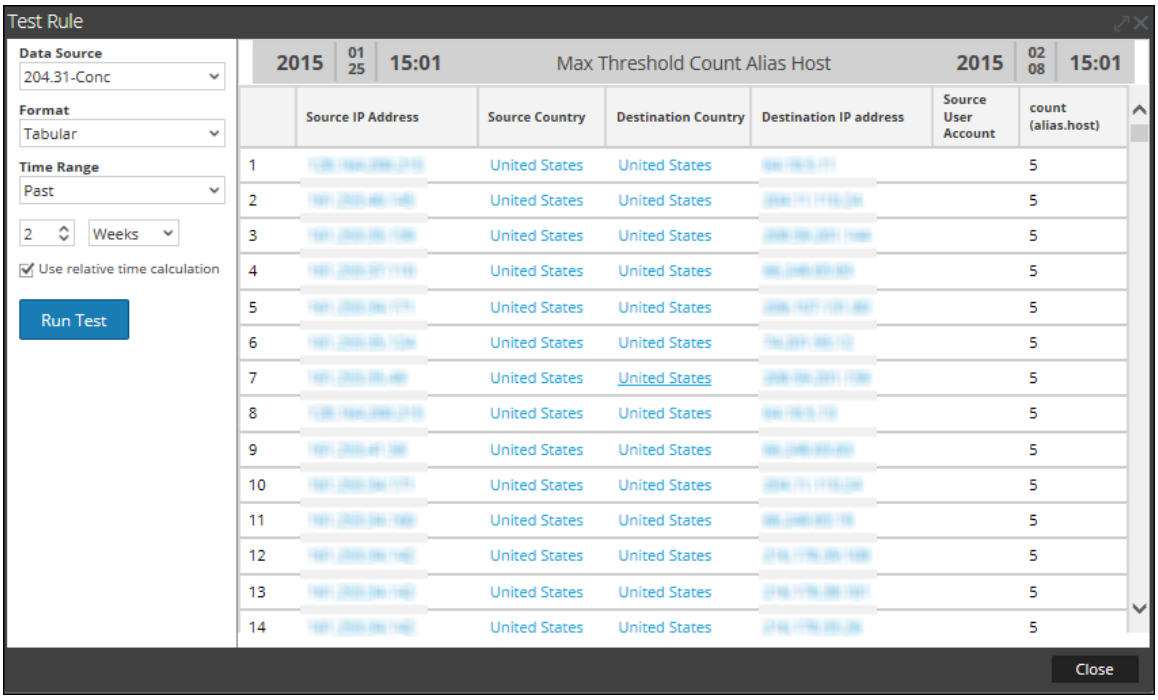
En la siguiente figura se muestra el resultado sin el argumento max_threshold. Los resultados de salida tienen un conteo de alias.host mayor de cinco.



En la siguiente figura se muestra la acción de regla max_threshold que pone un límite de cinco en la salida. No se enumera ninguna salida que tenga un valor mayor de cinco.



En la siguiente figura se muestra el resultado cuando se aplica la acción de regla max_threshold. Cualquier salida que tenga un valor mayor de cinco se elimina del resultado.



min_threshold (string quantity)

min_threshold elimina los resultados con una cantidad que es menor a la cantidad del umbral mínimo de un conjunto de resultados. Se puede especificar la cantidad en términos de conteo o de tamaño y es relativa a las opciones de orden de la regla principal. Esto significa que si clasifica una regla por tamaño, la acción de la regla espera que especifique el parámetro en bytes (puede agregar KB, MB, GB o TB al parámetro para facilitar la conversión del tamaño).

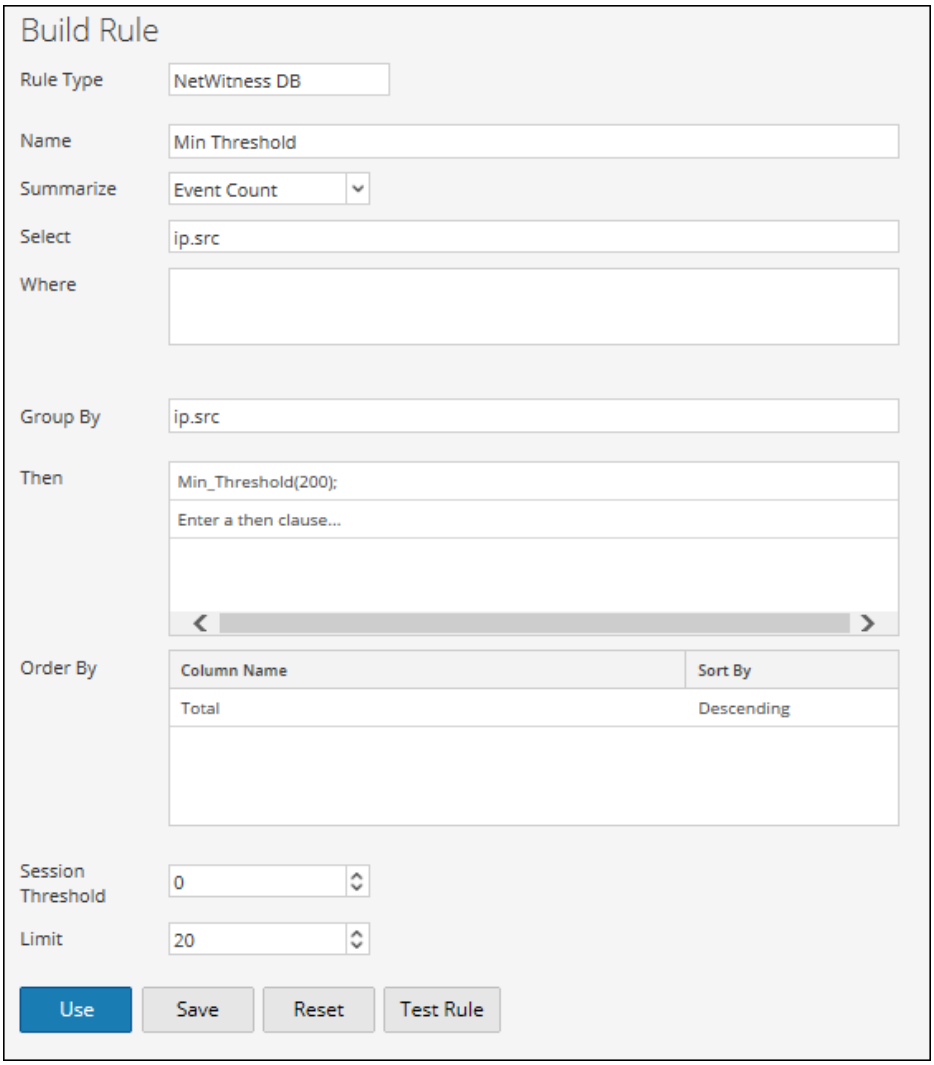
La regla min_threshold también se puede usar para filtrar valores de acuerdo con los valores de la función de agregado. Use la sintaxis según el tipo de resumen que se utiliza en la regla que se muestra a continuación:

- min_threshold(String quantity): se puede usar para filtrar Conteo de eventos, Conteo de paquetes y Tamaño de sesión.
- min_threshold(String quantity, String field): se puede usar para filtrar valores de agregados personalizados o cualquier metadato.

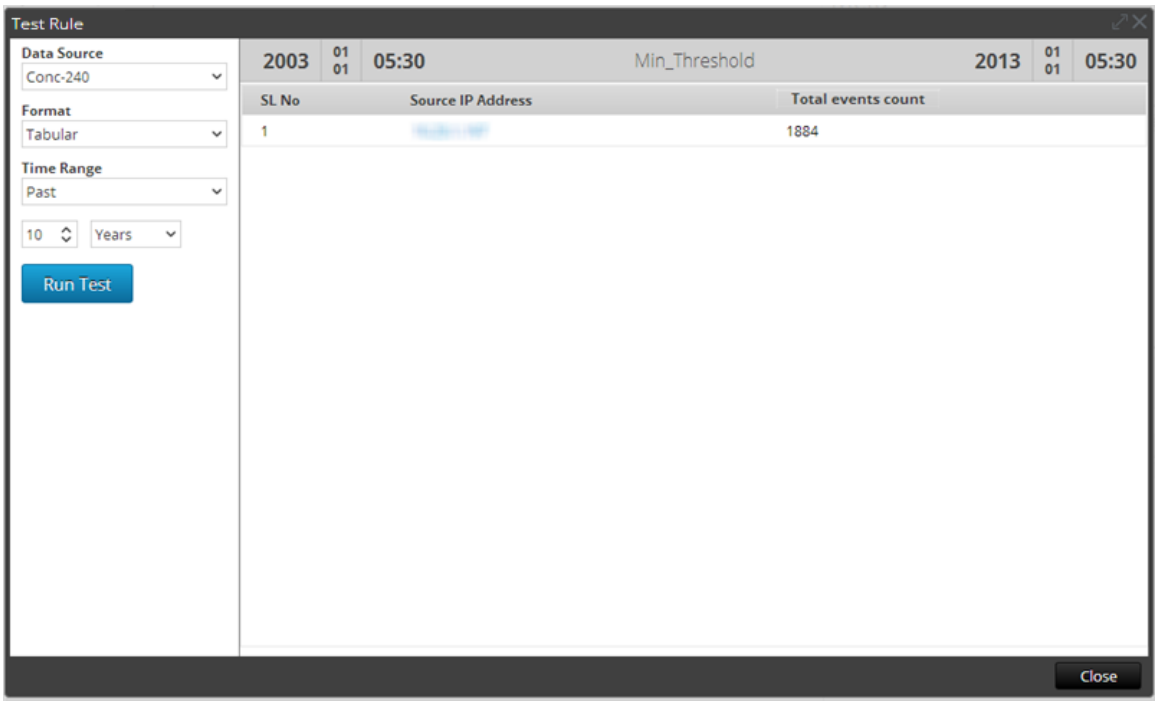
Ejemplos:

1. min_threshold(200);

En la siguiente se figura muestra un ejemplo de la consulta min_threshold.



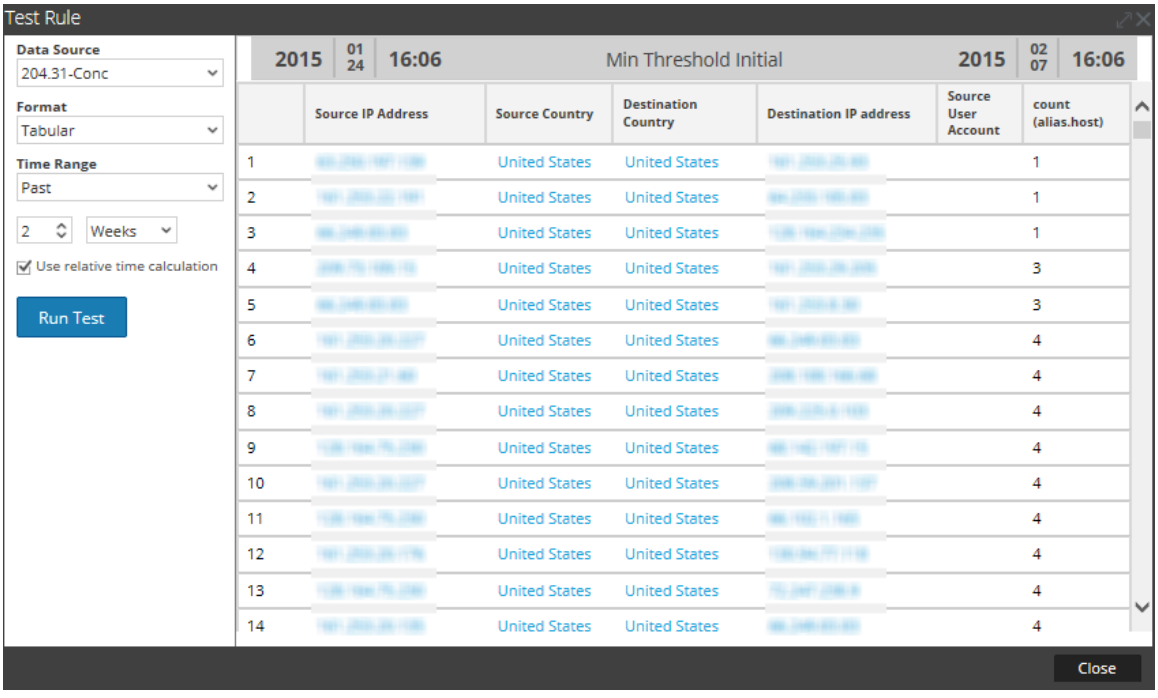
En la figura anterior se establece un límite de 200 bytes en la salida. No se enumera ninguna salida que tenga menos de 200 bytes de datos. Se aplica la salida con la acción de regla min_threshold.



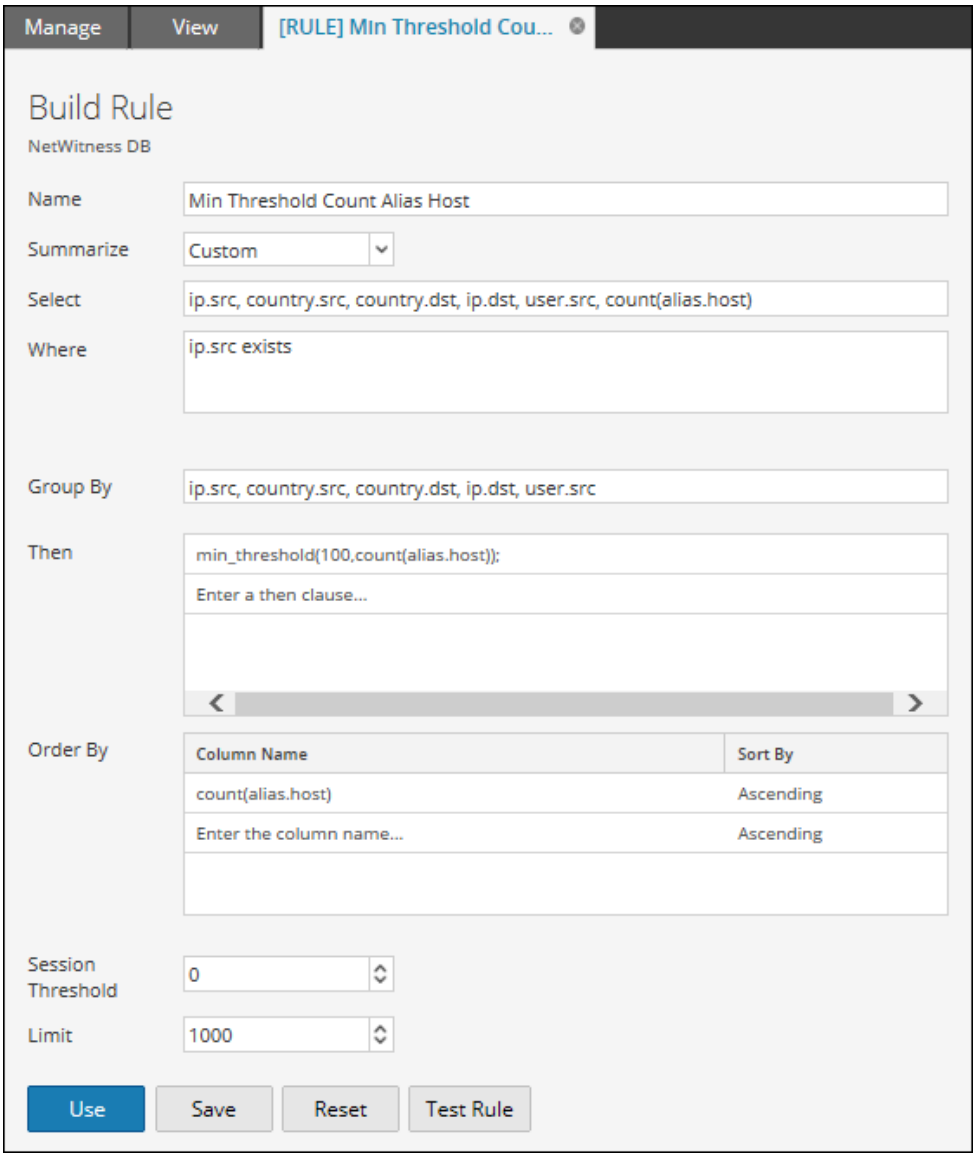
Como se muestra, todos los valores son más grandes que 200 bytes.

2. min_threshold(100,count(alias.host));

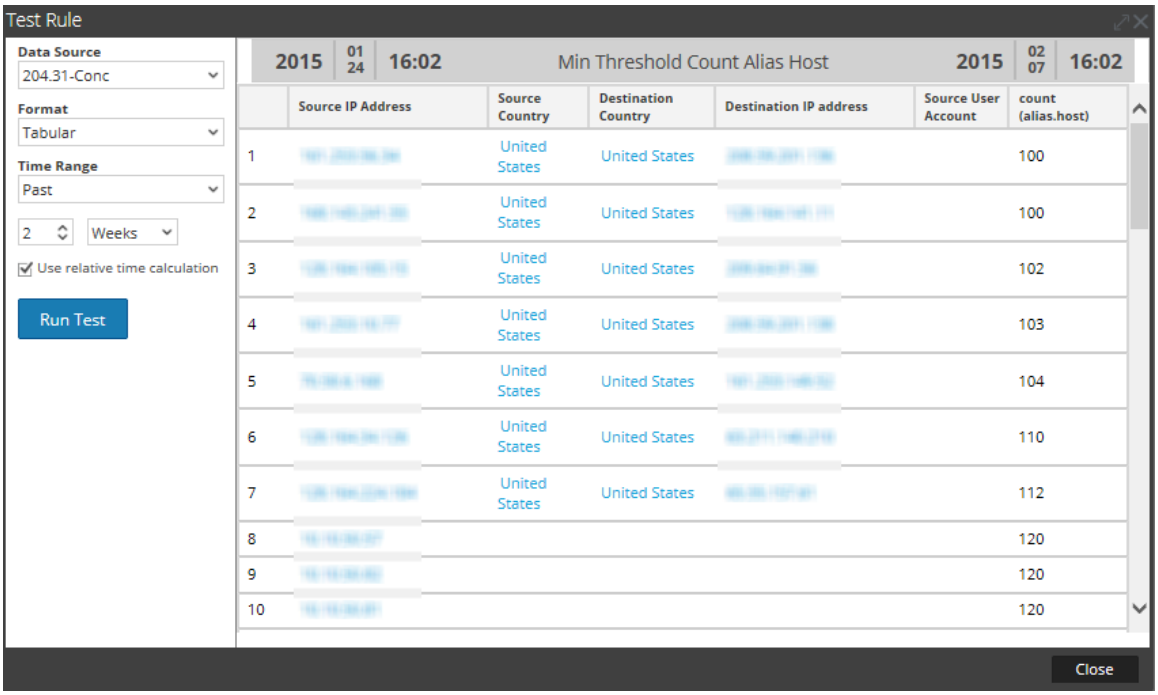
En la siguiente figura se muestra el resultado sin el argumento min_threshold. Los resultados de salida tienen un conteo de alias.host menor de 100.



En la siguiente figura se muestra la acción de regla min_threshold que establece el límite mínimo de 100 en la salida. No se lista ninguna salida que tenga datos menores de 100.



En la siguiente figura se muestra el resultado cuando se aplica la acción de regla min_threshold. Cualquier salida que tenga datos de menos de 100 se quita del resultado.



regex (string regex, string field)

La acción de regla regex aplica la expresión regular al conjunto de resultados. El siguiente es el formato de la acción de regla regex:

regex(regular_expression, meta_name)

Donde:

- regular_expression: es la expresión regular para igualar el valor de los metadatos.
- meta_name: nombre del campo o de los metadatos donde se debe aplicar regex.

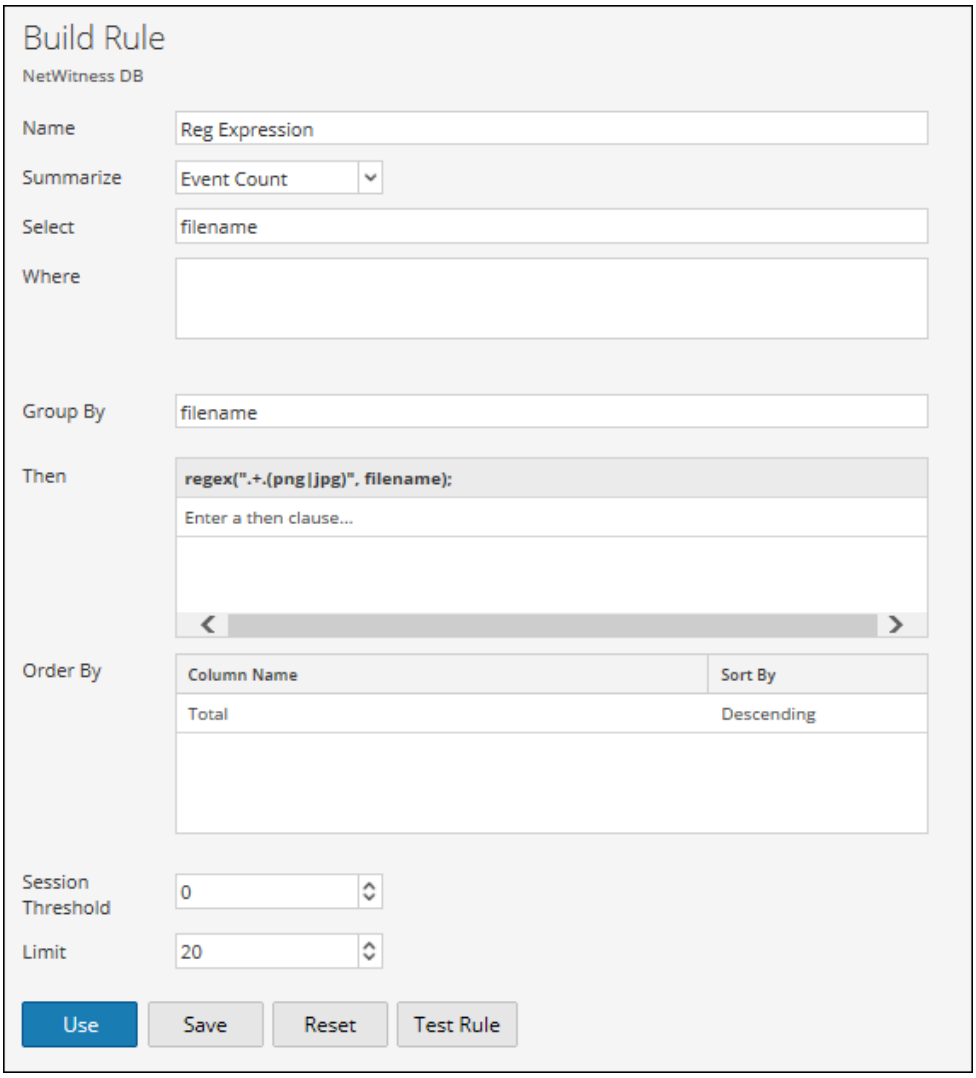
Para ver una lista completa de los patrones de regex compatibles, consulte http://docs.oracle.com/javase/7/docs/api/java/util/regex/Pattern.html.

Ejemplo de la acción de regla regex:

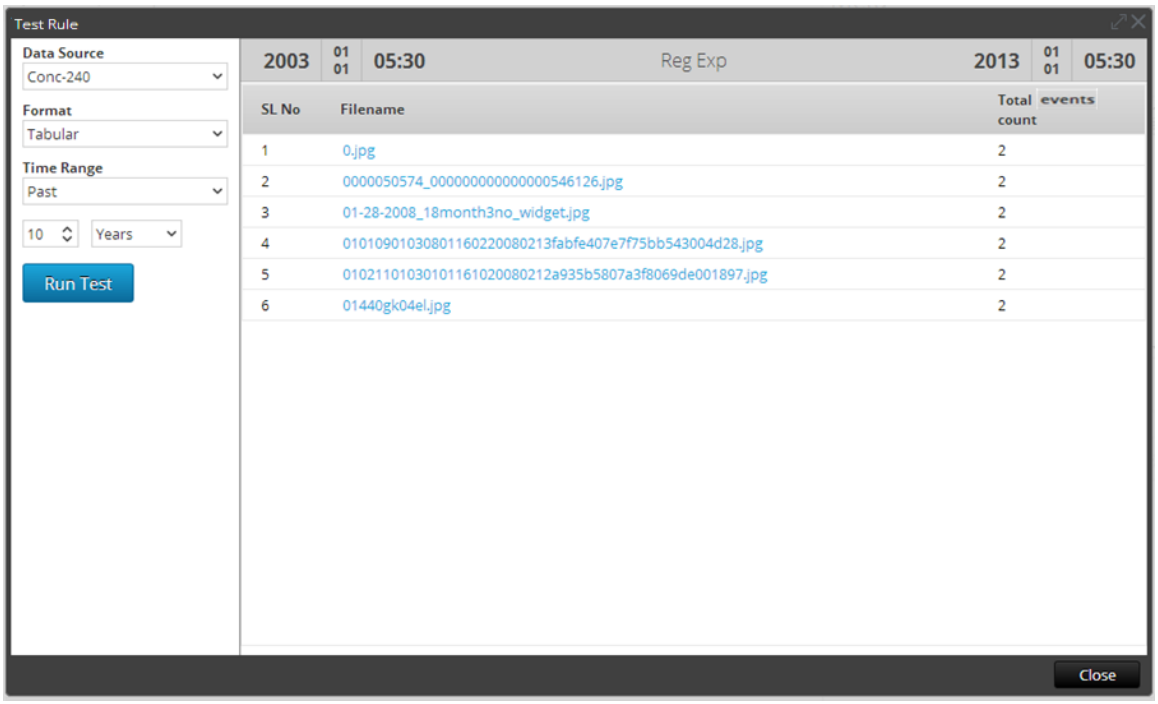
Si desea incluir nombres de archivos de todos los formatos de archivo PNG y JPEG de diferentes sesiones, puede escribir una regla con la siguiente acción de regla regex:

regex(".+.(png|jpg)", filename);

En la siguiente se figura muestra la regla.



La salida con la acción de regla regex aplicada se muestra en la siguiente figura:

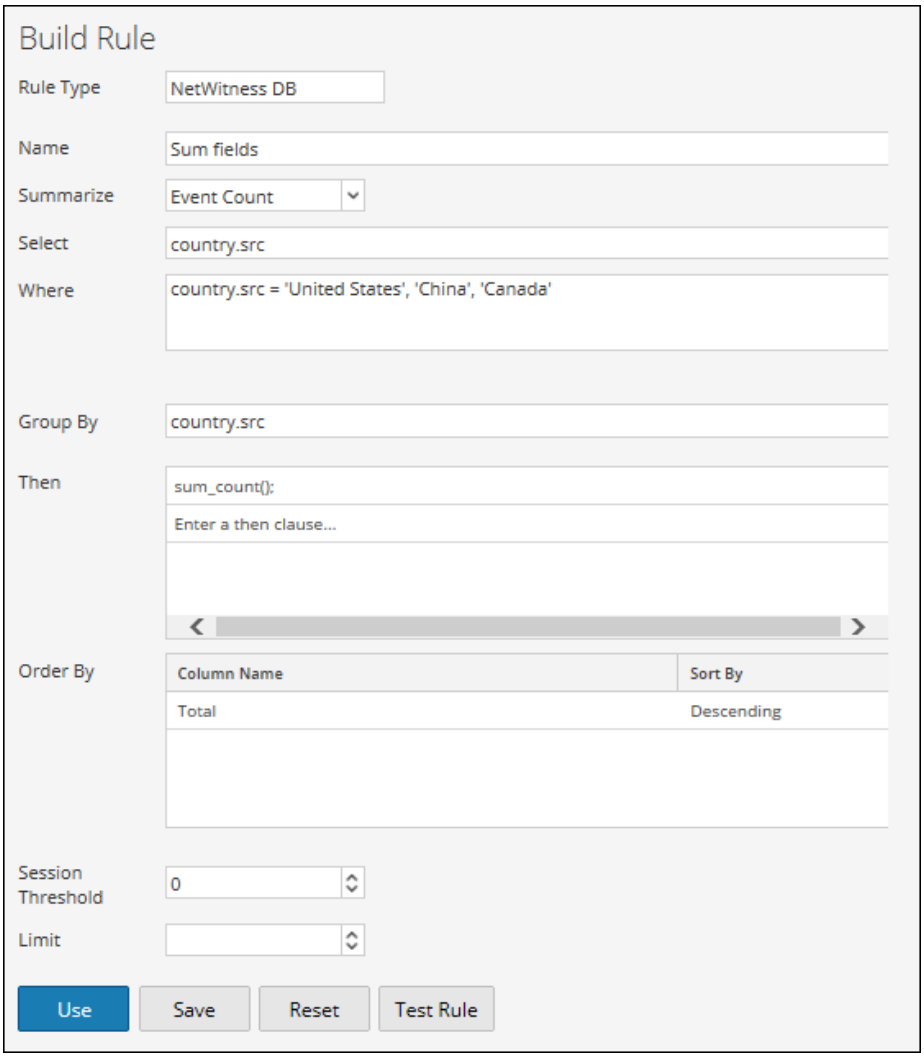


`sum_count()`

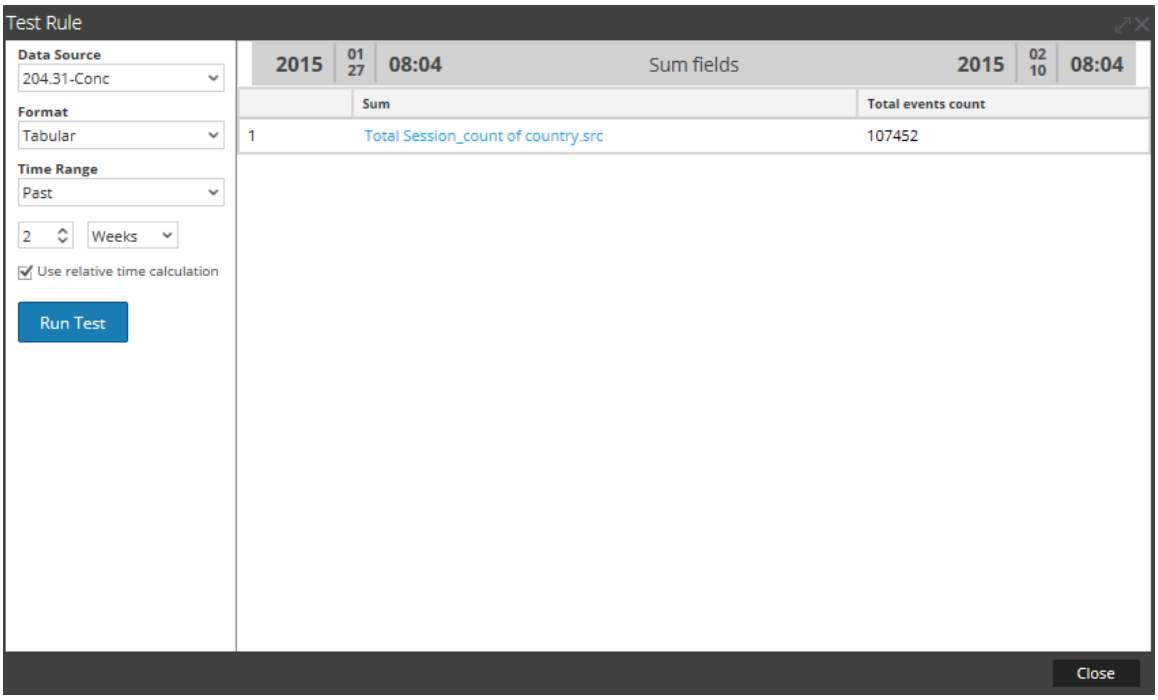
Calcula el total de los cuantificadores de un conjunto de resultados específico. Por ejemplo, al llamar un sum_count() para una regla que está clasificada por conteos de eventos, se calcula el tamaño total de todos los valores en el conjunto de resultados y se muestra el total implementado del conjunto de resultados.

Ejemplo:

En la siguiente se figura muestra la regla de acción sum_count().



Con la regla de acción sum_count(), la salida muestra el tamaño total de todos los conteos de eventos:

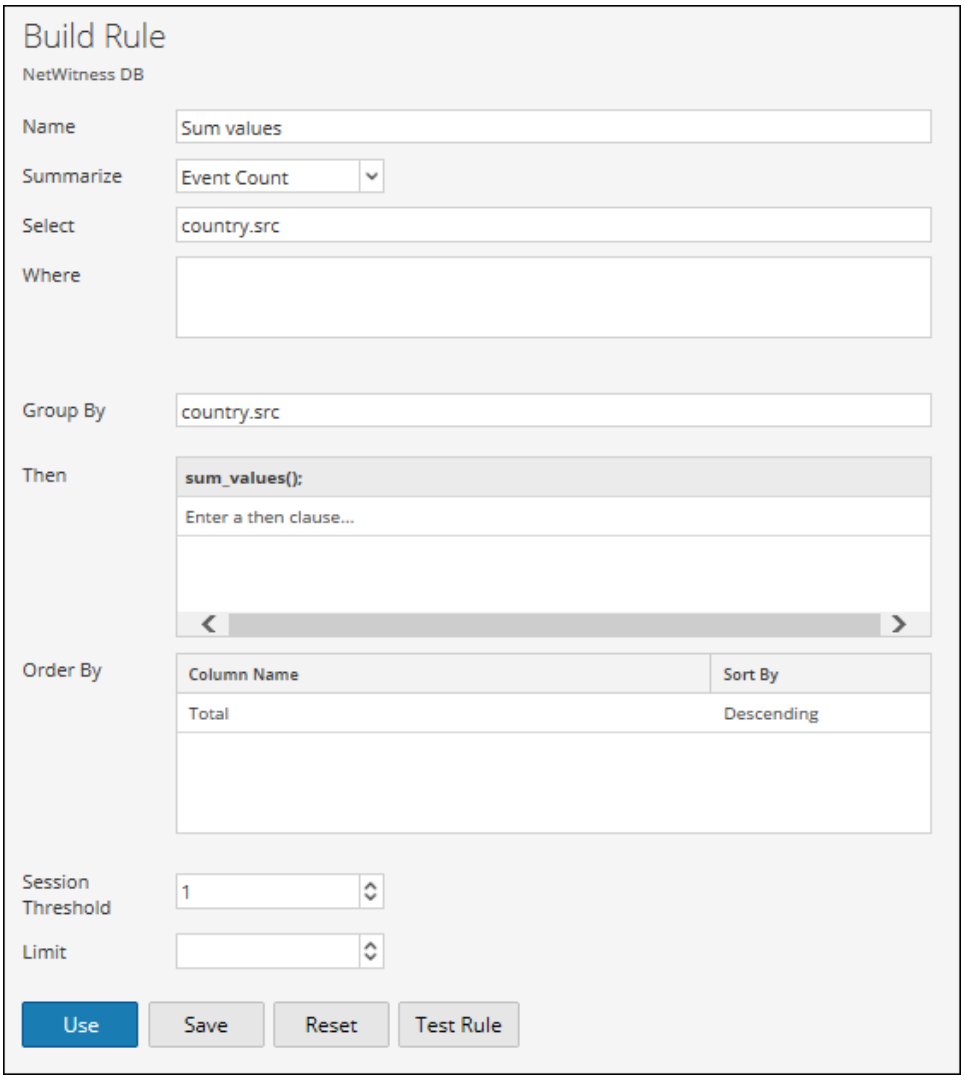


`sum_values()`

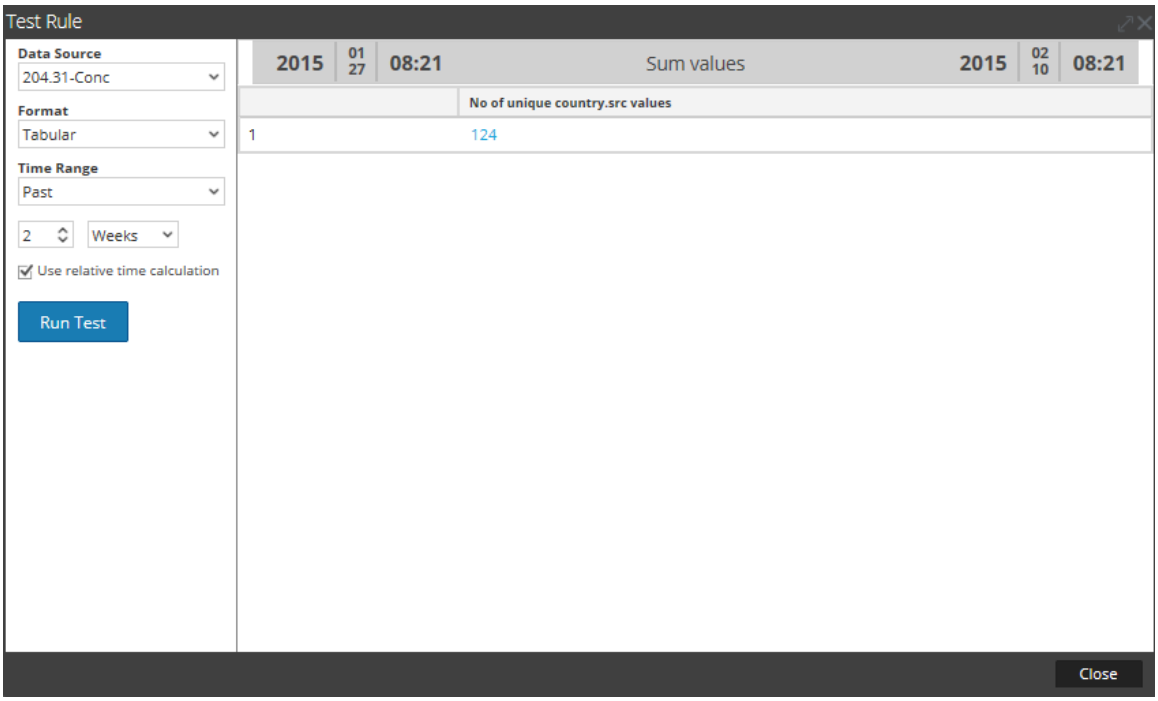
Calcula la cantidad total de valores de un conjunto de resultados específico. Use esta acción para mostrar la cantidad de coincidencias que se encontraron para una regla determinada.

Ejemplo:

En la siguiente figura se muestra la acción de regla sum_values().



En la siguiente figura se muestra el resultado con la acción de regla sum_value:



show_whats_new()

La acción de regla show_whats_new() toma cualquier resultado de un conjunto de resultados y filtra cualquier valor disponible en la base de datos de metadatos de NetWitness antes del marco de tiempo del informe en ejecución. Cuando se ejecuta un informe, Security Analytics determina el ID de la primera sesión en el rango de tiempo del informe. Si un valor en un conjunto de resultados tiene un ID de primera sesión mayor al ID de primera sesión del marco de tiempo del informe, no existía en la base de datos de metadatos de NetWitness antes de que el informe se ejecutara y, por lo tanto, es nueva para el sistema NetWitness relacionado con el marco de tiempo del informe.

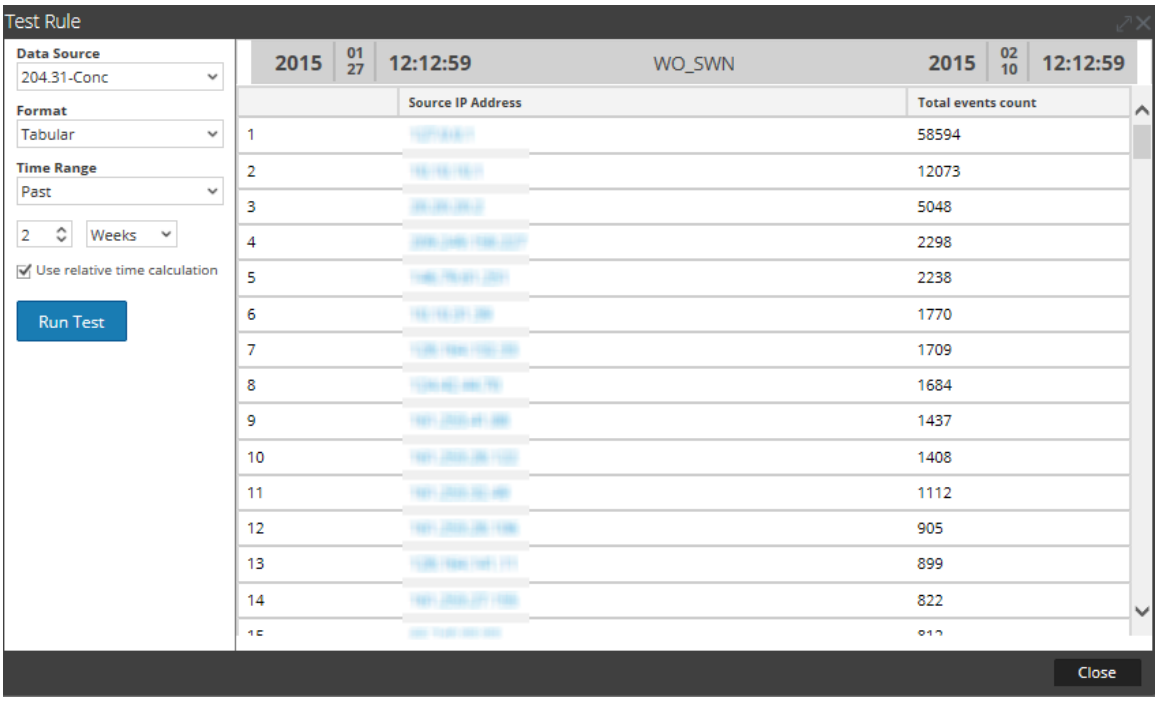
La acción de regla show_whats_new() también es compatible con la regla agregada personalizada. Cuando se seleccionan múltiples metadatos en la regla Personalizada, se consideran los primeros para filtrar los valores antiguos. Consulte el ejemplo 2 más adelante para comprender cómo se usa esta acción de regla para la regla agregada personalizada.

Nota: La acción de regla show_whats_new() se puede usar solo con una regla agregada.

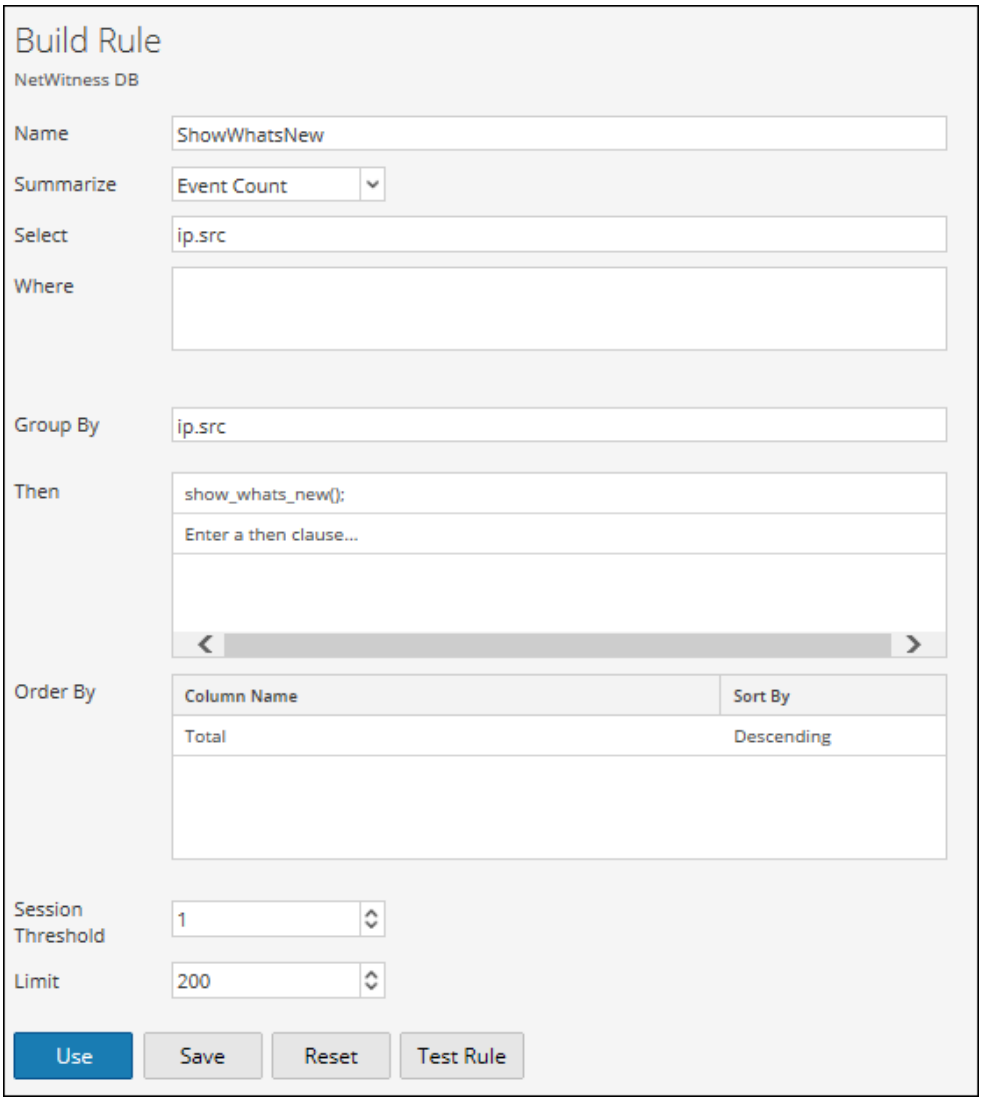
Ejemplos:

1. show_whats_new() para una regla agregada con Conteo de eventos

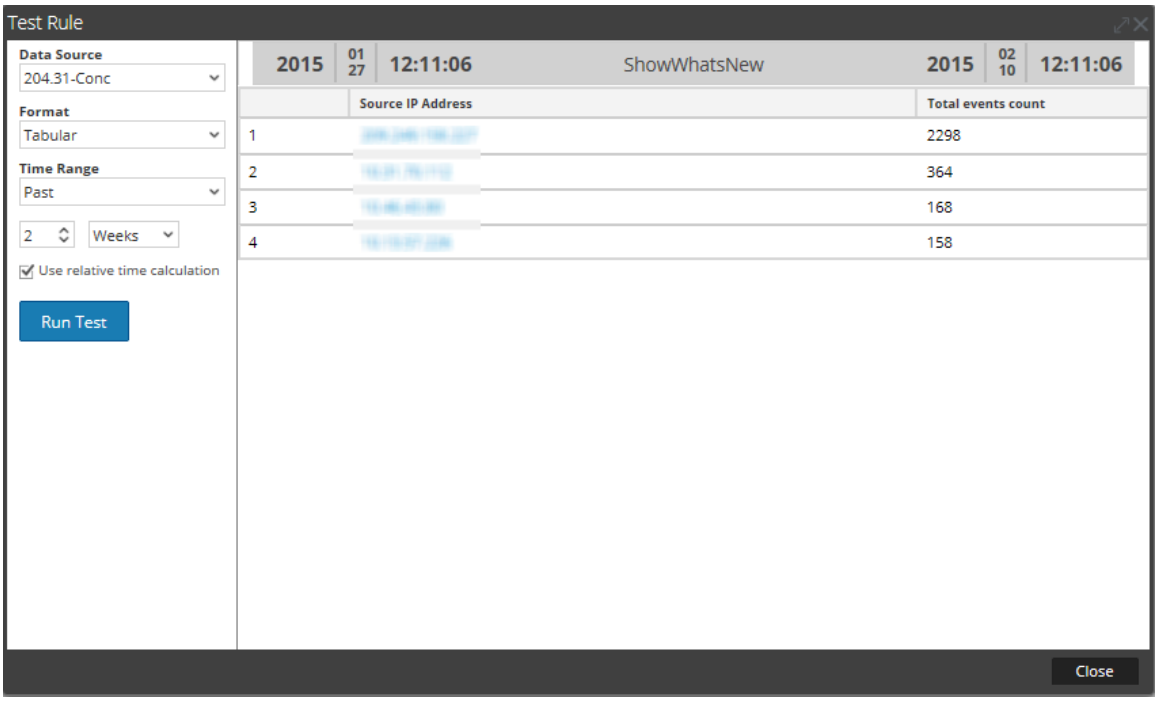
En el siguiente ejemplo se enumeran todas las direcciones IP de origen disponibles durante las últimas dos semanas.



En la siguiente figura se muestra el uso de la acción de regla show_whats_new para mostrar solo las entradas nuevas en las últimas dos semanas.

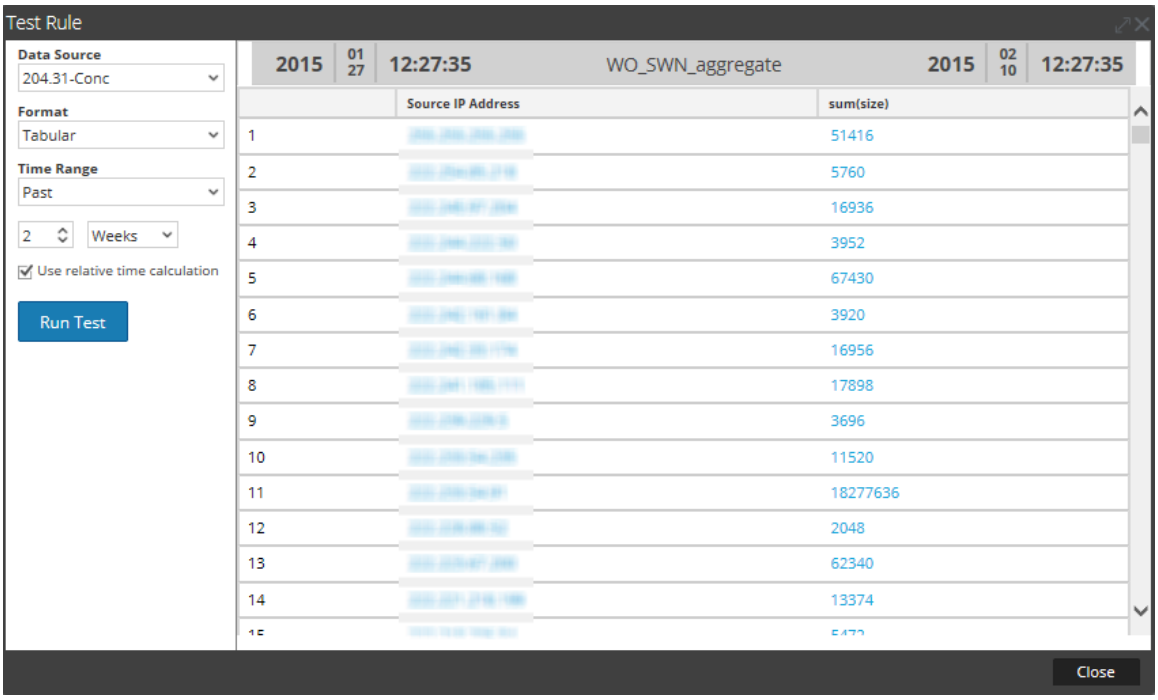


En la siguiente figura se muestran las entradas nuevas en las últimas dos semanas.

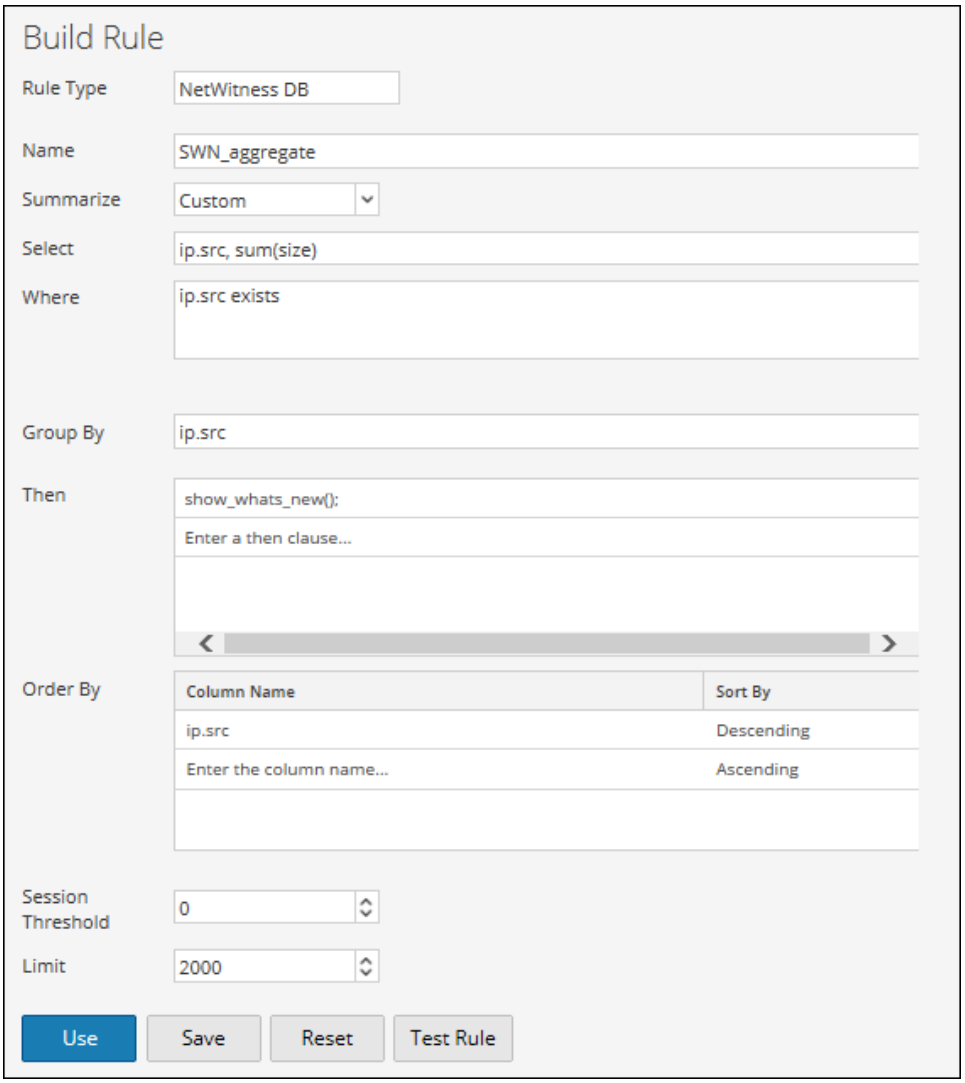


2. show_whats_new() para una regla agregada personalizada

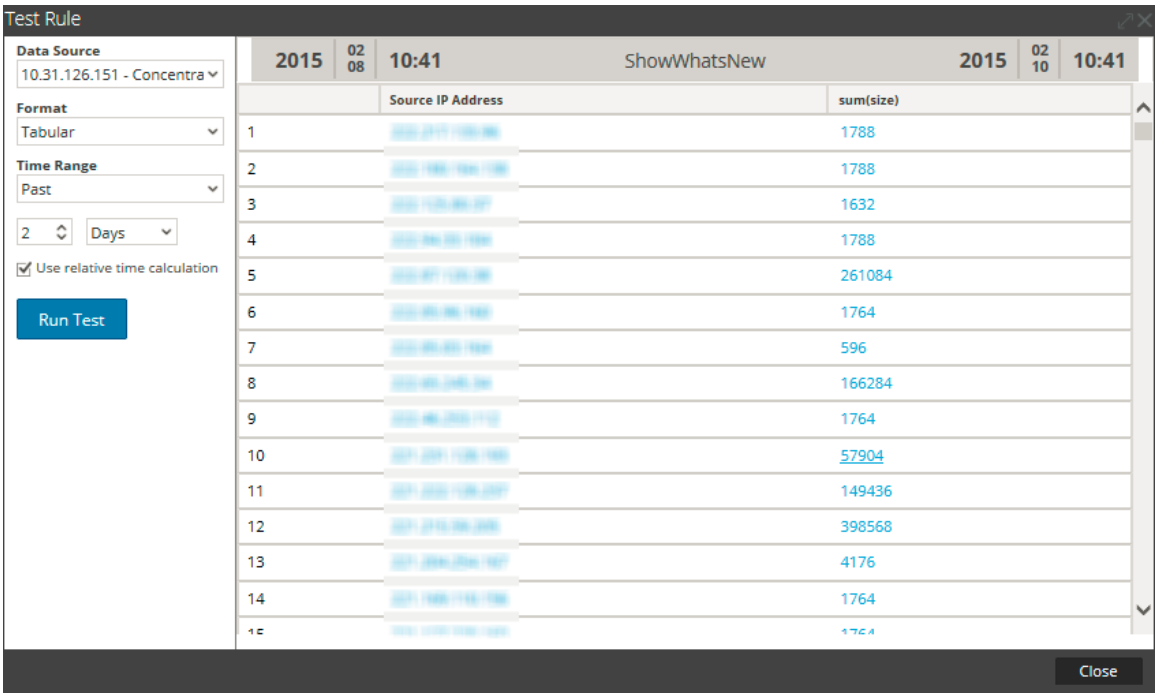
En el siguiente ejemplo se enumeran todas las direcciones IP de origen disponibles durante las últimas dos semanas.



En la siguiente figura se muestra el uso de la acción de regla show_whats_new para mostrar solo las entradas nuevas en las últimas dos semanas.



En la siguiente figura se muestran las entradas nuevas de direcciones IP de origen en las últimas dos semanas.



El poder de esta función es que no importa cuándo se ejecuta el informe en los valores identificados que son nuevos para NetWitness. Preste atención con esta función porque si se restablecen los datos, se perderán. Sin embargo, es fácil establecer un punto de base en un sistema e identificar cambios y nuevos elementos sin una gran cantidad de esfuerzo en el sistema (según el tamaño del conjunto de resultados).

Operadores de reglas compatibles

La sintaxis de regla de origen de datos del Reporting Engine de NWDB es compatible con un subconjunto de operadores de reglas que son compatibles con Security Analytics.

Sintaxis	Descripción
*	Use un asterisco (*) como el único operador de una regla para seleccionar todo el tráfico.
=	Es igual al operador
!=	No es igual al operador
&&	Operador Y lógico
||	Operador O lógico

Sintaxis	Descripción
-u	Límite superior. Por ejemplo, **tcp.port = 40000-u** selecciona todos los puertos TCP superiores a 40,000.
-l	Límite inferior. Por ejemplo, **tcp.port = I-40000** selecciona todos los puertos TCP inferiores a 40,000.
-	El operador guion (-) solo se aplica a valores numéricos. Separe los límites inferiores y superiores del rango con un guion (-). Por ejemplo, **tcp.port = 25-443** selecciona todos los puertos TCP entre 25 y 443.

Tipos de regla

En este tema se describen los diversos tipos de regla del módulo Reporting. Los tipos de regla designan el origen de datos de la regla de informes. Estos son los tipos de regla:

Tipo de regla	Descripción
Base de datos de NetWitness	La base de datos de NetWitness extrae los metadatos de un Reporting Engine configurado para el uso de un Concentrator, un Broker y un Archiver como orígenes de datos, y proporciona los metadatos para las reglas.
Base de datos de protocolo de Internet (**IPDB**)	La base de datos de protocolo de Internet (IPDB) proporciona mensajes de eventos crudos y normalizados que pueden abarcar periodos de tiempo históricos importantes. Debe configurar el servicio IPDB Extractor y asociarlo con un Reporting Engine, según lo descrito en la lista de verificación de la configuración de Reporting Engine. Hay diferentes implementaciones de IPBD, que incluyen la implementación de IPBD en múltiples sitios. También se puede implementar IPDB Extractor en ambientes virtuales. Para obtener más información, consulte Implementaciones del servicio IPDB Extractor compatibles en ambientes virtuales.

Tipo de regla	Descripción
Base de datos de Warehouse	La base de datos de Warehouse, conocida también como RSA Analytics Warehouse, contiene grandes cantidades de datos. Warehouse está diseñado para que pueda recuperar grandes volúmenes de datos con facilidad y eficiencia. Warehouse también extrae los metadatos del Reporting Engine.

Temas

Implementaciones del servicio IPDB Extractor compatibles en ambientes virtuales

Implementaciones del servicio IPDB Extractor compatibles en ambientes virtuales

En este tema se describen las implementaciones de IPDB Extractor compatibles en ambientes virtuales. Security Analytics es compatible con la implementación del servicio Internet Protocol Database (IPDB) Extractor en ambientes virtuales. En la siguiente tabla se incluyen las especificaciones de implementación virtual que RSA recomienda para el servicio IPDB Extractor. Tenga en cuenta que estas recomendaciones están basadas en pruebas realizadas por RSA.

Elemento	Especificación
Procesador	4 CPU virtuales
Memoria	8 GB RAM
HDD	320 GB

Plataformas de VMware compatibles

Plataformas	Versiones
VMware ESX Server	5.0
VMware vSphere Client	5.0

Implementación virtual del servicio IPDB Extractor

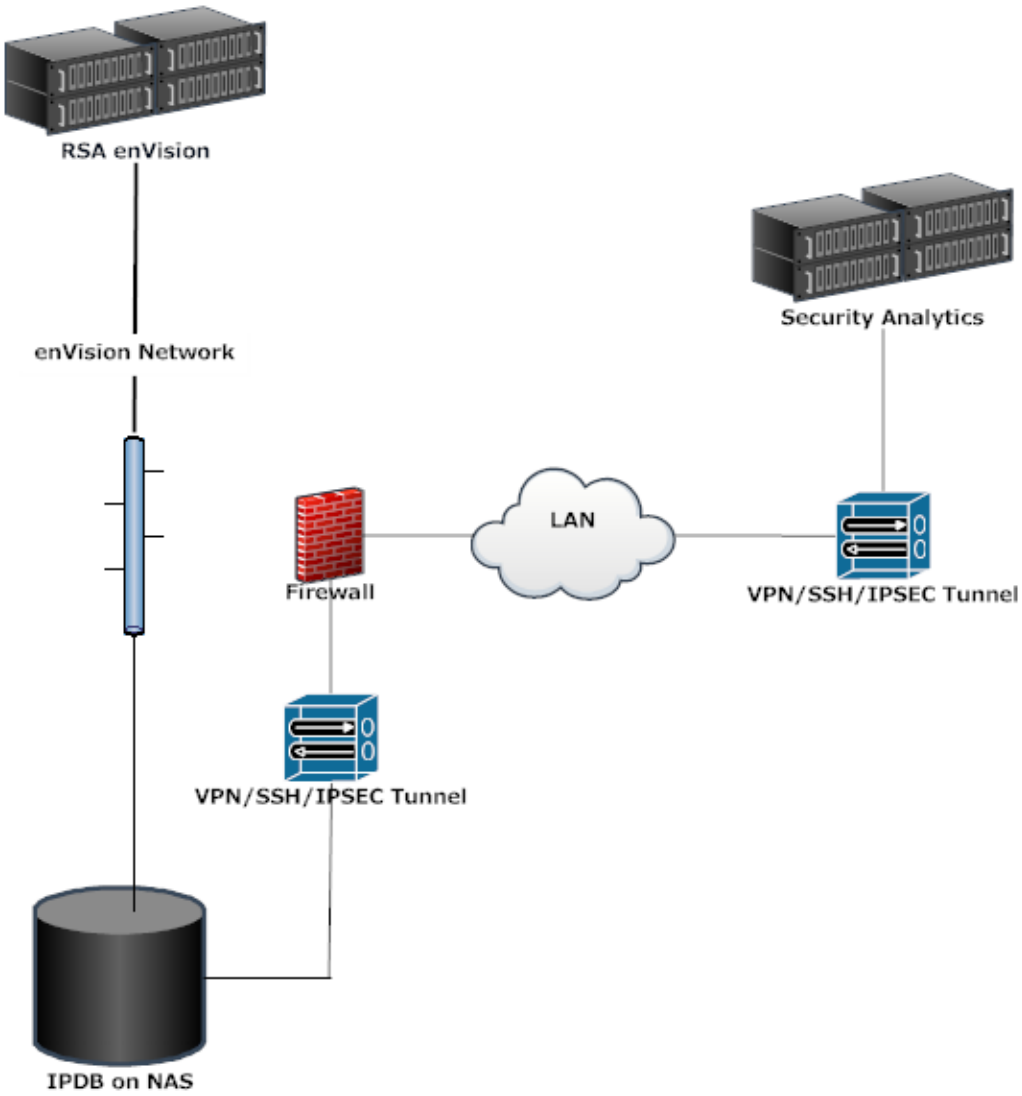
En la siguiente tabla se indica la implementación de IPDB Extractor Service Virtual para las diferentes implementaciones de IPDB.

Implementación de IPDB	Conexión al servicio IPDB Extractor en VM	Modos de conexión segura
IPDB en NAS	A través de LAN	SSH/VPN/IPSEC
A través de switch privado	Switch físico	
A través de switch distribuido virtual	Switch virtual	
IPDB en host de hardware de sitio único	Mediante el montaje CIFS	SSH/VPN/IPSEC
IPDB en host virtual desitio único	Mediante el montaje CIFS	SSH/VPN/IPSEC

Nota: En el caso de IPDB en un host virtual de sitio único, se da por hecho que el servicio IPDB Extractor está instalado en el mismo ESX Server que el sitio único.

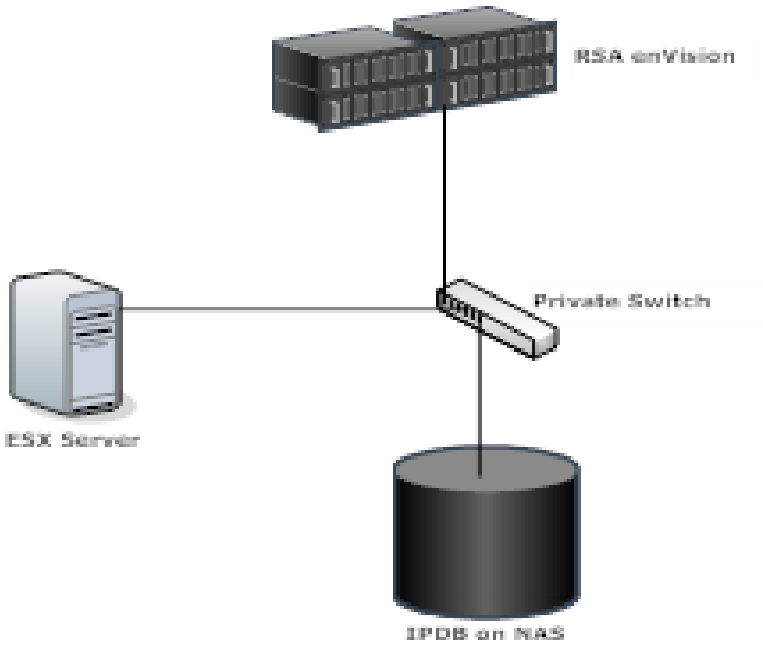
IPDB en NAS mediante LAN

Si implementa el IPDB que reside en el almacenamiento conectado en red (NAS) a través de una red de área local (LAN), debe establecer el túnel VPN/SSH/IPSEC entre el NAS y el host de servicio IPDB Extractor. Puede alojar el servicio IPDB Extractor en un host de Security Analytics, un host R710 o una máquina virtual.



IPDB en NAS a través de un switch privado

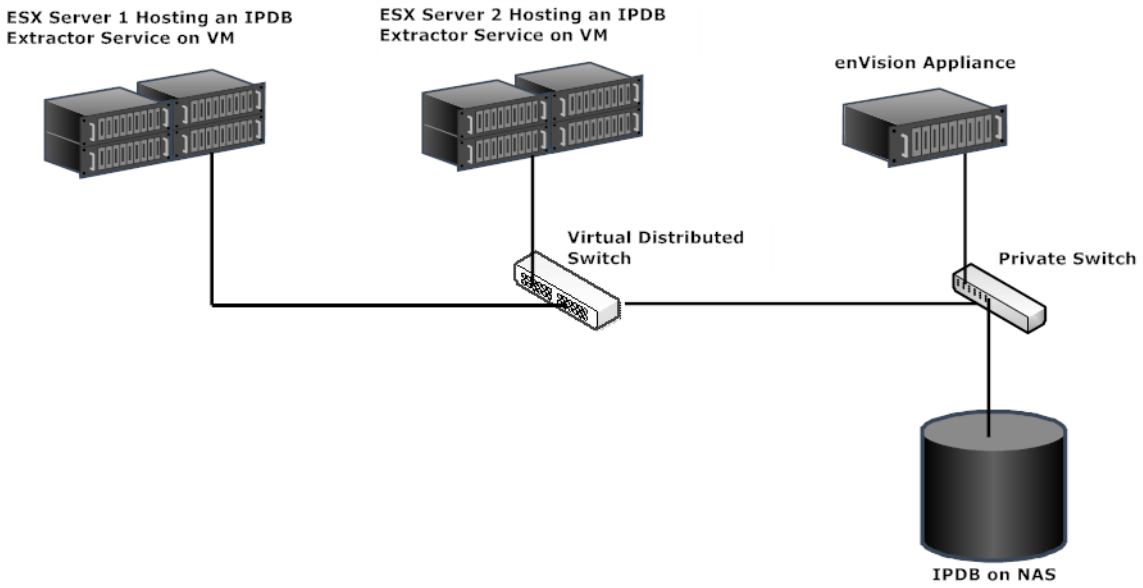
En la siguiente implementación, el servicio IPDB Extractor se aloja en una máquina virtual (VM). Debe conectar ESX Server mediante el uso del mismo switch que utiliza para conectar un host enVision a NAS.



IPDB en NAS a través de un switch distribuido virtual

En la siguiente implementación hay múltiples servicios de IPDB Extractor alojados en varias máquinas virtuales; debe conectar los servidores ESX Server con un switch distribuido virtual. En esta implementación:

- Un servicio de extractor de IPDB alojado en una máquina virtual tiene una tarjeta NIC/puerto Ethernet dedicados en el ESX Server que se ejecuta la máquina virtual.
- Ninguna otra máquina virtual en ese ESX comparte este puerto Ethernet.
- Cada puerto Ethernet está conectado a un switch virtual distribuido que a su vez está conectado al switch privado de NAS (IPDB reside en NAS).
- Aparte de la máquina virtual que aloja el servicio de extractor de IPDB, ninguna otra máquina virtual comparte la misma red, de modo que puede no obtener acceso a los datos de NAS.



Definir reglas y grupos de reglas

Este tema es un conjunto de tareas para configurar grupos de informes e informes. Puede definir, eliminar, editar, importar y exportar grupos y listas de informes en Security Analytics. Cada tema describe los procedimientos pertinentes.

Temas:

- Agregar un grupo de reglas
- Definir una regla
- Probar una regla
- Ajustar reglas de IPDB
- Usar alias de metadatos para Reporting Engine

Agregar un grupo de reglas

En este tema se proporcionan instrucciones para definir un grupo de reglas o un subgrupo de reglas.

Requisitos previos

Asegúrese de comprender los componentes de la vista Regla. Para obtener más información, consulte Vista Regla.

Procedimiento

Realice los siguientes pasos para agregar grupos de reglas o subgrupos de reglas.

Para agregar un grupo de reglas o subgrupo de reglas:

1. En el menú de Security Analytics, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Realice una de las siguientes acciones:
   - Para definir un grupo de reglas:
     a. En el panel Grupos de reglas, haga clic en  .
        Se agrega un nuevo grupo de reglas al panel Grupos de reglas.
     b. Escriba el nombre del grupo de reglas y presione INTRO.
   - Para agregar un subgrupo de reglas:
     a. En el panel Grupos de reglas, seleccione el grupo de reglas para el que desea agregar un subgrupo.
     b. Haga clic en  .
        Se agrega un nuevo subgrupo de reglas al grupo de reglas.
     c. Escriba el nombre del subgrupo de reglas y presione INTRO.

Definir una regla

En este tema se describen los tipos de reglas que puede definir o agregar mediante distintos orígenes de datos. Las reglas se pueden definir para obtener datos o eventos desde un origen de datos de NetWitness, IPDB o Warehouse. Según sus requisitos, puede seleccionar cualquiera de las siguientes opciones para definir una regla:

- Requisitos previos
- Requisitos previos
- Requisitos previos

Definir una regla mediante un origen de datos IPDB

Este tema proporciona instrucciones para definir una regla para obtener datos o eventos a partir de un origen de datos de IPDB.

Requisitos previos

Asegúrese de que:

- Comprender qué tipo de regla se debe usar en la regla. Para obtener más información acerca de los tipos de reglas, consulte Tipos de regla.
- Comprender la sintaxis de las reglas de IPDB. Para obtener más información, consulte Sintaxis de reglas de IPDB.
- Comprender los componentes de la vista Regla. Para obtener más información, consulte Vista Regla.
- Comprender los componentes de la vista Crear regla. Para obtener más información, consulte Vista Crear regla.

Procedimiento

Realice los siguientes pasos para definir una regla para obtener datos o eventos desde un origen de datos de IPDB:

1. En el menú de Security Analytics, haga clic en **Administration** > **Informes**.

   Se muestra la pestaña Administrar.

2. En la barra de herramientas Regla, haga clic en  > **IPDB**.

   Se muestra la vista Crear regla.

3. En el campo **Tipo de regla**, **IPDB** está seleccionado de manera predeterminada.
4. En el campo **Nombre**, ingrese el nombre que se usará para identificar o etiquetar la regla en alertas e informes.
5. En el campo **Select**, ingrese metadatos o selecciónelos en la lista de tipos de metadatos disponibles que se proporciona en el panel Metadatos. Para obtener más información, consulte el tema **Panel Metadatos** en la vista Crear regla.
6. En el campo **Origen de eventos**, puede configurar la especificación de origen de eventos para asignar dispositivos dinámicamente a la misma regla. Para obtener más información, consulte Especificación de orígenes de eventos de IPDB. También puede insertar una lista en este campo mediante la selección de una lista y la navegación a **Insertar > Origen de evento** en el panel Listas.
7. En el campo **Where**, ingrese metadatos o selecciónelos en la lista de tipos de metadatos disponibles que se proporciona en el panel Metadatos. La cláusula Where proporciona los criterios de consulta base para la regla. También puede insertar una lista en este campo mediante la selección de una lista y la navegación a **Insertar > Where** en el panel Listas.
8. En el campo **Agrupar por**, ingrese los metadatos que seleccionó en la cláusula Select de modo que el conjunto de resultados se agrupe de acuerdo con los metadatos.

9. En el campo **Ordenar por**, realice lo siguiente:
   a. En la columna **Nombre de la columna**, ingrese el nombre de las columnas según las cuales desea agrupar los resultados.
   b. En la columna **Ordenar por**, seleccione una de las siguientes formas de clasificar los resultados:
      - Orden ascendente
      - Orden descendente
10. En el campo **Límite**, ingrese el límite que se introducirá en la consulta mientras se obtienen los datos de la base de datos. Si un resultado se ordena según el conteo de la sesión, el conteo del paquete o el tamaño de la sesión, el límite representa los primeros (o los últimos) valores N que se devolvieron. Si el conjunto de resultados no se ordena, se devuelven los primeros valores N.
11. Haga clic en **Guardar**.

Próximos pasos

Para probar la exactitud de la regla que creó, haga clic en **Probar regla**. Para obtener instrucciones, consulte Probar una regla.

Definir una regla mediante el origen de datos de NetWitness

En este tema se proporcionan instrucciones para definir una regla para obtener datos o eventos desde un origen de datos de NetWitness. Puede definir reglas para obtener datos o eventos desde un origen de datos de NetWitness. Se usa el mismo procedimiento para definir una regla para obtener datos o eventos desde un origen de datos de Archiver.

El origen de datos de Archiver se puede agregar en la vista Configuración de servicios de Reporting Engine. Para obtener más información, consulte (Opcional) Agregar Archiver como un origen de datos en Reporting Engine en la *Guía de configuración de hosts y servicios*.

Requisitos previos

Asegúrese de que:

- Comprender qué tipo de regla se debe usar en la regla. Para obtener más información acerca de los tipos de reglas, consulte Tipos de regla.
- Comprender la sintaxis de las reglas de NWDB. Para obtener más información, consulte Sintaxis de reglas de NWDB.
- Comprender los componentes de la vista Regla. Para obtener más información, consulte Vista Regla.

- Comprender los componentes de la vista Crear regla. Para obtener más información, consulte Vista Crear regla.
- Comprender cómo se crean las claves de metadatos personalizados mediante feeds personalizados. Para obtener más información, consulte el tema Crear claves de metadatos personalizados mediante un feed personalizado en la *Guía de configuración de hosts y servicios*.

Procedimiento

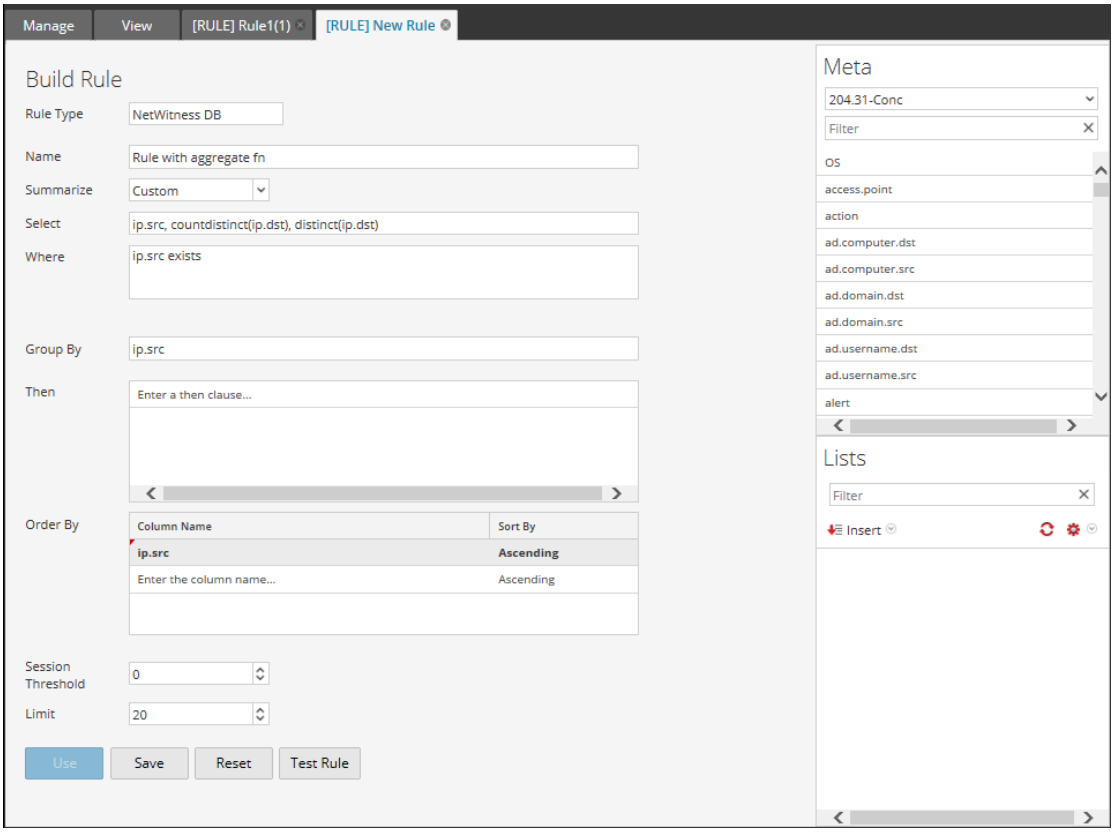
Realice los siguientes pasos para definir una regla con el fin de obtener datos o eventos desde un origen de datos de NetWitness:

1. En el menú de Security Analytics, haga clic en **Administration** > **Informes**.

   Se muestra la pestaña Administrar.

2. En la barra de herramientas Regla, haga clic en  >**Base de datos de NetWitness**.

   Se muestra la pestaña de la vista Crear regla.



3. En el campo **Tipo de regla**, **Base de datos de NetWitness** está seleccionado de manera predeterminada.

4. En el campo **Nombre**, ingrese el nombre que se usará para identificar o etiquetar la regla en alertas e informes.
5. El campo **Resumir** determina el tipo de resumen o agregación para la regla. De acuerdo con el tipo de regla que se definirá, debe seleccionar una de las siguientes opciones:
   - Para definir una regla **no agregada** sin ninguna agrupación, seleccione: **Ninguno**
   - Para definir una regla **agregada** con agregación especial, como los agregados relacionados con la recopilación (sesiones/eventos/paquetes), seleccione una de las siguientes opciones:
     - Conteo de eventos
     - Conteo de paquetes
     - Tamaño de sesión
   - Para definir una regla **agregada** con valores de metadatos y agregados personalizados, como sum(), count(), etc., seleccione: **Personalizado**

     Si selecciona “Personalizada” en el campo **Resumir**, podrá definir la función de agregado que desee en la cláusula *Select*. Por ejemplo, select ip.src, countdistinct(ip.dst), distinct(ip.dst).Las funciones de agregado compatibles son:
     - sum(<meta>)
     - count(<meta>)
     - countdistinct(<meta>)
     - min(<meta>)
     - max(<meta>)
     - avg(<meta>)
     - first(<meta>)
     - last(<meta>)
     - len(<meta>)
     - distinct(<meta>)

     Para obtener información más detallada sobre las reglas agregadas y no agregadas, consulte Sintaxis de reglas de NWDB.
6. En el campo **Select**, ingrese metadatos o selecciónelos en la lista de tipos de metadatos disponibles que se proporciona en la Biblioteca de metadatos. Para obtener más información, consulte el tema *Panel Metadatos* en la Vista Crear regla. El nombre de metadatos para buscar un registro crudo es raw. raw solo se puede usar en el campo **Select**. No se puede

usar en los campos **Where** y **Then**. Varias funciones de agregado son compatibles para la regla agregada personalizada en el campo **Select**.

Nota: En versiones anteriores de Security Analytics, solo era compatible una función de agregado para la regla agregada personalizada en la cláusula **Select**. Desde ahora, varias funciones de agregado son compatibles en la cláusula **Select**. Por ejemplo, Select: *ip.src, username, service, distinct(country.src), sum(payload)*.

7. En el campo **Where**, ingrese metadatos o seleccione metadatos de la lista de tipos de metadatos disponibles y use los operadores para crear la cláusula Where para los criterios de consulta base.
8. El campo **Agrupar por** es un campo de solo lectura que se completa con metadatos que se definen en la cláusula Select. Para una función no de agregado, este campo no es visible. El campo **Agrupar por** es compatible con un máximo de seis metadatos.

   Nota: En versiones anteriores de Security Analytics, solo era compatible un metadato para la regla agregada personalizada en la cláusula **Group By**. Desde ahora, la cláusula **Group By** es compatible con un máximo de seis metadatos.
9. En el campo **Then**, ingrese las acciones de regla que manipulan el conjunto de resultados original de una regla para lograr que la salida en un informe sea más concreta o agregar una funcionalidad adicional distinta a la consulta de datos y su visualización, por ejemplo, la creación de un feed a partir de los resultados. Para obtener una lista completa de acciones de regla disponibles, consulte Sintaxis de reglas de NWDB.

   Nota: Cuando se ejecuta una regla para un origen de datos de Archiver, se recomienda no usar acciones de regla intensivas como lookup_and_add() y show_whats_new().
10. En el campo **Ordenar por**, realice lo siguiente:
    a. En la columna **Nombre de la columna**, ingrese el nombre de las columnas según las cuales desea ordenar los resultados. De forma predeterminada, el valor está vacío. El valor se completa de acuerdo con el valor que se selecciona en el campo **Resumir**.
       - En el caso de Resumir “Ninguno”, si no se selecciona ningún valor para **Ordenar por**, se aplica un orden predeterminado por hora de recopilación o sesión.
       - Para otros valores de Resumen, el orden predeterminado se basa en el primer metadato “group by” seleccionado cuando no se define ningún “order by”. Para Conteo de eventos, Conteo de paquetes y Tamaño de sesión, los valores aceptados son Total y Valor.

    b. En la columna **Ordenar por**, seleccione una de las siguientes formas de clasificar los resultados:

- Orden ascendente
- Orden descendente

11. En el campo **Umbral de sesión**, ingrese la configuración de optimización para dejar de escanear las sesiones coincidentes en busca de cada valor único posible para los metadatos seleccionados. El umbral es un entero entre 0 (predeterminado) y 2,147,483,647.

    Nota: Esto se aplica solo a las reglas agregadas de NWDB. Si se especifica el valor predeterminado, se escanearán todas las sesiones coincidentes y se devolverá el valor preciso. Un umbral de sesión permite conteos precisos para un valor. Sin embargo, esto produce un tiempo de ejecución de reglas más prolongado. Por ejemplo, considere establecer el umbral de sesión en 1,000 para ip.src. Si hay 5,000 sesiones coincidentes para un valor de ip.src específico, que está presente en más de 1,000 sesiones, NWDB deja de escanear después de 1,000 sesiones y devuelve el valor agregado extrapolado. Esto optimiza el tiempo de ejecución de consultas. Si el valor está presente en menos de 1,000 sesiones, se devuelve el valor real.

12. En el campo **Límite**, ingrese el límite que se introducirá en la consulta mientras se obtienen los datos de la base de datos. Si un conjunto de resultados se ordena por conteo de eventos, conteo de paquetes o tamaño de sesión, el límite representa los N valores superiores (o inferiores) que se devolverán. Si el conjunto de resultados no se ordena, se devuelven los primeros valores N.
13. Haga clic en **Guardar**.

    Nota: A diferencia de los metadatos analizados, los registros crudos se obtienen desde los Decoders. Cuando tanto el registro crudo como los metadatos analizados se consultan en una única regla, debido a los distintos periodos de retención, puede haber metadatos analizados disponibles y puede que falten registros crudos en la misma sesión. De modo que el resultado tendrá valores de metadatos analizados y un valor crudo vacío para esas sesiones. Por ejemplo, para la regla "Select **ip.src**, **ip.dst**, **service**, **username**, **raw**", los metadatos analizados podrían completarse y los metadatos **crudos** permanecen vacíos para algunas sesiones.

Próximos pasos

Para probar la exactitud de la regla que creó, haga clic en **Probar regla**. Para obtener instrucciones, consulte Probar una regla.

Definir una regla mediante el origen de datos de Warehouse

Este tema proporciona instrucciones para definir una regla para obtener datos o eventos a partir de un origen de eventos de Warehouse. Puede definir las reglas en dos modos:

- Modo Predeterminado
- Modo experto

Para obtener más información acerca de los modelos, consulte Modos de definición de reglas de la base de datos de Warehouse.

Requisitos previos

Asegúrese de que:

- Comprender qué tipo de regla se debe usar en la regla. Para obtener más información acerca de los tipos de regla, consulte Tipos de regla.
- Comprender los componentes de la vista Regla. Para obtener más información, consulte Vista Regla.
- Comprender los componentes de la vista Crear regla. Para obtener más información, consulte Vista Crear regla.
- Comprender cómo se crean las claves de metadatos personalizados mediante feeds personalizados. Para obtener más información, consulte el tema Crear claves de metadatos personalizados mediante un feed personalizado en la *Guía de configuración de hosts y servicios*.

Procedimiento

Realice los siguientes pasos para definir una regla con el fin de obtener datos o eventos desde un origen de datos de Warehouse:

1. En el menú de Security Analytics, haga clic en **Administration** > **Informes**.

   Se muestra la pestaña Administrar.

2. En la barra de herramientas Regla, haga clic en  > **Base de datos de Warehouse.**
3. Se muestra la pestaña de la vista Crear regla.
4. En el campo **Tipo de regla**, **Base de datos de Warehouse** está seleccionado de forma predeterminada.

   Si va a definir la regla en modo Predeterminado, realice lo siguiente:

   a. En el campo **Nombre**, ingrese el nombre que se usará para identificar o etiquetar la regla en alertas e informes.

   b. En el campo **Seleccionar**, ingrese metadatos o selecciónelos desde el menú desplegable o desde la lista de tipos de metadatos disponibles que se proporciona en el panel

Metadatos. Para obtener más información, consulte el tema *Panel Metadatos* en la vista Crear regla.

c. En el menú desplegable **Desde**, seleccione una de las siguientes opciones:
   - Sesión
   - Logs

d. En el campo **Alias**, ingrese el nombre de alias de las columnas que se usan en la cláusula Select.

e. En el campo **Where**, ingrese metadatos o selecciónelos en la lista de tipos de metadatos disponibles que se proporciona en el panel Metadatos. La cláusula Where proporciona los criterios de consulta base para la regla.

f. En el campo **Agrupar por**, ingrese los metadatos que seleccionó en la cláusula Select de modo que el conjunto de resultados se agrupe de acuerdo con los metadatos.

g. En el campo **Que contenga**, ingrese los criterios para filtrar el conjunto de resultados para consultas adicionales.

h. En el campo **Ordenar por**, realice lo siguiente:
   1. En la columna **Nombre de la columna**, ingrese el nombre de las columnas según las cuales desea agrupar los resultados.
   2. En la columna **Ordenar por**, seleccione una de las siguientes formas de clasificar los resultados:
      - Orden ascendente
      - Orden descendente

i. En el campo **Límite**, ingrese el límite que se introducirá en la consulta mientras se obtienen los datos de la base de datos. Si un resultado se ordena según el conteo de la sesión, el conteo del paquete o el tamaño de la sesión, el límite representa los primeros (o los últimos) valores N que se devolvieron. Si el conjunto de resultados no se ordena, se devuelven los primeros valores N.

j. Haga clic en **Guardar**.

5. Si va a definir la regla en modo experto, seleccione la casilla de verificación **Modo experto** y realice lo siguiente:

   a. En el campo **Nombre**, ingrese el nombre que se usará para identificar o etiquetar la regla en alertas e informes.

b. En el campo **Consulta**, ingrese la declaración de consulta de Hive para realizar la consulta al origen de datos.

c. En el campo **Alias**, ingrese el nombre de alias de las columnas que se usan en la cláusula Select.

d. Haga clic en **Guardar**.

Próximos pasos

Para probar la exactitud de la regla que creó, haga clic en **Probar regla**. Para obtener instrucciones, consulte Probar una regla.

Probar una regla

En este tema se proporcionan instrucciones para probar una regla basada en el rango de tiempo y el origen de datos seleccionado.

Requisitos previos

Asegúrese de que:

- Comprender los componentes de la vista Regla. Para obtener más información, consulte Vista Regla.
- Comprender los componentes de la vista Crear regla. Para obtener más información, consulte Vista Crear regla.

Procedimiento

Realice los siguientes pasos para probar una regla:

1. En el menú de Security Analytics, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. En el panel Lista de reglas, realice una de las siguientes acciones:
   - Seleccione una regla y haga clic en  en la barra de herramientas Reglas.
   - Haga clic en  > **Editar**.
     Se muestra la pestaña de la vista Crear regla.
3. Haga clic en **Probar regla**.
   Se muestra la vista Probar regla:

> **Nota:** Al hacer clic en **Probar regla**, no se guarda la regla. Debe hacer clic en **Guardar** en la vista Crear regla para guardarla.

4. En la lista desplegable **Origen de datos**, seleccione un origen de datos.
   Debe seleccionar el origen de datos adecuado para la regla definida.
5. Desde la lista desplegable **Formato**, seleccione el formato en el que desea que se muestren los resultados.
6. En la lista desplegable **Rango de tiempo**, seleccione una de las siguientes opciones.
   - **Pasado**: Para especificar una cantidad de años, días, semanas, meses, días u horas.
   - **Rango**: Para especificar un rango de fechas y un período.

   > **Nota:** En la interfaz del usuario, la fecha o la hora mostradas dependen del perfil de zona horaria que seleccionó el usuario.

7. **Eje X** y **Eje Y** se usan para especificar los metadatos que se trazarán en los gráficos.
   En **Eje X** se muestran los metadatos de la regla “Group by”. En **Eje Y** se muestran las funciones de agregado que se usan en la regla.

Nota: Sum, Count, Countdistinct y Average son las funciones de agregado compatibles con la regla. De manera predeterminada, para las reglas personalizadas con múltiples “Group by”, puede seleccionar solo los primeros metadatos en el **Eje X**.

8. Haga clic en **Ejecutar prueba** para ejecutar la regla.
   Se muestran los datos de reglas (en caso de haberlos) para el rango de tiempo seleccionado.

Ajustar reglas de IPDB

En este tema se describe cómo crear definiciones de reglas para mejorar el rendimiento de los informes. Puede crear definiciones de reglas para mejorar el rendimiento de los informes. A continuación se indica cómo definir reglas para lograr ganancias de rendimiento:

- Se obtienen ganancias de rendimiento si las variables de la cláusula WHERE contienen variables de índice de IPDB con cláusulas de coincidencia exacta (“=”, “IN”).
- NO se obtienen ganancias de rendimiento cuando se usan cláusulas de coincidencia exacta como operadores “LIKE”, GREATER THAN “>” y LESS THAN “<” con las variables de índice de IPDB.

Los ejemplos de consultas de la siguiente tabla permiten comprender el impacto de la consulta en el rendimiento de los informes.

N.º de caso	Cláusula Where	Ganancia de rendimiento esperada	Comentarios
1	IndexedVar1 = “value1” AND UnIndexedVar2 = “value2”	Sí	Se comprueba el índice del filtro de IPDB para IndexedVar1 con el fin de verificar si “value1” existe o no. Si “value1” existe, el archivo de datos se lee; de lo contrario, se omite.

N.º de caso	Cláusula Where	Ganancia de rendimiento esperada	Comentarios
2	UnIndexedVar2 = “value2” AND IndexedVar1 = “value1”	Sí	El índice del filtro de IPDB solo se aplica en IndexedVar1 con el fin de verificar si “value1” existe o no. Si “value1” existe, el archivo de datos se lee; de lo contrario, se omite. El orden de la variable indexada y no indexada es irrelevante.
3	IndexedVar1 = “value1” OR UnIndexedVar2 = “value2”	No	El índice del filtro de IPDB no puede determinar la disponibilidad de los datos debido al operador “OR” entre la variable indexada y no indexada.
4	IndexedVar1 = “value1” OR IndexedVar2 = “value2”	Sí	El índice del filtro de IPDB se aplicará en IndexedVar1 e IndexedVar2 para verificar “value1” y “value2”, respectivamente. Si cualquiera de los valores existe, el archivo de datos se lee; de lo contrario, se omite.
5	IndexedVar1 = “value1” AND UnIndexedVar2 LIKE “value%”	Sí	El índice del filtro de IPDB solo se aplica en IndexedVar1 con el fin de verificar si “value1” existe o no. Si “value1” existe, el archivo de datos se lee; de lo contrario, se omite.

N.º de caso	Cláusula Where	Ganancia de rendimiento esperada	Comentarios
6	IndexedVar1 LIKE “value1%” AND UnIndexedVar2 LIKE “value2%”	No	Ningún índice del filtro de IPDB funciona solo con cláusulas de coincidencia exacta.
7	IndexedVar1 LIKE “value1%” AND UnIndexedVar2 LIKE “value2%” AND IndexedVar3 = “value3”	Sí	El índice del filtro de IPDB solo se aplica en IndexedVar3 con el fin de verificar si “value3” existe o no. Si “value1” existe, el archivo de datos se lee; de lo contrario, se omite.

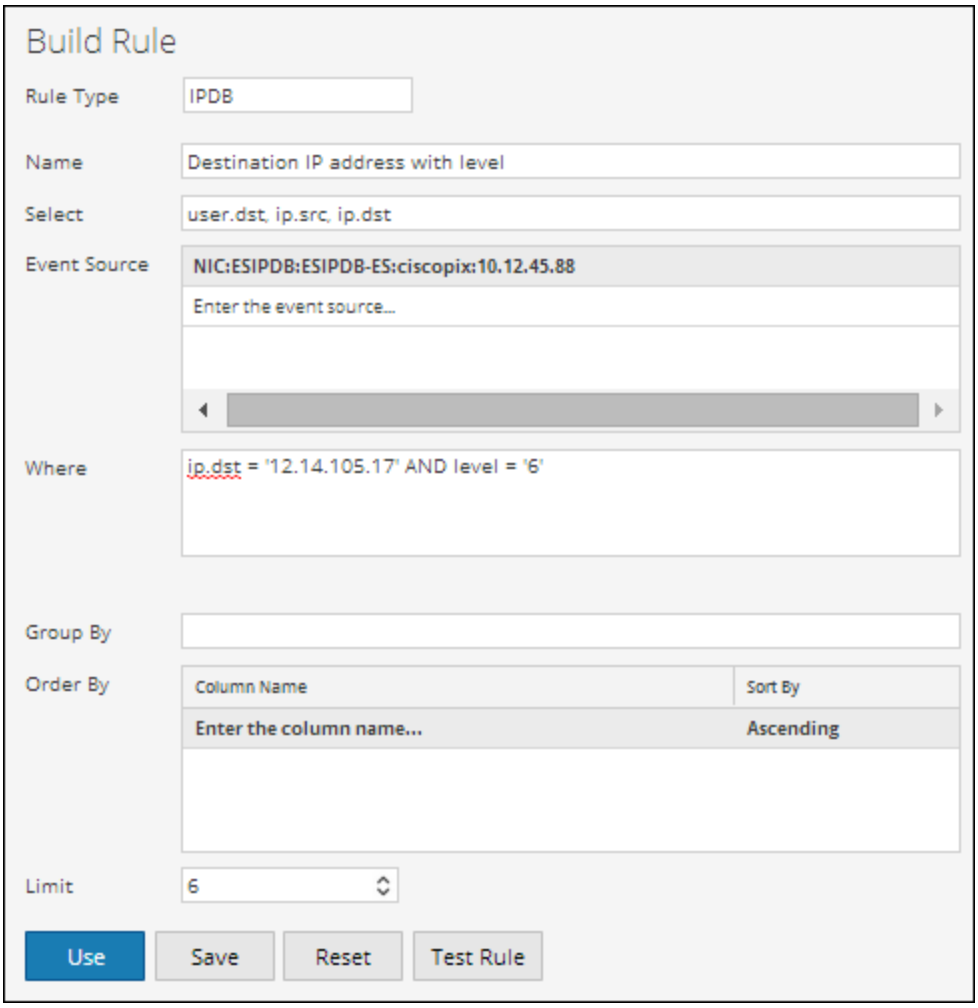
En esta sección se proporcionan algunos ejemplos de las definiciones de reglas con variables indexadas.

Ejemplo del caso 1: Variable indexada con operador AND

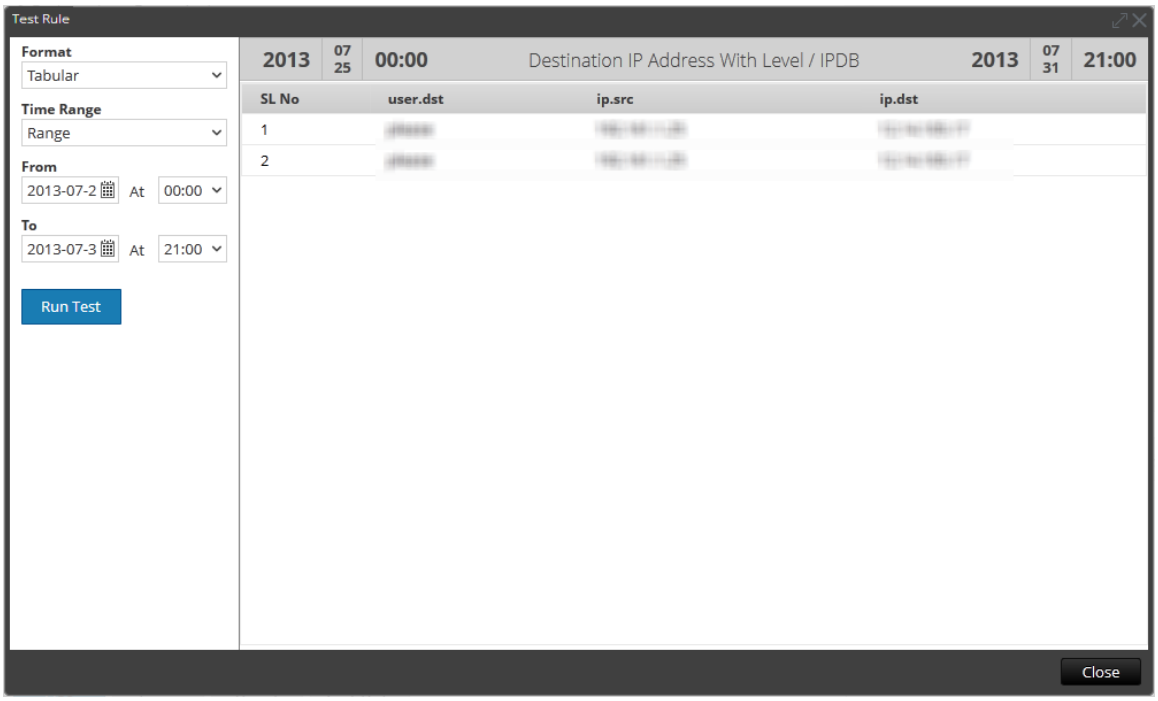
El siguiente es un ejemplo de una consulta para el caso 1:

N.º de caso	Cláusula Where	Ganancia de rendimiento esperada	Comentarios
1.	IndexedVar1 = “value1” AND UnIndexedVar2 = “value2”	Sí	Se comprueba el índice del filtro de IPDB para IndexedVar1 con el fin de verificar si “value1” existe o no. Si “value1” existe, el archivo de datos se lee; de lo contrario, se omite.

La consulta se define para ver las direcciones IP de destino con un valor de nivel específico. Observe que la cláusula Where contiene la variable indexada ip.dst y el nivel de variable no indexada con el operador AND.



Aunque hay millones de registros, el informe se genera rápidamente con la ayuda de la variable indexada:

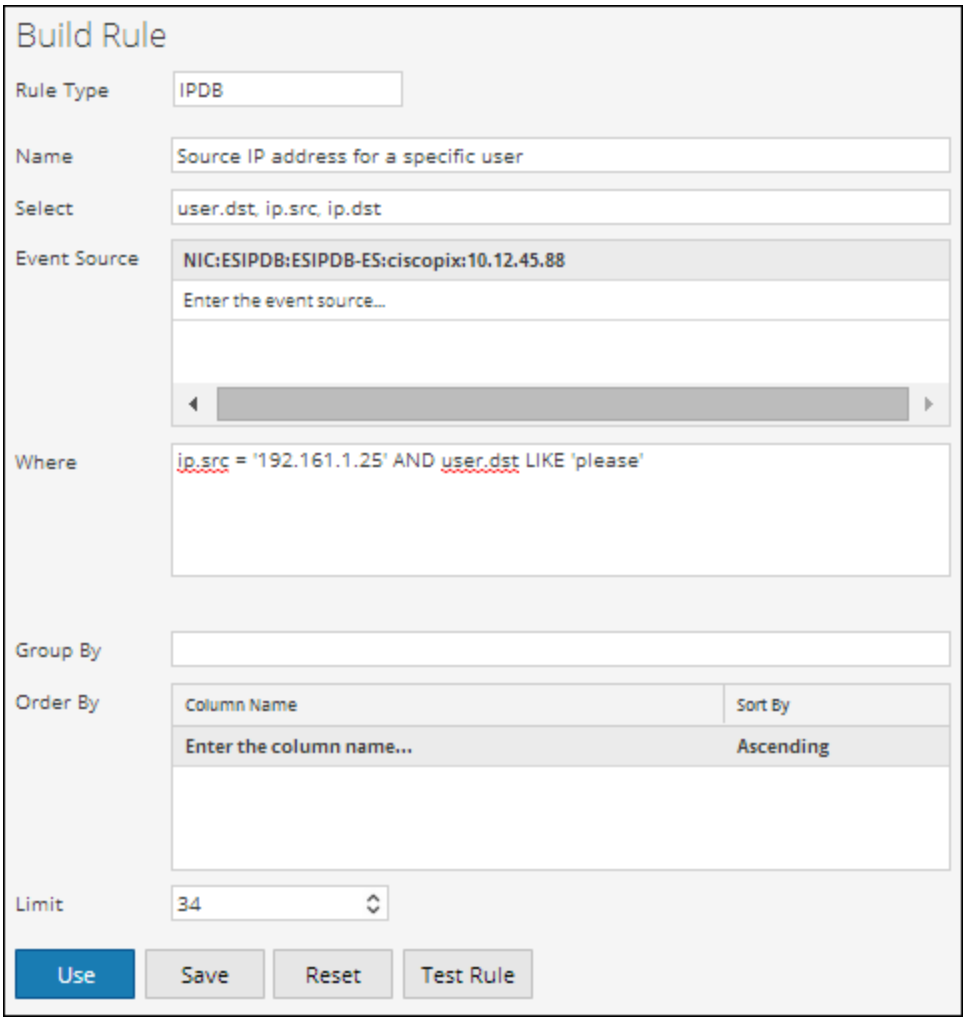


Ejemplo del caso 5: Variable indexada con función LIKE

El siguiente es un ejemplo de una consulta para el caso 5:

N.º de caso	Cláusula Where	Ganancia de rendimiento esperada	Comentarios
5.	IndexedVar1 = “value1” AND UnIndexedVar2 LIKE “value%”	Sí	El índice del filtro de IPDB solo se aplica en IndexedVar1 con el fin de verificar si “value1” existe o no. Si “value1” existe, el archivo de datos se lee; de lo contrario, se omite.

El siguiente es un ejemplo de una consulta para ver las direcciones IP de origen de un usuario específico. Observe que la cláusula Where contiene la variable indexada ip.src y la variable no indexada user.dst con la opción LIKE, como se mencionó en el caso 5 de la tabla.

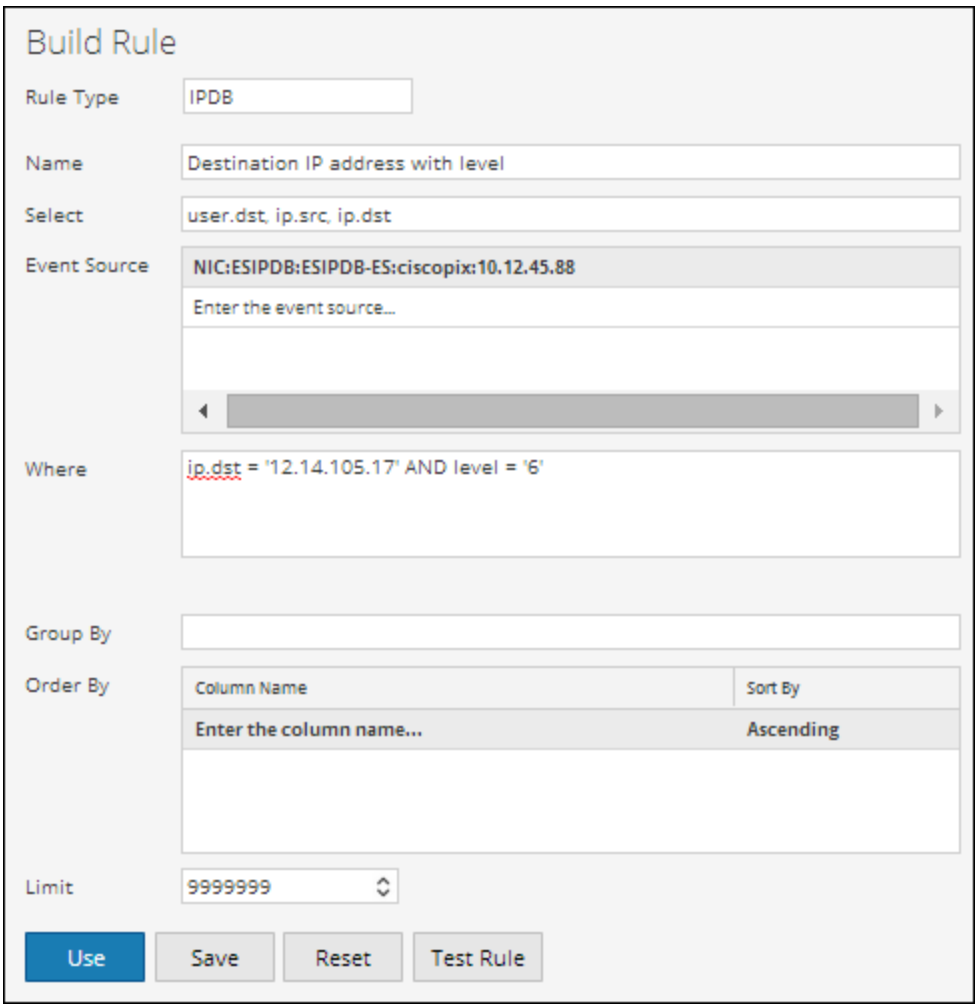


Ejemplo del caso 3: Variable indexada con operador OR

El siguiente es un ejemplo de una consulta para el caso 3:

N.º de caso	Cláusula Where	Ganancia de rendimiento esperada	Comentarios
3.	<IndexedVar1 = “value1” OR UnIndexedVar2 = “value2”	No	El índice del filtro de IPDB no puede determinar la disponibilidad de los datos debido al operador “OR” entre la variable indexada y no indexada.

La consulta siguiente se define para ver las direcciones IP de destino con un valor de nivel específico. Observe que la cláusula Where contiene la variable indexada ip.dst y el nivel de variable no indexada con el operador OR. La consulta siguiente no permitirá una ganancia de rendimiento.



Usar alias de metadatos para Reporting Engine

En este tema se abordan los distintos alias de metadatos compatibles con Reporting Engine. Cuando hace referencia a metadatos en informes y gráficos, solo puede ver alias de los nombres de metadatos. Estos alias los hacen más comprensibles para una audiencia más amplia.

Solo puede usar los alias predefinidos para los metadatos, pero no puede modificar estos valores.

No puede proporcionar valores de alias para los metadatos en la cláusula WHERE, porque Security Analytics utiliza la cláusula WHERE para obtener datos del origen de datos (por ejemplo, en Concentrator) y estos no son compatibles con alias. Es decir, no puede proporcionar el valor de alias **HTTP** para el puerto HTTP n.º 80.

Nota: * No puede crear alias para metadatos distintos de aquellos que ya existen en Reporting Engine. Además, el formato de los alias no se puede cambiar.
* Los alias no son compatibles con alertas ni informes CSV.

Procedimiento

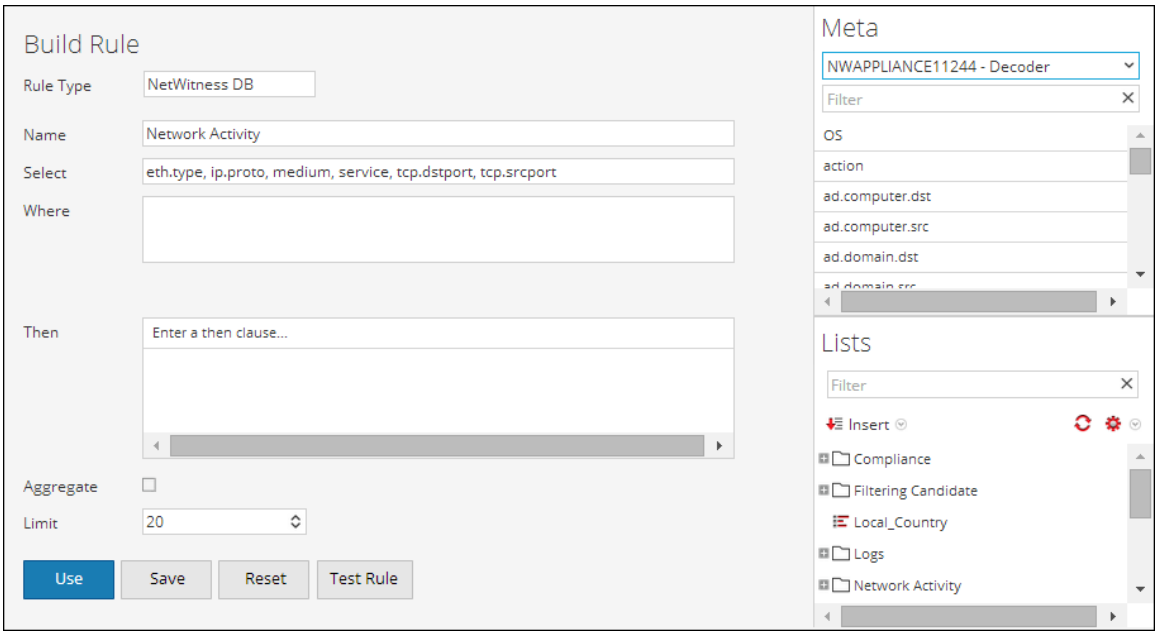
Para usar alias en una regla, siga estos pasos:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. En el panel Lista de reglas, realice una de las siguientes acciones:

   - Seleccione una regla y haga clic en en la barra de herramientas Reglas.
   - Haga clic en > **Editar**.

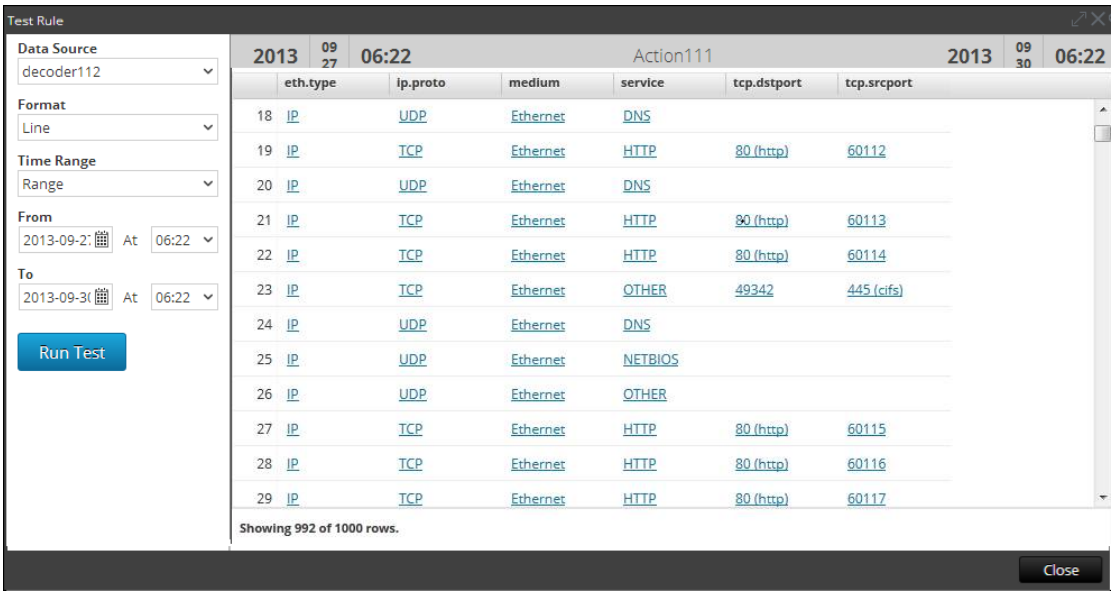
3. Especifique los metadatos con alias en el campo **Seleccionar**.

En el siguiente ejemplo se especifican los metadatos **eth.type**, **ip.proto**, **medium**, **service**, **tcp.dstport**, and **tcp.srcport** en el campo Seleccionar.



4.

Haga clic en **Probar regla** para consultar los resultados que devuelve esta regla.
En el siguiente ejemplo se muestran los resultados bajo las columnas de alias **eth.type**, **ip.proto**, **medium**, **service**, **tcp.dstport** y **tcp.srcport** que se especificaron en el campo **Seleccionar** de la regla.



Definiciones de alias que suministra RSA

Los archivos de alias que aparecen en este tema son solamente ejemplos y se basan en las definiciones de alias actuales de Reporting Engine. Security Analytics no puede modificar estas definiciones en Reporting Engine en función de los cambios realizados en el archivo xml de Concentrator. Por lo tanto, los cambios realizados en el archivo xml de Concentrator no se reflejan en Reporting Engine.

Los detalles de los distintos metadatos se explican en cada uno de los **meta.aliases**.

eth.type

```
ALIAS_FORMAT=$alias
 0=802.3
 257=Experimental
 512=Xerox PUP
 513=Xerox PUP
 1024=Nixdorf
 1536=Xerox NS IDP
 1537=XNS Address Translation (3Mb only)
 2048=IP
 2049=X.75 Internet
 2050=NBS Internet
 2051=ECMA Internet
 2052=CHAOSnet
 2053=X.25 Level 3
 2054=ARP
 2055=XNS Compatibility
 2076=Symbolics Private
 2184=Xyplex
 2304=Ungermann-Bass network debugger
 2560=Xerox IEEE802.3 PUP
 2561=Xerox IEEE802.3 PUP Address Translation
 2989=Banyan Systems
 2991=Banyon VINES Echo
 4096=Berkeley Trailer negotiation
 4097=Berkeley Trailer encapsulation for IP
 4660=DCA - Multicast
 5632=VALID system protocol
 6537=Artificial Horizons
 6549=Datapoint Corporation (RCL lan protocol)
 15360=3Com NBP virtual circuit datagram (like XNS SPP) not registered
 15361=3Com NBP System control datagram not registered
 15362=3Com NBP Connect request (virtual cct) not registered
 15363=3Com NBP Connect repsonse not registered
 15364=3Com NBP Connect complete not registered
 15365=3Com NBP Close request (virtual cct) not registered
 15366=3Com NBP Close response not registered
 15367=3Com NBP Datagram (like XNS IDP) not registered
 15368=3Com NBP Datagram broadcast not registered
 15369=3Com NBP Claim NetBIOS name not registered
 15370=3Com NBP Delete Netbios name not registered
 15371=3Com NBP Remote adaptor status request not registered
 15372=3Com NBP Remote adaptor response not registered
 15373=3Com NBP Reset not registered
 16972=Information Modes Little Big LAN diagnostic
 17185=THD - Diddle
 19522=Information Modes Little Big LAN
```

```
21000=BBN Simnet Private
24576=DEC unassigned
24577=DEC Maintenance Operation Protocol (MOP) Dump/Load Assistance
24578=DEC Maintenance Operation Protocol (MOP) Remote Console
24579=DECNET Phase IV
24580=DEC Local Area Transport (LAT)
24581=DEC diagnostic protocol (at interface initialization?)
24582=DEC customer protocol
24583=DEC Local Area VAX Cluster (LAVC)
24584=DEC AMBER
24585=DEC MUMPS
24592=3Com Corporation
28672=Ungermann-Bass download
28673=Ungermann-Bass NIUs
28674=Ungermann-Bass diagnostic/loopback
28675=Ungermann-Bass ??? (NMC to/from UB Bridge)
28677=Ungermann-Bass Bridge Spanning Tree
28679=OS/9 Microware
28681=OS/9 Net?
28704=LRT (England) (now Sintrom)
28720=Racal-Interlan
28721=Prime NTS (Network Terminal Service)
28724=Cabletron
32771=Cronus VLN
32772=Cronus Direct
32773=HP Probe protocol
32774=Nestar
32776=AT&amp;amp;T/Stanford Univ.
32784=Excelan
32787=Silicon Graphics diagnostic
32788=Silicon Graphics network games
32789=Silicon Graphics reserved
32790=Silicon Graphics XNS NameServer
32793=Apollo DOMAIN
32814=Tymshare
32815=Tigan
32821=Reverse Address Resolution Protocol (RARP)
32822=Aeonic Systems
32823=IPX (Novell Netware?)
32824=DEC LanBridge Management
32825=DEC DSM/DDP
32826=DEC Argonaut Console
32827=DEC VAXELN
32828=DEC DNS Naming Service
32829=DEC Ethernet CSMA/CD Encryption Protocol
32830=DEC Distributed Time Service
32831=DEC LAN Traffic Monitor Protocol
32832=DEC PATHWORKS DECnet NETBIOS Emulation
```

```
32833=DEC Local Area System Transport
32834=DEC unassigned
32836=Planning Research Corp.
32838=AT&amp;amp;T
32839=AT&amp;amp;T
32840=DEC Availability Manager for Distributed Systems DECamds
32841=ExperData
32859=VMTP
32860=Stanford V Kernel
32861=Evans &amp;amp; Sutherland
32864=Little Machines
32866=Counterpoint Computers
32869=University of Mass. at Amherst
32870=University of Mass. at Amherst
32871=Veeco Integrated Automation
32872=General Dynamics
32873=AT&amp;amp;T
32874=Autophon
32876=ComDesign
32877=Compugraphic Corporation
32878=Landmark Graphics Corporation
32890=Matra
32891=Dansk Data Elektronik
32892=Merit Internodal
32893=Vitalink Communications
32896=Vitalink TransLAN III Management
32897=Counterpoint Computers
32904=Xyplex
32923=EtherTalk - AppleTalk over Ethernet
32924=Datability
32927=Spider Systems Ltd.
32931=Nixdorf Computers
32932=Siemens Gammasonics Inc.
32960=DCA Data Exchange Cluster
32966=Pacer Software
32967=Applitek Corporation
32968=Intergraph Corporation
32973=Harris Corporation
32975=Taylor Instrument
32979=Rosemount Corporation
32981=IBM SNA Services over Ethernet
32989=Varian Associates
32990=TRFS (Integrated Solutions Transparent Remote File System)
32992=Allen-Bradley
32996=Datability
33010=Retix
33011=AppleTalk Address Resolution Protocol (AARP)
33012=Kinetics
```

```
33015=Apollo Computer
33023=Wellfleet Communications
33026=Wellfleet BOFL
33027=Wellfleet Communications
33031=Symbolics Private
33067=Talaris
33072=Waterloo Microsystems Inc.
33073=VG Laboratory Systems
33079=IPX
33080=Novell Inc
33081=KTI
33087=M/MUMPS data sharing
33093=Vrije Universiteit (NL)
33094=Vrije Universiteit (NL)
33095=Vrije Universiteit (NL)
33100=SNMP
33103=Technically Elite Concepts
33169=PowerLAN
33149=XTP
33238=Artisoft Lantastic
33239=Artisoft Lantastic
33283=QNX Software Systems Ltd.
33680=Accton Technologies (unregistered)
34091=Talaris multicast
34178=Kalpana
34525=IPv6
34617=Control Technology Inc.
34618=Control Technology Inc.
34619=Control Technology Inc.
34620=Control Technology Inc.
34848=Hitachi Cable (Optoelectronic Systems Laboratory)
34902=Axis Communications AB
34952=HP LanProbe test?
36864=Loopback (Configuration Test Protocol)
36865=3Com XNS Systems Management
36866=3Com TCP/IP Systems Management
36867=3Com loopback detection
43690=DECNET
64245=Sonix Arpeggio
65280=BBN VITAL-LanBridge cache wakeups
34915=PPPoe
34916=PPPoe
2056=Frame Relay ARP
16962=IEEE bridge spanning protocol
25944=Bridged Ethernet/802.3 packet
65278=ISO CLNP/ISO ES-IS DSAP/SSAP
```

ip.proto

```
ALIAS_FORMAT=$alias
 0=HOPOPT
 1=ICMP
 2=IGMP
 3=GGP
 4=IP
 5=ST
 6=TCP
 7=CBT
 8=EGP
 9=IGP
 10=BBN-RCC-M
 11=NVP-II
 12=PUP
 13=ARGUS
 14=EMCON
 15=XNET
 16=CHAOS
 17=UDP
 18=MUX
 19=DCN-MEAS
 20=HMP
 21=PRM
 22=XNS-IDP
 23=TRUNK-1
 24=TRUNK-2
 25=LEAF-1
 26=LEAF-2
 27=RDP
 28=IRTP
 29=ISO-TP4
 30=NETBLT
 31=MFE-NSP
 32=MERIT-INP
 33=SEP
 34=3PC
 35=IDPR
 36=XTP
 37=DDP
 38=IDPR-CMTP
 39=TP++
 40=IL
 41=IPv6
 42=SDRP
 43=IPv6-Rout
 44=IPv6-Frag
```

```
45=IDRP
46=RSVP
47=GRE
48=MHRP
49=BNA
50=ESP
51=AH
52=I-NLSP
53=SWIPE
54=NARP
55=MOBILE
56=TLSP
57=SKIP
58=IPv6-ICMP
59=IPv6-NoNx
60=IPv6-Opts
61=AnyHost
62=CFTP
63=AnyNetwork
64=SAT-EXPAK
65=KRYPTOLAN
66=RVD
67=IPPC
68=AnyFile
69=SAT-MON
70=VISA
71=IPCV
72=CPNX
73=CPHB
74=WSN
75=PVP
76=BR-SAT-MO
77=SUN-ND
78=WB-MON
79=WB-EXPAK
80=ISO-IP
81=VMTP
82=SECURE-VM
83=VINES
84=TTP
85=NSFNET-IG
86=DGP
87=TCF
88=EIGRP
89=OSPFIGP
90=Sprite-RP
91=LARP
92=MTP
```

```
93=AX.25
94=IPIP
95=MICP
96=SCC-SP
97=ETHERIP
98=ENCAP
99=AnyPrivate
100=GMTP
101=IFMP
102=PNNI
103=PIM
104=ARIS
105=SCPS
106=QNX
107=A/N
108=IPComp
109=SNP
110=Compaq-Pe
111=IPX-in-IP
112=VRRP
113=PGM
114=AnyHop
115=L2TP
116=DDX
117=IATP
118=STP
119=SRP
120=UTI
121=SMP
122=SM
123=PTP
124=ISIS
125=FIRE
126=CRTP
127=CRUDP
128=SSCOPMCE
129=IPLT
130=SPS
131=PIPE Pr
132=SCTP St
133=FC Fi
134=RSVP-E2E-
255=Reserved
```

medium

```
ALIAS_FORMAT=$alias
 1=Ethernet
 2=Tokenring
 3=FDDI
 4=HDLC
 5=NetWitness
 6=802.11
 7=802.11 Radio
 8=802.11 AVS
 9=802.11 PPI
 10=802.11 PRISM
 11=802.11 Management
 12=802.11 Control
 13=DLT Raw
 32=Logs
```

Servicio

```
ALIAS_FORMAT=$alias
 0=OTHER
 20=FTPD
 21=FTP
 22=SSH
 23=TELNET
 25=SMTP
 53=DNS
 67=DHCP
 69=TFTP
 80=HTTP
 110=POP3
 111=SUNRPC
 119=NNTP
 123=NTP
 135=RPC
 137=NETBIOS
 139=SMB
 143=IMAP
 161=SNMP
 179=BGP
 443=SSL
 502=MODBUS
 520=RIP
 1024=EXCHANGE
 1080=SOCKS
 1122=MSN IM
 1344=ICAP
 1352=NOTES
 1433=TDS
 1521=TNS
 1533=SAMETIME
 1719=H.323
 1720=RTP
 2000=SKINNY
 2040=SOULSEEK
 2049=NFS
 3270=TN3270
 3389=RDP
 3700=DB2
 5050=YAHOO IM
 5060=SIP
 5190=AOL IM
 5222=Google Talk
 5900=VNC
 6346=GNUTELLA
```

```
6667=IRC
6801=Net2Phone
6881=BITTORRENT
8000=QQ
8002=YCHAT
8019=WEBMAIL
8082=FIX
20000=DNP3
1000000=KERNEL
1000001=USER
1000003=SYSTEM
1000004=AUTH
1000005=LOGGER
1000006=LPD
1000008=UUCP
1000009=SCHEDULE
1000010=SECURITY
1000013=AUDIT
1000014=ALERT
1000015=CLOCK
```

tcp.dstport

```
ALIAS_FORMAT=$value ($alias)
 7=echo
 9=discard
 13=daytime
 17=qotd
 19=chargen
 20=ftp-data
 21=ftp
 22=ssh
 23=telnet
 25=smtp
 37=time
 42=nameserver
 43=nicname
 53=domain
 70=gopher
 79=finger
 80=http
 88=kerberos
 101=hostname
 102=iso-tsap
 107=rtelnet
 109=pop2
 110=pop3
 111=sunrpc
 113=auth
 117=uucp-path
 119=nntp
 135=epmap
 137=netbios-ns
 139=netbios-ssn
 143=imap
 158=pcmail-srv
 170=print-srv
 179=bgp
 194=irc
 389=ldap
 443=https
 445=cifs
 464=kpasswd
 512=exec
 513=login
 514=cmd
 515=printer
 520=efs
 526=tempo
```

```
530=courier
531=conference
532=netnews
540=uucp
543=klogin
544=kshell
556=remotefs
636=ldaps
749=kerberos-adm
993=imaps
995=pop3s
1109=kpop
1433=ms-sql-s
1434=ms-sql-m
1512=wins
1524=ingreslock
1723=pptp
2053=knetd
1122=msn im
1352=notes
1521=tns
1533=sametime
1718=h323
1720=rtp
1863=msn im
2049=nfs
3389=rdp
5050=yahoo im
5060=sip
5190=aim
6346=gnuetella
6667=irc
9001=tor
9030=tor
9535=man
```

tcp.srcport

```
ALIAS_FORMAT=$value ($alias)
 7=echo
 9=discard
 13=daytime
 17=qotd
 19=chargen
 20=ftp-data
 21=ftp
 22=ssh
 23=telnet
 25=smtp
 37=time
 42=nameserver
 43=nicname
 53=domain
 70=gopher
 79=finger
 80=http
 88=kerberos
 101=hostname
 102=iso-tsap
 107=rtelnet
 109=pop2
 110=pop3
 111=sunrpc
 113=auth
 117=uucp-path
 119=nntp
 135=epmap
 137=netbios-ns
 139=netbios-ssn
 143=imap
 158=pcmail-srv
 170=print-srv
 179=bgp
 194=irc
 389=ldap
 443=https
 445=cifs
 464=kpasswd
 512=exec
 513=login
 514=cmd
 515=printer
 520=efs
 526=tempo
```

```
530=courier
531=conference
532=netnews
540=uucp
543=klogin
544=kshell
556=remotefs
636=ldaps
749=kerberos-adm
993=imaps
995=pop3s
1109=kpop
1433=ms-sql-s
1434=ms-sql-m
1512=wins
1524=ingreslock
1723=pptp
2053=knetd
1122=msn im
1352=notes
1521=tns
1533=sametime
1718=h323
1720=rtp
1863=msn im
2049=nfs
3389=rdp
5050=yahoo im
5060=sip
5190=aim
6346=gnuetella
6667=irc
9001=tor
9030=tor
9535=man
```

udp.dstport

```
ALIAS_FORMAT=$value ($alias)
 7=echo
 9=discard
 13=daytime
 17=qotd
 19=chargen
 37=time
 39=rlp
 42=nameserver
 53=domain
 67=bootps
 68=bootpc
 69=tftp
 88=kerberos
 111=sunrpc
 123=ntp
 135=epmap
 137=netbios-ns
 138=netbios-dgm
 161=snmp
 162=snmptrap
 213=ipx
 443=https
 445=cifs
 464=kpasswd
 500=isakmp
 512=biff
 513=who
 514=syslog
 517=talk
 518=ntalk
 525=timed
 533=netwall
 550=new-rwho
 560=rmonitor
 561=monitor
 749=kerberos-adm
 1167=phone
 1433=ms-sql-s
 1434=ms-sql-m
 1512=wins
 1701=l2tp
 1812=radiusauth
 1813=radacct
 2049=nfsd
 2504=nlbs
```

Eliminar una regla

En este tema se proporcionan instrucciones para eliminar una regla.

Requisitos previos

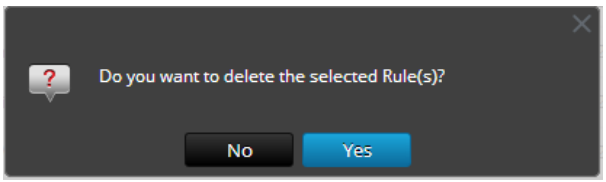
Asegúrese de comprender los componentes de la vista Regla. Para obtener más información, consulte Vista Regla.

Procedimiento

Realice los siguientes pasos para eliminar una regla**:**

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. En el panel **Reglas**, realice una de las siguientes acciones.
   - Seleccione una regla y haga clic en en la barra de herramientas Regla.
   - Haga clic en > **Eliminar**.

     Se muestra un cuadro de diálogo de confirmación.

     Nota: si una regla se usa en un informe, se muestra una advertencia que indica que la regla está en uso y no se puede eliminar.
3. Haga clic en **Sí** para eliminar la regla.

   Se muestra un mensaje que confirma la correcta eliminación de la regla y la regla seleccionada se elimina del panel Lista de reglas.

Eliminar un grupo de reglas

En este tema se proporcionan instrucciones para eliminar un grupo de reglas.

Requisitos previos

Asegúrese de comprender los componentes de la vista Regla. Para obtener más información, consulte Vista Regla.

Procedimiento

Realice los siguientes pasos para eliminar un grupo de reglas:

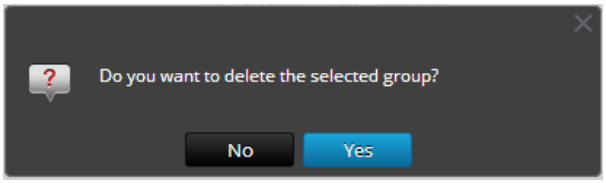
1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.

   Se muestra la pestaña Administrar.

2. En el panel **Grupos de reglas**, seleccione el grupo de reglas que desea eliminar.

3. Haga clic en .

   Se muestra un cuadro de diálogo de confirmación.



   Nota: Si una regla del grupo se usa en los informes, se muestra una advertencia que indica que la regla está en uso y no se puede eliminar.

4. Haga clic en **Sí** para eliminar el grupo.

   Se muestra un mensaje que confirma la correcta eliminación del grupo y el grupo seleccionado se elimina del panel Grupos de reglas.

Duplicar una regla

En este tema se proporcionan instrucciones para duplicar una regla.

Requisitos previos

Asegúrese de comprender los componentes de la vista Regla. Para obtener más información, consulte Vista Regla.

Procedimiento

Realice los siguientes pasos para duplicar una regla:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.

2. En el panel de lista **Reglas**, seleccione una regla que desee duplicar.

3. En la barra de herramientas Regla, haga clic en .

Editar una regla

En este tema se proporcionan instrucciones para editar una regla.

Requisitos previos

Asegúrese de que:

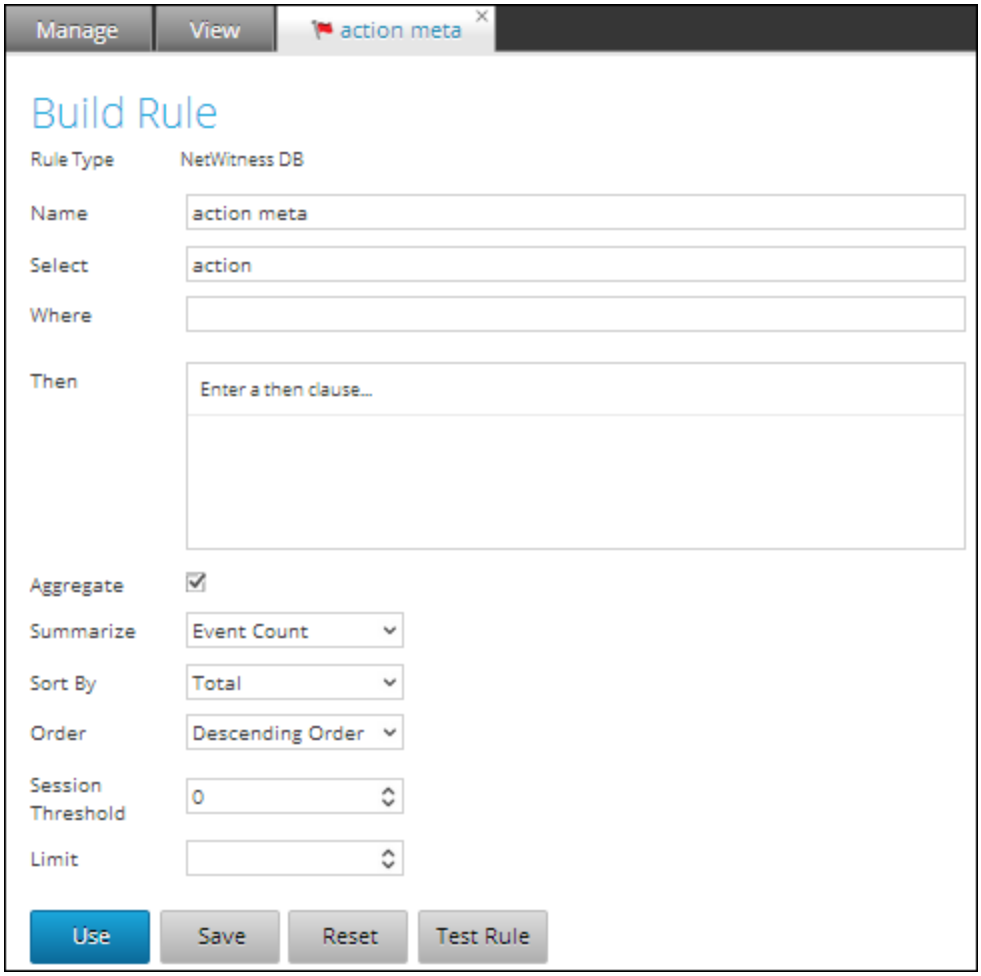
- Comprender los componentes de la vista Regla. Para obtener más información, consulte Vista Regla.
- Comprender los componentes de la vista Crear regla. Para obtener más información, consulte Vista Crear regla.

Procedimiento

Realice los siguientes pasos para editar una regla:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. En el panel de la lista **Reglas**, realice una de las siguientes acciones:
   - Seleccione una regla y haga clic en en la barra de herramientas Regla.
   - Haga clic en > **Editar**.

   Se muestra la pestaña de la vista Crear regla.



Nota: Si se edita una regla, la definición de la regla actualizada se aplica a los informes, gráficos y alertas donde se incluye la regla.

3. Modifique los campos obligatorios.
4. Haga clic en **Guardar**.
   Se muestra un mensaje de confirmación que indica que la regla se guardó correctamente.

Exportar una regla

En este tema se proporcionan instrucciones para exportar una regla. Solo puede exportar una regla por vez.

Requisitos previos

Asegúrese de:

- Tener reglas en el grupo de reglas.
- Comprender los componentes de la vista Regla. Para obtener más información, consulte Vista Regla.

Procedimiento

Realice los siguientes pasos para exportar una regla:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. En el panel de la lista **Reglas**, realice una de las siguientes acciones:
   - Seleccione una regla y haga clic en  > **Exportar** en la barra de herramientas Regla.
   - Haga clic en  > **Exportar**.

   Puede aparecer un cuadro de diálogo de exportación específico del navegador que permite abrir o guardar el archivo.

Nota: Si desea exportar múltiples reglas, puede hacerlo solo exportando grupos de reglas. Para obtener más información, consulte Exportar un grupo de reglas.

Exportar un grupo de reglas

En este tema se proporcionan instrucciones para exportar un grupo de reglas.

Requisitos previos

Asegúrese de:

- Tener reglas en el grupo de reglas.
- Comprender los componentes de la vista Regla. Para obtener más información, consulte Vista Regla.

Procedimiento

Realice los siguientes pasos para exportar un grupo de reglas:

1. En el menú de Security Analytics, haga clic en **Administration > Informes**.
   Se muestra la pestaña Administrar.
2. En el panel **Grupos de reglas**, seleccione el grupo de reglas que contiene las reglas que desea exportar.
3. Haga clic en  >**Exportar**.
   Puede aparecer un cuadro de diálogo de exportación específico del navegador que permite abrir o guardar el archivo.

Importar reglas y grupos de reglas

En este tema se proporcionan instrucciones para importar reglas y grupos de reglas. Puede importar reglas y grupos de reglas desde una instancia de Security Analytics en un árbol de reglas en el panel Grupos de reglas. Las reglas deben estar en un archivo binario válido que se haya exportado desde una instancia de Security Analytics. No puede importar reglas a un grupo de reglas. Los archivos importados se almacenan en una carpeta raíz, **Todos**.

Requisitos previos

Asegúrese de:

- Haber exportado las reglas o grupos de reglas desde una instancia de Security Analytics.
- Comprender los componentes de la vista Regla. Para obtener más información, consulte Vista Regla.

Procedimiento

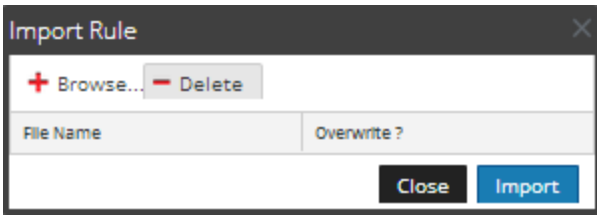
Realice los siguientes pasos para importar reglas o grupos de reglas:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.

2. Realice una de las siguientes acciones

   - En el panel Grupos de reglas, haga clic en  y seleccione **Importar**.
   - En la barra de herramientas Regla, haga clic en  y seleccione **Importar**.

     Se muestra el cuadro de diálogo **Importar regla**.



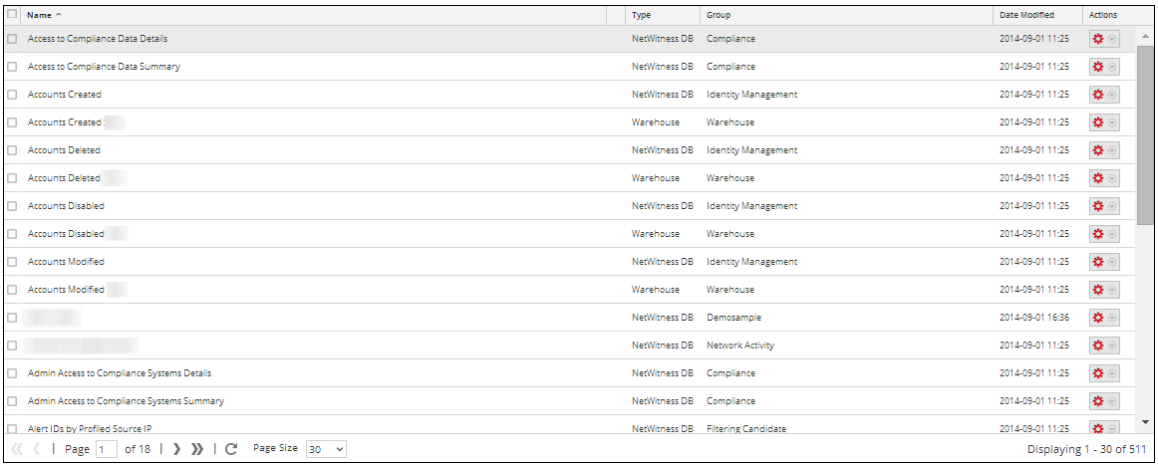
3. Haga clic en **Navegar** para navegar y seleccionar el archivo que contiene las reglas.
4. Haga clic en **Importar**.

> **Nota:** Durante el proceso de importación, Si hay una regla y una lista duplicada y no selecciona la opción para sobrescribir, se importan la regla y la lista y no se muestra un mensaje acerca de la duplicación de reglas y listas.

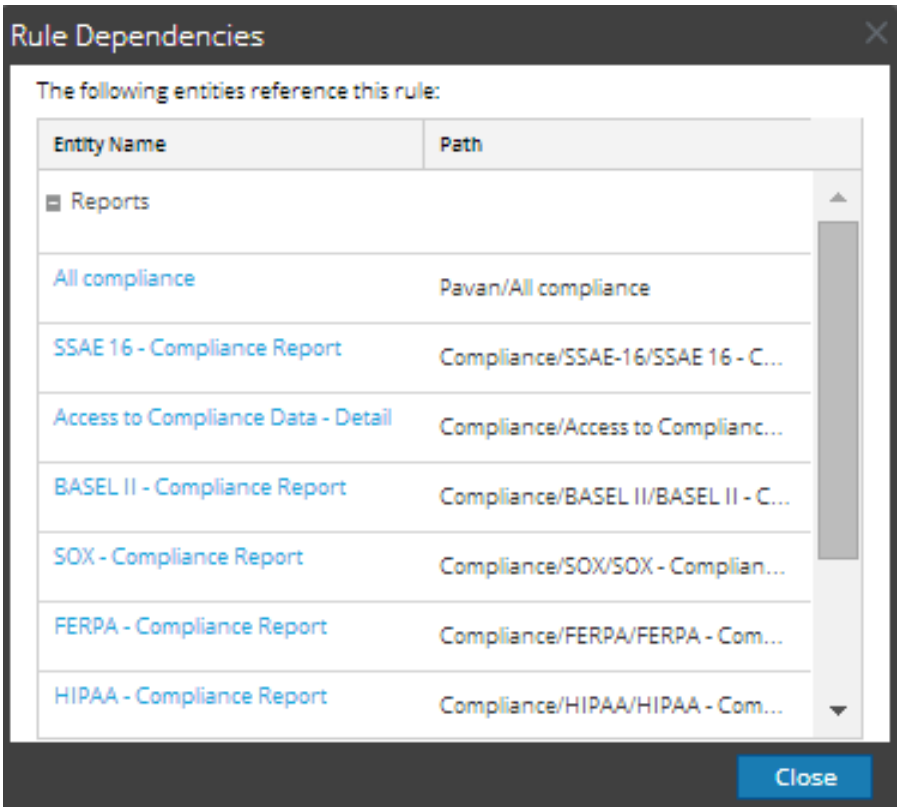
Ver dependientes de una regla

En este tema se proporcionan instrucciones para ver los dependientes de una regla. Debe recorrer una lista de reglas, seleccionar una regla para la cual desea identificar la dependencia de un informe, gráfico o alerta.

En la siguiente figura se muestra la vista Regla, donde se selecciona la regla “Acceso a los datos de cumplimiento de normas”.



En la siguiente figura se muestra la dependencia que tiene la regla de las alertas y los informes.



En la siguiente tabla se indican las diversas columnas del cuadro de diálogo Dependencias de regla y su descripción.

Columna	Descripción
Nombre de entidad	El nombre de la entidad que hace referencia a la regla.
Ruta	La ruta donde se encuentra la entidad en la interfaz del usuario.

Requisitos previos

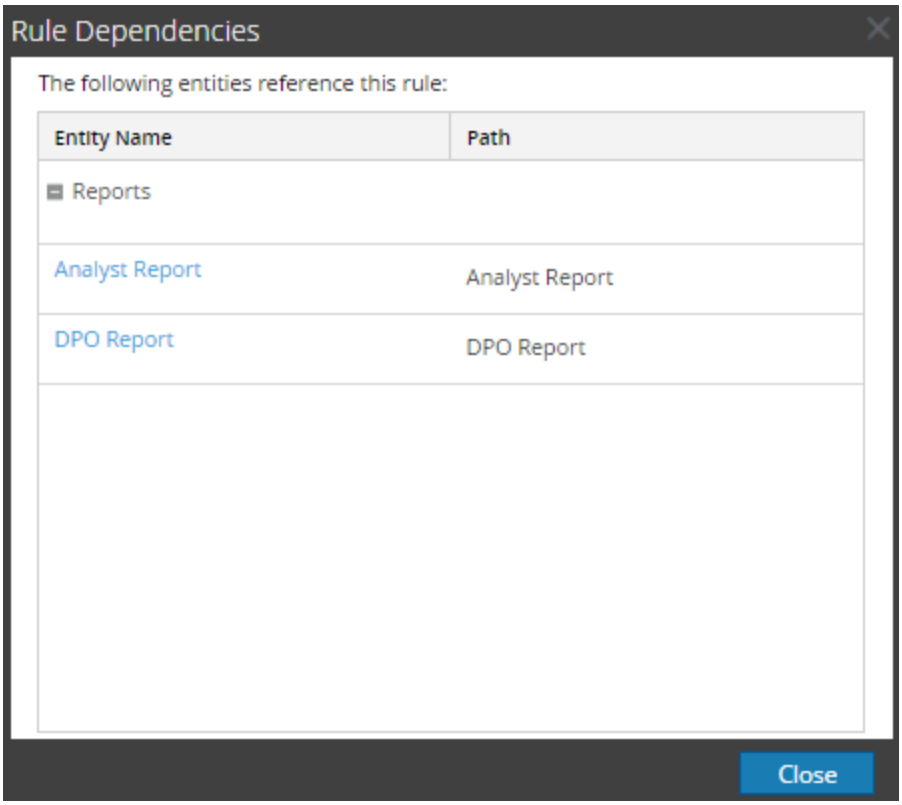
Asegúrese de comprender los componentes de la vista Regla. Para obtener más información, consulte Vista Regla.

Procedimiento

Realice los siguientes pasos para ver los dependientes de una regla:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.

2. Haga clic en **Rules**.
   Se muestra la vista Regla.
3. En el panel **Lista de reglas**, haga clic en  > **Dependientes**.
   Se muestra el cuadro de diálogo Dependencias de regla.



Los próximos pasos

Puede editar un informe, un gráfico o una alerta.

Administrar el acceso para una regla o un grupo de reglas

En este tema se describen los permisos de acceso que tendrá el usuario según la función del usuario para administrar una regla o un grupo de reglas. El módulo Reporting proporciona un control de acceso en el nivel de regla y grupo de reglas. Solo un usuario con el conjunto de permisos correcto puede ejecutar las tareas del módulo Reporting. El administrador administra el control de acceso desde la pestaña **Administration > Seguridad > Funciones**.

Cuando crea usuarios y funciones de usuario, el administrador debe asegurarse de que las funciones creadas para tareas específicas tengan acceso a todos los permisos más altos en la jerarquía de funciones.

Las reglas o los grupos de reglas se pueden vincular a un conjunto específico de funciones de usuario de modo que, cuando un usuario inicie sesión en Security Analytics, las únicas reglas a las que pueda acceder sean reglas accesibles al grupo al cual pertenece. Los usuarios que pertenecen a una función de usuario con el permiso de acceso "Lectura y escritura" tienen derechos de acceso completos para la regla. Además, el acceso se puede restringir de modo que solo accedan a las reglas quienes tengan el acceso de "Solo lectura".

Nota: Debe tener por lo menos el permiso de "Solo lectura" en un grupo para ver las reglas dentro de ese grupo.

En el nivel de la regla, puede establecer los siguientes permisos de acceso para las funciones de usuario en Security Analytics:

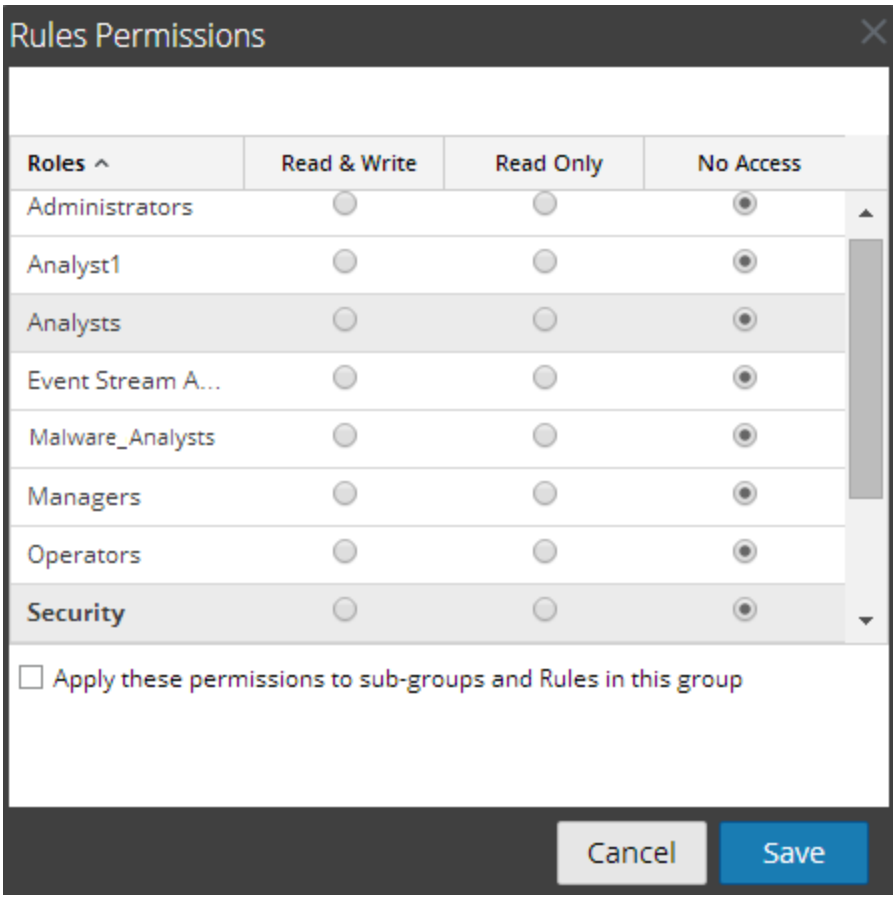
- Lectura y escritura
- Solo lectura
- Sin acceso

Suponga que desea que los **analistas de seguridad** tengan acceso a todas las reglas de un grupo de reglas. Para esto, puede configurar el permiso "**Lectura y escritura**" en el nivel del grupo de reglas. Y si no desea que la función **Operador** tenga acceso a un conjunto específico de reglas de un grupo de reglas, puede configurar el permiso "**Sin acceso**" en el nivel del grupo de reglas. El permiso se configura solo para el grupo de reglas, pero no para las reglas ni los subgrupos del grupo de reglas.

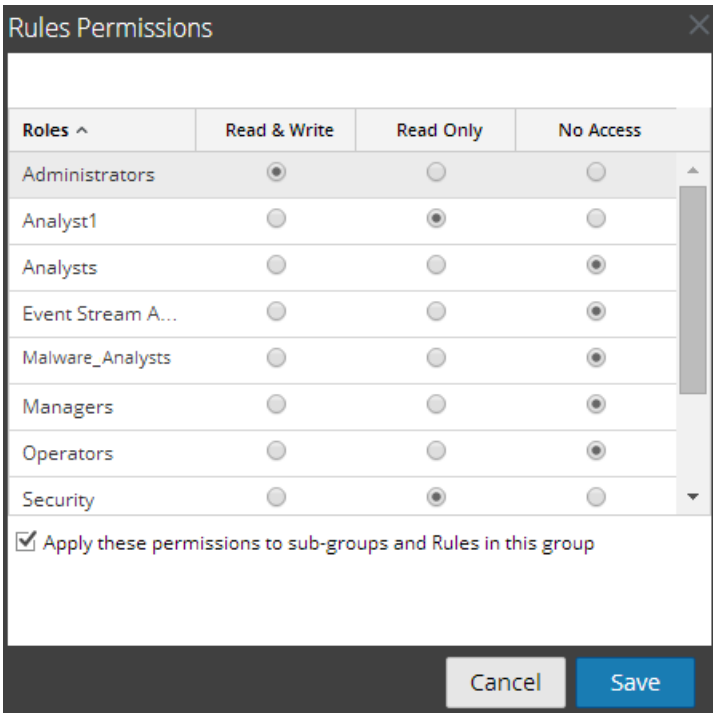
Control de acceso para un grupo de reglas

Cuando desea cambiar los permisos del grupo de reglas, debe seleccionar un grupo de reglas y configurar sus permisos de acceso en el panel Permisos de reglas.

Antes de aplicar permisos del grupo de reglas, el conjunto de permisos predeterminado configurado para todas las funciones de usuario es el permiso "Sin acceso" y las casillas de verificación están deseleccionadas.



Si desea cambiar el permiso de acceso para una función de usuario específica, debe configurarlo en el nivel del grupo de reglas, como se muestra en la figura. Suponga que desea que los **administradores** tengan acceso a todas las reglas de un grupo de reglas. Para esto, puede configurar el permiso "**Lectura y escritura**" en el panel Permisos de grupo de reglas.



También puede aplicar permisos a los subgrupos y a las reglas del grupo si selecciona la casilla de verificación.

Los dos escenarios se explican de forma resumida:

- Escenario 1: Permisos aplicados a grupo de reglas/subgrupo/reglas según la función de usuario.
- Escenario 2:Permisos aplicados a subgrupo y reglas del grupo.

Función (analistas)	Permisos aplicados a grupo de reglas/subgrupo/reglas según la función de usuario	Permisos aplicados a subgrupo y reglas del grupo
Grupo	**Lectura y escritura**	**Lectura y escritura**
Subgrupo	**Lectura**	**Lectura y escritura: heredados**
Reglas	**Lectura**	**Lectura y escritura: heredados**

Los permisos de acceso que configura se pueden aplicar a subgrupos y objetos secundarios de este grupo.

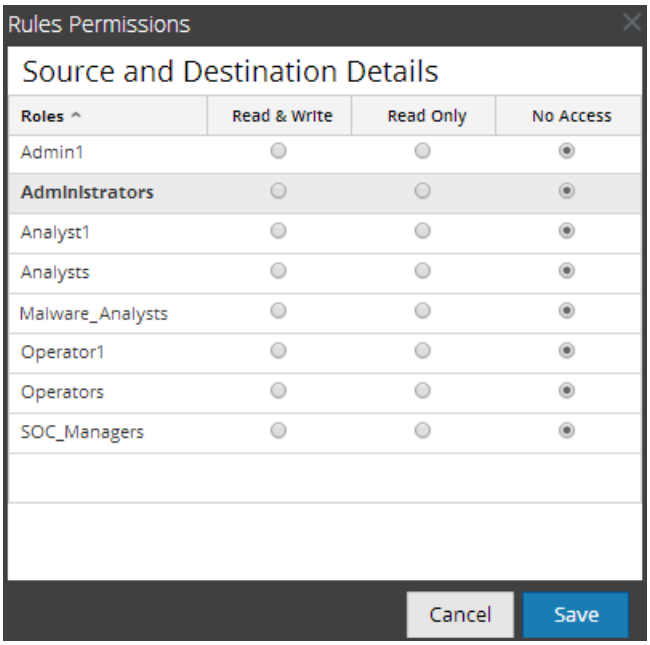
Al grupo de reglas se asignará la función de un **analista de seguridad** y los permisos se configuran en **Lectura y escritura** para el grupo de reglas.

En el escenario 1, cada uno de los niveles tendrá un permiso configurado de acuerdo con la función del usuario. En el escenario 2, el subgrupo y las reglas del grupo heredarán el permiso en el nivel del grupo de reglas.

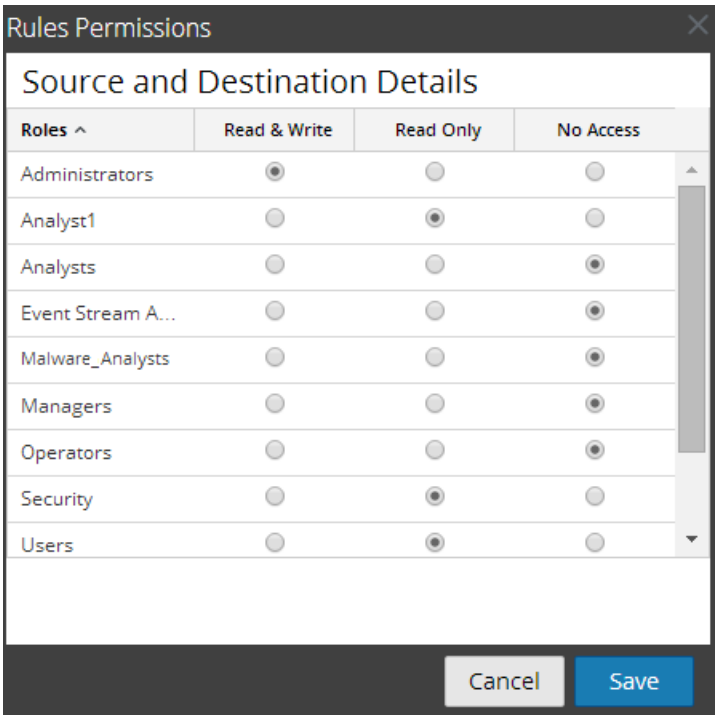
Control de acceso para una regla

Cuando desea cambiar los permisos de reglas, debe seleccionar una regla y configurar sus permisos de acceso en el panel Permisos de reglas.

Antes de aplicar permisos de reglas, el conjunto de permisos predeterminado para todas las funciones de usuario es el permiso “Sin acceso” y la casilla de verificación está deseleccionada.



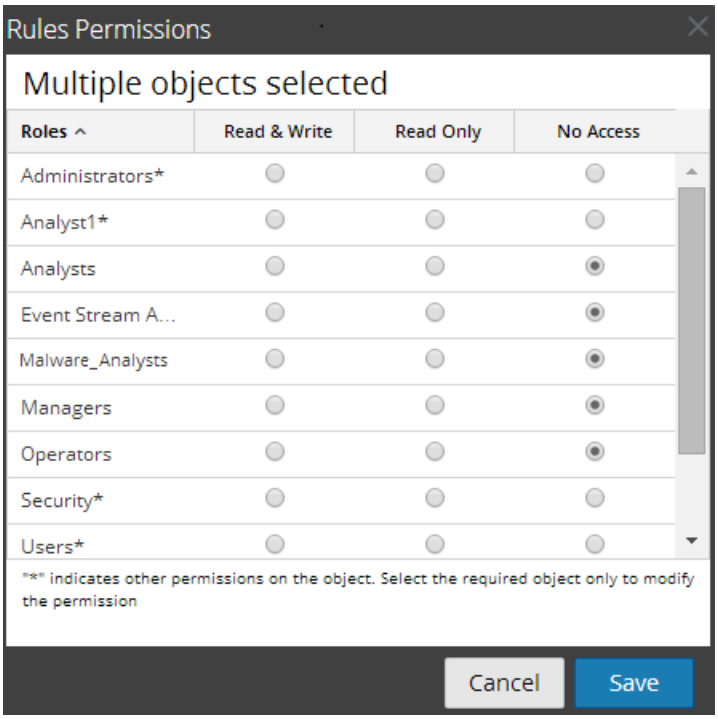
Si desea cambiar el permiso de acceso para una función de usuario específica, debe configurarlo en el nivel de regla, como se muestra en la figura. Suponga que desea que los **administradores** tengan acceso a una regla específica. Para esto, puede configurar el permiso “**Lectura y escritura**” en el panel Permisos de reglas.



Control de acceso para una regla cuando se seleccionan múltiples reglas

Cuando desea cambiar los permisos de múltiples reglas, puede seleccionar simultáneamente varias reglas y configurar sus permisos de acceso en el panel Permisos de reglas. El permiso de acceso que elige se aplica a todas las reglas seleccionadas.

Nota: El carácter "*" junto al nombre de función indica que hay otros permisos disponibles en la función de usuario. Si desea cambiar el permiso de acceso para la función de usuario requerida, seleccione la función de usuario y cambie el permiso de acceso.

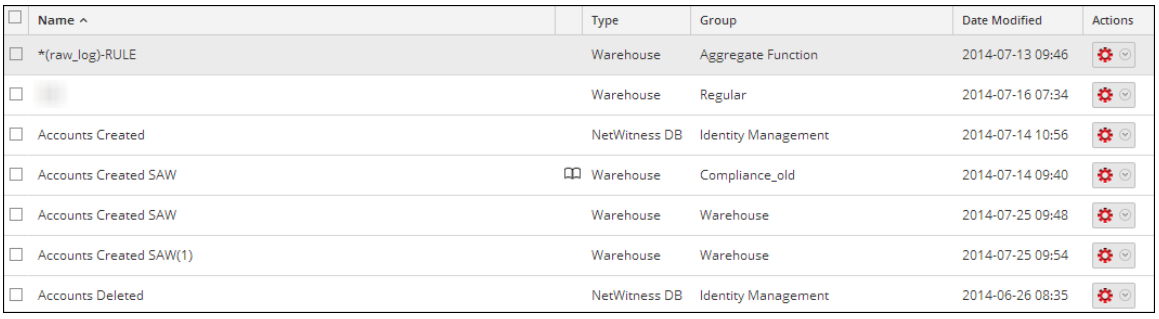


Inicie sesión como un usuario específico y vea los detalles de acceso

Cuando inicia sesión en la interfaz del usuario de Security Analytics como un usuario que tiene el permiso "Acceso de lectura", todas las reglas se marcan con el símbolo (📖) y, cuando hace clic en el símbolo, se muestra la leyenda "Solo lectura" en el panel Lista de reglas.

Cuando inicia sesión en la interfaz del usuario de Security Analytics como un usuario que no tiene el permiso de acceso "Lectura y escritura" en una regla, todas las reglas se marcan con el símbolo (👁) y aparecen en gris en el panel Lista de reglas.

En la siguiente figura se muestra el panel Lista de reglas cuando se inicia sesión con un permiso de acceso de "Lectura y escritura" mínimo.



Nota: Si un usuario (distinto del administrador) crea una regla, el administrador no puede acceder a ella.

Lista tabular

En la siguiente tabla se indican las diversas columnas del panel Permisos de reglas:

Columna	Descripción
Funciones	La función del usuario que inició sesión en la interfaz del usuario de Security Analytics.
Lectura y escritura	El usuario puede acceder, ver, editar, eliminar, importar y exportar reglas en la vista Reglas. El usuario también puede cambiar el permiso en la regla.
Solo lectura	El usuario solo puede acceder a la regla y verla en la vista Reglas
Sin acceso	El usuario no puede acceder a una regla ni verla cuando tiene configurado este permiso.

Temas

- Establecer el control de acceso para un informe
- Establecer el control de acceso para un grupo de informes

Establecer el control de acceso para una regla

En este tema se proporcionan instrucciones para establecer el control de acceso para una regla. El módulo Reporting proporciona un control de acceso en el nivel de reglas. Solo un usuario con el conjunto de permisos correcto puede ejecutar las tareas de la regla. Cuando el administrador crea usuarios y funciones, debe asegurarse de que las funciones creadas para tareas específicas tengan acceso a todos los permisos más altos en la jerarquía de funciones.

En el nivel de la regla, puede establecer los siguientes permisos de acceso para las funciones de usuario en Security Analytics:

- Lectura y escritura: Ver o editar las reglas del grupo de reglas.
- Solo lectura. ver las reglas del grupo de reglas.
- Sin acceso: las reglas del grupo de reglas no se pueden ver ni editar.

Requisitos previos

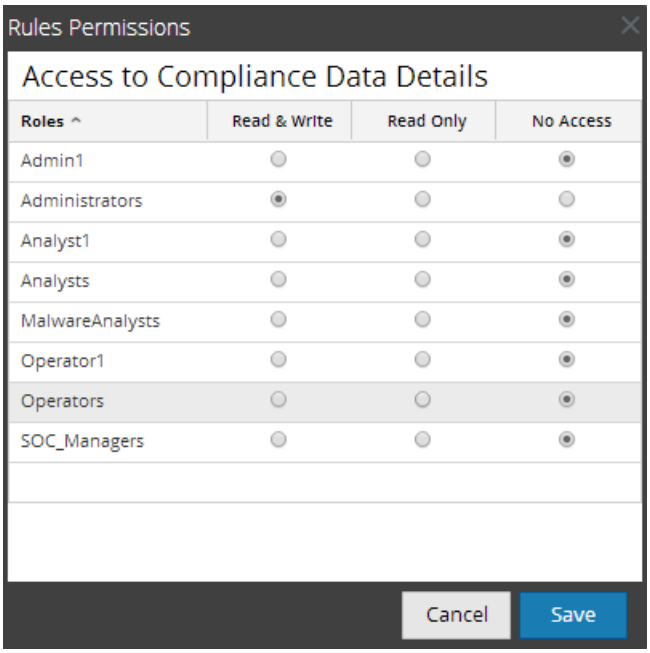
Asegúrese de:

- Haber comprendido los componentes de la vista Regla. Para obtener más información, consulte Vista Regla.
- Tener un permiso de acceso de “Lectura y escritura” mínimo para establecer permisos de acceso para una regla.

Procedimiento

Realice los siguientes pasos para establecer el control de acceso para una regla:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. En el panel **Lista de reglas**, seleccione la regla.
3. Haga clic en  > **Permisos** en la barra de herramientas Regla.
   Aparece el cuadro de diálogo **Permisos de reglas**.



4. Seleccione el permiso de acceso apropiado siguiente para la función de usuario y haga clic en **Guardar**.
   - Lectura y escritura
   - Solo lectura
   - Sin acceso

Establecer el control de acceso para un grupo de reglas

En este tema se proporcionan instrucciones para establecer el control de acceso en el nivel del grupo de reglas. Solo un usuario con el conjunto de permisos correcto puede ejecutar las tareas en la regla. Cuando el administrador crea usuarios y funciones, debe asegurarse de que las funciones creadas para tareas específicas tengan acceso a todos los permisos más altos en la jerarquía de funciones.

En el nivel del grupo de reglas, puede establecer los siguientes permisos de acceso para las funciones de usuario en Security Analytics:

- Lectura y escritura: Ver o editar las reglas del grupo de reglas.
- Solo lectura. ver las reglas del grupo de reglas.
- Sin acceso: la regla de los grupos de reglas no se puede ver ni editar.

Requisitos previos

Asegúrese de:

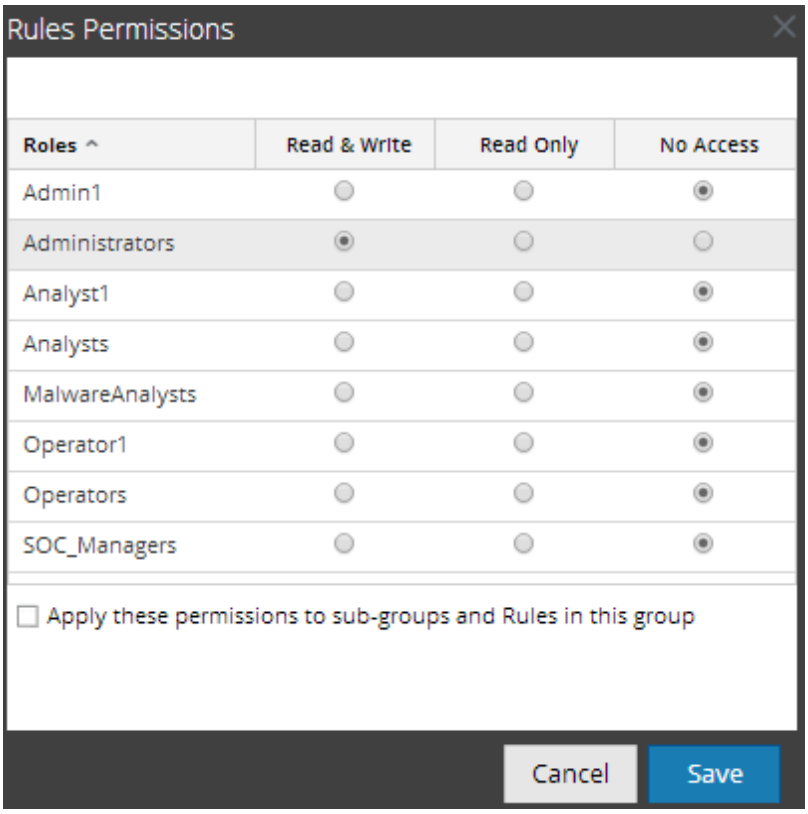
- Haber comprendido los componentes de la vista Regla. Para obtener más información, consulte Vista Regla.
- Tener un permiso de acceso de “Lectura y escritura” mínimo para establecer permisos de acceso para un grupo de reglas.

Procedimiento

Realice los siguientes pasos para establecer el control de acceso para un grupo de reglas:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. En el panel **Grupos de reglas**, seleccione el grupo de reglas y realice una de las siguientes acciones:
   - Haga clic en  y seleccione **Permisos**.
   - Haga clic con el botón secundario en el grupo de reglas seleccionado y elija **Permisos**.

   Aparece el cuadro de diálogo **Permisos de reglas**.



3. (Opcional) Seleccione la casilla de verificación correspondiente para aplicar estos permisos a subgrupos y objetos secundarios de este grupo.
4. Haga clic en **Guardar**.
   Se muestra un mensaje de confirmación que indica que el permiso se estableció correctamente para el grupo de reglas seleccionado.

Crear un gráfico mediante una regla

En este tema se proporcionan instrucciones para crear un gráfico mediante una regla.

Requisitos previos

Asegúrese de que:

- Comprender los componentes de la vista Regla. Para obtener más información, consulte Vista Regla.
- Comprender los componentes de la vista Crear regla. Para obtener más información, consulte Vista Crear regla.

Procedimiento

Ejecute los siguientes pasos para crear un gráfico:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Realice una de las siguientes acciones
   - Puede crear un gráfico mediante una regla cuando crea o edita la regla. Para obtener más información, consulte Definir una regla y Editar una regla.
     realice lo siguiente:
     1. En la vista **Crear regla**, haga clic en **Usar**.
        Se muestra el cuadro de diálogo Usar regla.
     2. Haga clic en **Gráfico**.
     3. Haga clic en **Seleccionar**.
   - Seleccione una regla en el panel Lista de reglas y haga clic en  en la barra de herramientas Regla. En el menú desplegable, seleccione **Usar** > **Gráfico**.
   - En el panel Lista de reglas, haga clic en  > **Crear gráfico**.

     Nota: Si la regla contiene la acción de regla lookup_and_add, sum_count o sum_values, el gráfico asociado no incluirá datos.

     Para obtener más información acerca de la definición de gráficos, consulte Descripción general de un gráfico.

Crear un informe mediante una regla

En este tema se proporcionan instrucciones para crear un informe mediante una regla. Cuando crea un informe mediante una regla, se crea el informe predeterminado con esta única regla. Puede editar aún más el informe para agregar más reglas.

Requisitos previos

Asegúrese de que:

- Comprender los componentes de la vista Regla. Para obtener más información, consulte Vista Regla.
- Comprender los componentes de la vista Crear regla. Para obtener más información, consulte Vista Crear regla.

Procedimiento

Realice los siguientes pasos para crear un informe mediante una regla:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Realice una de las siguientes acciones
   - Puede crear un informe mediante una regla cuando crea o edita la regla. Para obtener más información, consulte Definir una regla y Editar una regla.
     realice lo siguiente:

     a. En la vista **Crear regla**, haga clic en **Usar**.
        Se muestra el cuadro de diálogo Usar regla.
     b. Haga clic en **Informe**.
     c. Seleccione **Nuevo informe** o **Informe existente** en función del requisito.
     d. Haga clic en **Seleccionar**.
   - Seleccione una regla en el panel Lista de reglas y haga clic en  en la barra de herramientas Regla. En el menú desplegable, seleccione **Usar** > **Informe**.
   - En el panel Lista de reglas, haga clic en  > **Crear informe**.

Nota: Se pueden usar reglas personalizadas para crear un informe y si la vista para la regla se selecciona como “Área” o “Circular”, se abre una ventana para las entradas **Eje X** y **Eje Y**. De manera predeterminada, solo puede seleccionar los primeros metadatos en **Eje X**.

Para obtener más información acerca de la definición de informes, consulte Descripción general de un informe.

Crear una alerta mediante una regla

En este tema se proporcionan instrucciones para crear una alerta mediante una regla. No puede crear una alerta mediante reglas de IPDB y Warehouse.

Requisitos previos

Asegúrese de que:

- Comprender los componentes de la vista Regla. Para obtener más información, consulte Vista Regla.
- Comprender los componentes de la vista Crear regla. Para obtener más información, consulte Vista Crear regla.

Procedimiento

Realice los siguientes pasos para crear una alerta mediante una regla:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Realice una de las siguientes acciones
   - Puede crear una alerta mediante una regla cuando crea o edita la regla. Para obtener más información, consulte Definir una regla y Editar una regla.
     Siga los pasos que se detallan a continuación:

     a. En la vista **Crear regla**, haga clic en **Usar**.
        Se muestra el cuadro de diálogo Usar regla.
     b. Haga clic en **Alerta**.
     c. Haga clic en **Seleccionar**.
   - Seleccione una regla en el panel Lista de reglas y haga clic en  en la barra de herramientas Regla. En el menú desplegable, seleccione **Usar** > **Alerta**.
   - Haga clic en  > **Crear alerta**.

     Para obtener más información acerca de la definición de alertas, consulte Descripción general de una alerta.

Descripción general de un informe

En este tema se proporciona una descripción breve de un informe. Un informe es una combinación de reglas y otros objetos de formato, como encabezados y notas con formato HTML, que describen e identifican los datos relacionados con un área de interés en especial. Los informes se definen y administran en la página Crear informe y se pueden programar para ejecutarse de forma ad hoc u oportuna. Una vez que se ejecuta un informe, los resultados se almacenan de manera central y se pueden enviar automáticamente por correo electrónico, SFTP, URL y NFS a los usuarios; se pueden ver mediante la interfaz web de SA y descargar como archivos PDF y CSV.

Un informe consta de lo siguiente:

Propiedad	Descripción	Ejemplo
Nombre de informe **Nota:** En el campo **Nombre**, el ícono para expandir el tamaño de la columna no se muestra al final del campo de la columna. Debe mover el mouse un poco hacia la izquierda para ver el ícono que permite ampliar la columna.	Se utiliza para identificar el informe con el fin de calendarizarlo posteriormente.	Report1
Texto	Campos de texto predefinidos que se utilizan dentro de un informe para hacer que el informe sea más significativo para el usuario.	Header1, Comment
Reglas	Las reglas (consultas) utilizadas para crear un informe.	select user.dst where ip.src = 10.10.10.1

Nota: En la interfaz del usuario de Reporting, la fecha o la hora mostradas siempre están de acuerdo con el perfil de zona horaria que seleccionó el usuario.

Definir grupos de informes e informes

Este tema es un conjunto de tareas para configurar grupos de informes e informes. Puede definir, eliminar, editar, importar y exportar grupos y listas de informes en Security Analytics. Cada tema describe los procedimientos pertinentes

Temas:

- Agregar un informe
- Agregar un grupo de informes
- Eliminar un informe
- Eliminar un grupo de informes
- Duplicar un informe
- Editar un informe
- Exportar un informe
- Exportar un grupo de informes
- Importar informes y grupos de informes
- Actualizar una lista de grupos o informes
- Ver una lista de todos los informes
- Ver un informe

Agregar un informe

En este tema se proporcionan instrucciones para agregar informes.

Requisitos previos

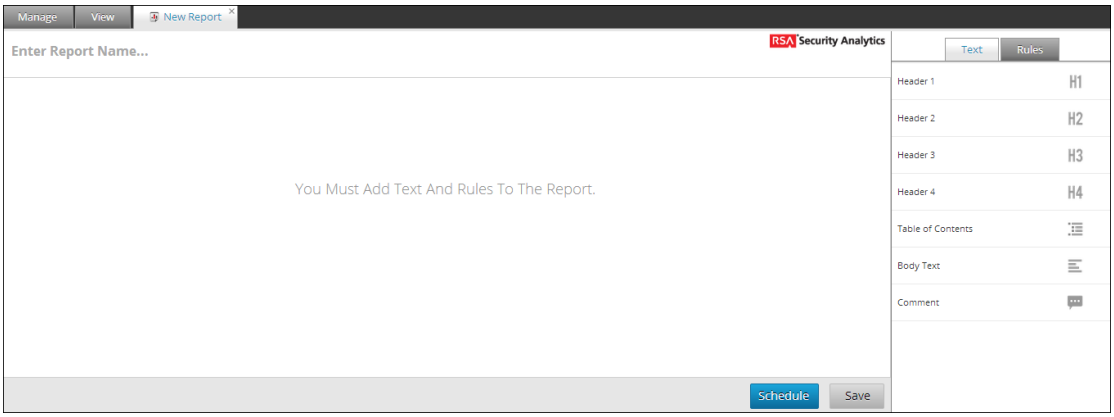
Asegúrese de:

- Haber definido reglas antes de agregar un informe.
- Haber comprendido los componentes de la vista Informe. Para obtener más información, consulte Vista Informe.
- Haber comprendido los componentes de la vista Crear un informe. Para obtener más información, consulte Vista Crear informe.

Procedimiento

Realice los siguientes pasos para agregar informes a un grupo o a un subgrupo desde el panel Informe:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Informes**.
   Se muestra la vista Informe.
3. En la barra de herramientas **Informe**, haga clic en +.
   Aparece la pestaña Crear informe.



4. Ingrese el nombre del informe.
5. Arrastre y suelte el texto y reglas al informe.

   Nota: el texto ingresado es opcional y tal vez necesite esta opción únicamente cuando desee mostrar encabezados o contenido definidos por el usuario.

6. Haga clic en **Guardar**.
   Se muestra un mensaje de confirmación que indica que el informe se guardó correctamente.

Los próximos pasos

Realice las siguientes tareas:

1. Puede editar, eliminar o actualizar un informe en el panel Informe.
2. Puede programar un informe en la vista Requisitos previos .

Agregar un grupo de informes

En este tema se proporcionan instrucciones para agregar grupos a la carpeta predeterminada o agregar subgrupos bajo un grupo de informes.

Requisitos previos

Asegúrese de haber comprendido los componentes de la vista Informe. Para obtener más información, consulte Vista Informe.

Procedimiento

Realice los siguientes pasos para agregar grupos a la carpeta predeterminada o agregar subgrupos bajo un grupo de informes:

1. En el menú de **Security Analytics**, seleccione **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Informes**.
   Se muestra la vista Informe.
3. En el panel **Grupos de informes**, haga clic en  .
   Se agrega un grupo predeterminado al panel Grupos de informes.
4. Ingrese el nombre del nuevo grupo.
5. Presione **Intro**.
   El grupo se agrega al panel Grupos de informes.

Los próximos pasos

Puede agregar informes al grupo de informes.

Eliminar un informe

Esta sección proporciona instrucciones para eliminar informes en un grupo o subgrupo.

Requisitos previos

Asegúrese de haber comprendido los componentes de la vista Informe. Para obtener más información, consulte Vista Informe.

Procedimiento

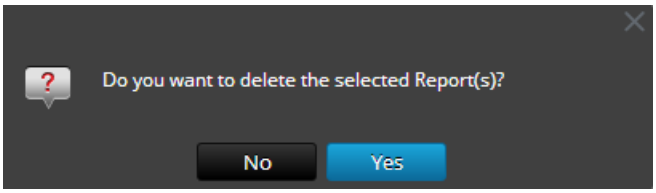
Realice los siguientes pasos para eliminar informes de un grupo o subgrupo desde el panel Lista de informes:

1. En el menú de **Security Analytics**, seleccione **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Informes**.
   Se muestra la vista Informe.

3. En el panel **Lista de informes**, realice una de las siguientes acciones:

   - Seleccione los informes y haga clic en .
   - Haga clic en >**Eliminar**.

     Se muestra un cuadro de diálogo de confirmación:



4. Haga clic en **Sí** para eliminar el informe.

   Se muestra un mensaje que confirma la correcta eliminación del informe y el informe seleccionado se elimina del panel Lista de informes.

Eliminar un grupo de informes

En este tema se proporcionan instrucciones para eliminar grupos de informes de la carpeta predeterminada o subgrupos bajo un grupo de informes.

Requisitos previos

Asegúrese de:

- Que no haya informes asociados al grupo de informes.
- Haber comprendido los componentes de la vista Informe. Para obtener más información, consulte Vista Informe.

Procedimiento

Realice los siguientes pasos para eliminar grupos de informes de la carpeta predeterminada o subgrupos bajo un grupo de informes:

1. En el menú de **Security Analytics**, seleccione **Administration** > **Informes**.

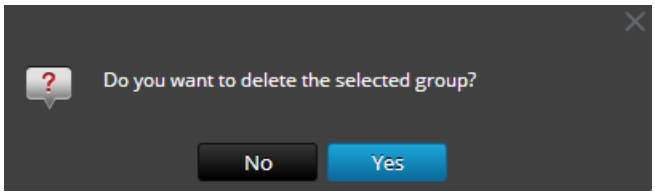
   Se muestra la pestaña Administrar.

2. Haga clic en **Informes**.

   Se muestra la vista Informe.

3. En el panel **Grupos de informes**, seleccione el grupo de informes y haga clic en .

   Se muestra un cuadro de diálogo de confirmación.



4. Haga clic en **Sí** para eliminar el grupo.
   Se muestra un mensaje que confirma la correcta eliminación del grupo y el grupo seleccionado se elimina del panel Grupos de informes.

Duplicar un informe

En este tema se proporcionan instrucciones para duplicar un informe con el fin de programar múltiples programas de informes y programar el mismo informe. El informe duplicado se muestra en el panel Lista de informes con sufijos. Por ejemplo, informe (1).

En general, la opción duplicada se utiliza en dos escenarios:

- Desea hacer una copia del informe, para transferir el mismo informe a otro grupo.
- Desea conservar la mayor parte de los ajustes de configuración para un objeto y modificar algunos de estos ajustes.
  Por ejemplo, cuando tiene una consulta compleja en una o en varias reglas en un informe, es muy útil utilizar la opción de duplicación.

Requisitos previos

Asegúrese de haber comprendido los componentes de la vista Informe. Para obtener más información, consulte Vista Informe.

Procedimiento

Realice los siguientes pasos para duplicar un informe existente:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Informes**.
   Se muestra la vista Informe.
3. En el panel **Lista de informes**, seleccione un informe que desee duplicar y haga clic en .
   El informe se guarda correctamente y se agrega a la lista de informes.

Los próximos pasos

Puede transferir a otro grupo el informe duplicado.

Editar un informe

En este tema se proporcionan instrucciones para editar informes en un grupo o un subgrupo.

Requisitos previos

- Haber comprendido los componentes de la vista Informe. Para obtener más información, consulte Vista Informe.
- Haber comprendido los componentes de la vista Crear un informe. Para obtener más información, consulte Vista Crear informe.

Procedimiento

Realice los siguientes pasos para editar informes en un grupo o subgrupo desde el panel Lista de informes:

1. En el menú de **Security Analytics**, seleccione **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Informes**.
   Se muestra la vista Informe.
3. En el panel **Lista de informes**, realice una de las siguientes acciones:
   - Seleccione un informe y haga clic en  .
   - Haga clic en  > **Editar**.

   Aparece la pestaña de la vista Crear informe.

4. Modifique el texto y agregue más reglas al informe (si es necesario).
5. Haga clic en **Guardar**.
   Se muestra un mensaje de confirmación que indica que el informe se guardó correctamente.

Exportar un informe

En este tema se proporcionan instrucciones para exportar informes seleccionados a un archivo externo que luego se puede importar en otro ambiente de Security Analytics.

Requisitos previos

Asegúrese de:

- Tener informes en el grupo de informes.
- Haber comprendido los componentes de la vista Informe. Para obtener más información, consulte Vista Informe.

Procedimiento

Realice los siguientes pasos para exportar informes seleccionados en el panel Grupos de informes a un archivo externo:

1. En el menú de **Security Analytics**, seleccione **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Informes**.
   Se muestra la vista Informe.
3. En el panel **Lista de informes**, realice una de las siguientes acciones:
   - Seleccione un informe y haga clic en  > **Exportar**.
   - Haga clic en  > **Exportar**.

   El archivo exportado se guarda en la unidad local en formato archivado.

Abrir archivos CSV con caracteres Unicode en MS Excel

Para abrir archivos CSV descargados que contienen caracteres Unicode en MS Excel, siga estos pasos:

1. Descargue y guarde un archivo CSV.
2. Abra Microsoft Excel y navegue hasta la pestaña **Datos**.
3. Haga clic en el elemento de menú **Desde texto**, busque el archivo CSV que descargó y haga clic en **Importar**.
   Se muestra el asistente Importar texto.

4. Seleccione el tipo de datos **Delimitado** o **Ancho fijo** desde el botón de opción **Tipo de datos original**.
5. Haga clic en la lista desplegable **Origen del archivo**, seleccione **65001: Unicode (UTF-8)** y haga clic en **Siguiente**.
6. Seleccione el delimitador que se usó en el archivo que importó y haga clic en **Siguiente**.
7. Seleccione el formato de datos para cada columna de datos que desea importar y haga clic en **Finalizar**.
   Se muestra el resultado correcto en una hoja de MS Excel.

Exportar un grupo de informes

En este tema se proporcionan instrucciones para exportar grupos de informes seleccionados a un archivo externo que pueda importarse posteriormente a otro ambiente de Security Analytics.

Requisitos previos

Asegúrese de:

- Tiene informes en el grupo de informes.
- Haber comprendido los componentes de la vista Informe. Para obtener más información, consulte Vista Informe.

Procedimiento

Realice los siguientes pasos para exportar grupos de informes seleccionados en el panel Grupos de informes a un archivo externo:

1. En el menú de **Security Analytics**, seleccione **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Informes**.
   Se muestra la vista Informe.
3. En el panel **Grupos de informes**, seleccione un grupo de informes y haga clic en  > **Exportar**.
   El archivo exportado se guarda en la unidad local.

Importar informes y grupos de informes

En este tema se proporcionan instrucciones para importar grupos que contienen subgrupos e informes de otras instancias de Security Analytics en el panel Grupos de informes. Los informes deben estar en un archivo binario válido que se haya exportado desde otra instancia de Security Analytics.

Durante el proceso de importación, debe seleccionar el archivo binario y especificar si los informes existentes se deben sobrescribir con informes del mismo nombre incluidos en el archivo binario de importación.

- Si decide sobrescribirlos, todas las reglas, las listas y los informes duplicados se sobrescribirán con el contenido del archivo binario de importación.
- Si decide no sobrescribirlos y existe una regla, una lista o un informe duplicados en la carpeta objetivo, la importación falla y se muestra un mensaje acerca de los informes duplicados.

No puede importar informes a un grupo de informes específico. Los archivos importados se almacenan en la carpeta raíz **All**.

Requisitos previos

Asegúrese de:

- Disponer de informes o grupos de informes exportados desde otras instancias de Security Analytics.
- Haber comprendido los componentes de la vista Informe. Para obtener más información, consulte Vista Informe.

Procedimiento

Realice los siguientes pasos para importar grupos que contienen subgrupos e informes de otras instancias de Security Analytics en el panel Grupos de informes:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Informes**.
   Se muestra la vista Informe.
3. En el panel **Grupos de informes**, seleccione una carpeta para importar el archivo.
4. Realice una de las siguientes acciones

   - En el panel **Grupos de informes**, haga clic en  > **Importar** para importar un grupo.

- En la barra de herramientas **Informe**, haga clic en  > **Importar** para importar un informe.
  Se muestra el cuadro de diálogo Importar informe.

5. Haga clic en **Navegar** para seleccionar el archivo binario.
   Security Analytics proporciona una vista del sistema de archivos de los archivos.
6. Busque el archivo binario y haga clic en **Abrir**.
   El archivo se agrega a la lista Importar informe.
7. (Opcional) Para sobrescribir cualquier regla existente en la biblioteca con una regla de nombre idéntico en el archivo binario cuando se realiza la importación, seleccione la casilla de verificación **Regla**. Si no selecciona la opción Sobrescribir y se encuentra una regla idéntica en el archivo binario, este archivo se importa y no se muestra ningún mensaje de error.
8. (Opcional) Para sobrescribir cualquier lista existente en la biblioteca con una lista de nombre idéntico en el archivo binario, seleccione la casilla de verificación **Lista**. Si no selecciona la opción Sobrescribir y se encuentra una lista idéntica en el archivo binario, este archivo se importa y no se muestra ningún mensaje de error.
9. (Opcional) Para sobrescribir cualquier informe existente en la biblioteca con un informe de nombre idéntico en el archivo binario cuando se realiza la importación, seleccione la casilla de verificación **Informe**. Si no selecciona la opción Sobrescribir y se encuentra un informe idéntico en el archivo binario, este archivo se importa y no se muestra ningún mensaje de error.
10. Haga clic en **Importar** para importar el archivo binario.

Actualizar una lista de grupos o informes

En este tema se proporcionan instrucciones sobre cómo actualizar un grupo de informes o informes individuales para ver la nueva disposición de grupos o informes.

Requisitos previos

Asegúrese de haber comprendido los componentes de la vista Informe. Para obtener más información, consulte Vista Informe.

Procedimiento

Realice los siguientes pasos para actualizar un grupo de informes o informes individuales:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.

2. Haga clic en **Informes**.
   Se muestra la vista Informe.
3. Haga lo siguiente para transferir el grupo o los informes a una nueva ubicación:
   - En el panel **Grupos de informes**, arrastre y suelte el grupo.
   - En el panel **Lista de informes**, arrastre y suelte los informes en el grupo deseado del panel Grupos de informes.
     El grupo de informes se transfiere a la ubicación nueva.
4. Haga lo siguiente para actualizar un grupo o una lista de informes:
   - En el panel **Grupos de informes**, haga clic en  .
     El grupo de informes se actualiza.
   - En el panel **Lista de informes**, haga clic en  .
     La lista de informes se actualiza.

Ver una lista de todos los informes

En este tema se proporcionan instrucciones para ver una lista de todos los informes.

Requisitos previos

Asegúrese de:

- Haber comprendido los componentes de la vista Informe. Para obtener más información, consulte Vista Informe.
- Haber comprendido los componentes del panel Ver todos los informes. Para obtener más información, consulte Panel Ver todos los informes.

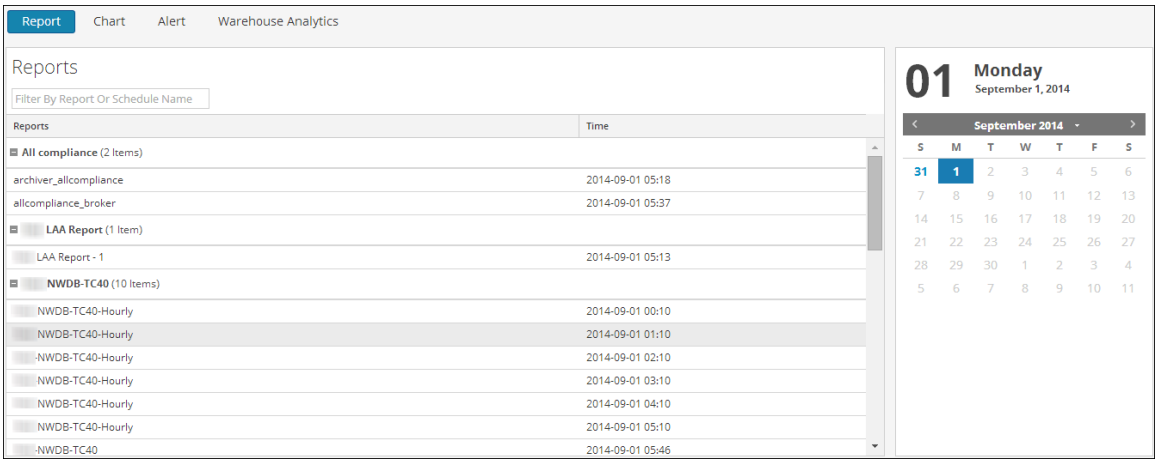
Procedimiento

Realice los siguientes pasos para ver una lista de todos los informes:

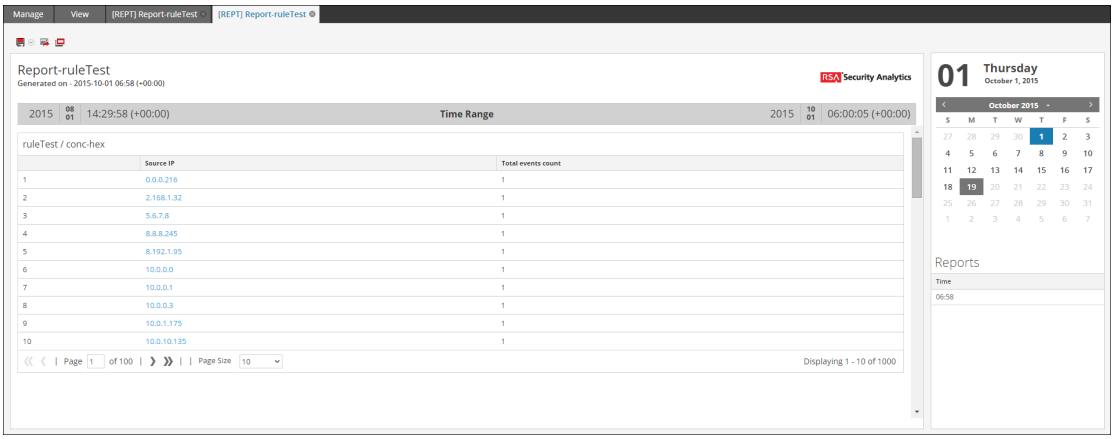
1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña **Administrar**.

2. Haga clic en **Informes**.
   Se muestra la vista Informe.
3. En el panel **Informe**, haga clic en **Ver todos los informes**.
   En la pestaña Ver se muestra una lista de todos los informes junto con el nombre del calendario y la hora.

Nota: Si no se muestra ninguna lista, seleccione una fecha del calendario para ver una lista de informes para esa fecha.



4. Haga clic en un informe programado e imprímalo, guárdelo como PDF/CSV, envíe notificaciones por correo electrónico o véalo en pantalla completa.



Los próximos pasos

Realice las siguientes tareas:

1. Puede imprimir, guardar, enviar por correo electrónico y ver informes en pantalla completa.
2. También puede seleccionar una fecha del calendario para ver una lista de los informes que se ejecutaron correctamente para la fecha seleccionada.

Ver un informe

En este tema se proporcionan instrucciones para ver un informe.

Requisitos previos

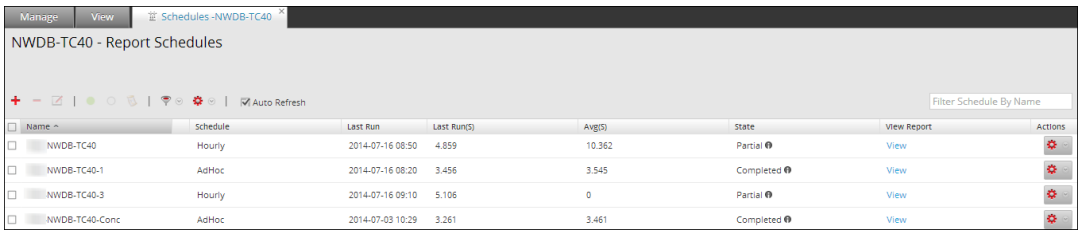
Asegúrese de:

- Haber comprendido los componentes de la vista Informe. Para obtener más información, consulte Vista Informe.
- Haber comprendido los componentes del panel Ver un informe. Para obtener más información, consulte Panel Ver un informe.

Procedimiento

Realice los siguientes pasos para ver un informe:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Informes**.
   Se muestra la vista Informe.
3. En el panel **Lista de informes**, realice una de las siguientes acciones:
   - Haga clic en  > **Ver informes calendarizados**.
   - Haga clic en la columna **N.º de calendarios**.
     La pestaña de la vista Calendarizar informes se muestra con el estado de cada uno de los informes calendarizados.



4. Seleccione un informe calendarizado y haga clic en **Ver**.
   Se muestra una de las siguientes opciones:

- El informe seleccionado.
- El panel Subinformes para un informe calendarizado que tiene seleccionado “Iterativo”.

Se muestra un informe para cada valor en la lista configurada.

> **Nota:** Si el estado del informe es parcial o completo, los valores de “registro de fecha y hora de última ejecución” y “última ejecución (segundos)” se actualizan. Sin embargo, el tiempo promedio que tardó la ejecución del informe se actualiza solo cuando el estado del informe es completo y no cuando es parcial.

Los próximos pasos

Realice las siguientes tareas:

1. Puede imprimir, guardar, enviar por correo electrónico y ver informes en pantalla completa.
2. Puede seleccionar una fecha del calendario para ver una lista de los informes que se ejecutaron correctamente para la fecha seleccionada.

Programar un informe

En este tema se proporcionan instrucciones para programar un informe. Después de la definición de un informe con los componentes y las reglas de formato requeridos, debe configurar sus propiedades de ejecución mediante la calendarización de un informe. Aquí, puede ver, agregar y editar los detalles del calendario de un informe.

Cuando calendariza un informe de Warehouse, puede usar un programador de tareas compatibles para asignar recursos específicos en un clúster para el trabajo calendarizado. Para obtener más información sobre los programadores de tareas compatibles, consulte Características.

Requisitos previos

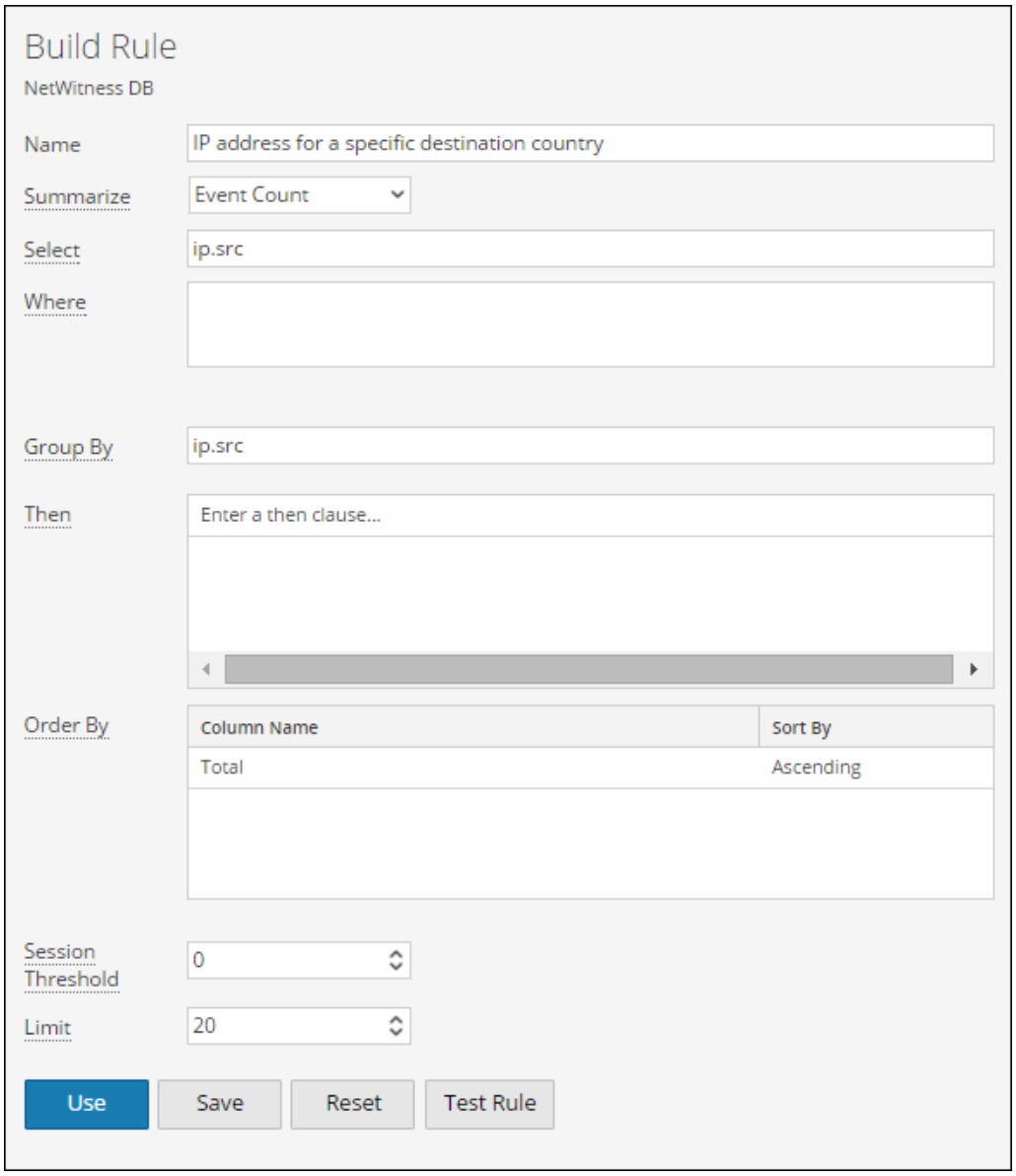
Asegúrese de:

- Haber comprendido los componentes de la vista Crear informe. Para obtener más información, consulte Vista Crear informe.
- Haber comprendido los componentes de la vista Programar un informe. Para obtener más información, consulte Características.
- Si desea usar pools de recursos, debe configurar los pools o las líneas de espera en Reporting Engine. Para obtener más información, consulte el tema Paso 5: Configurar un programador de tareas para Reporting Engine en la *Guía de configuración de hosts y servicios*.

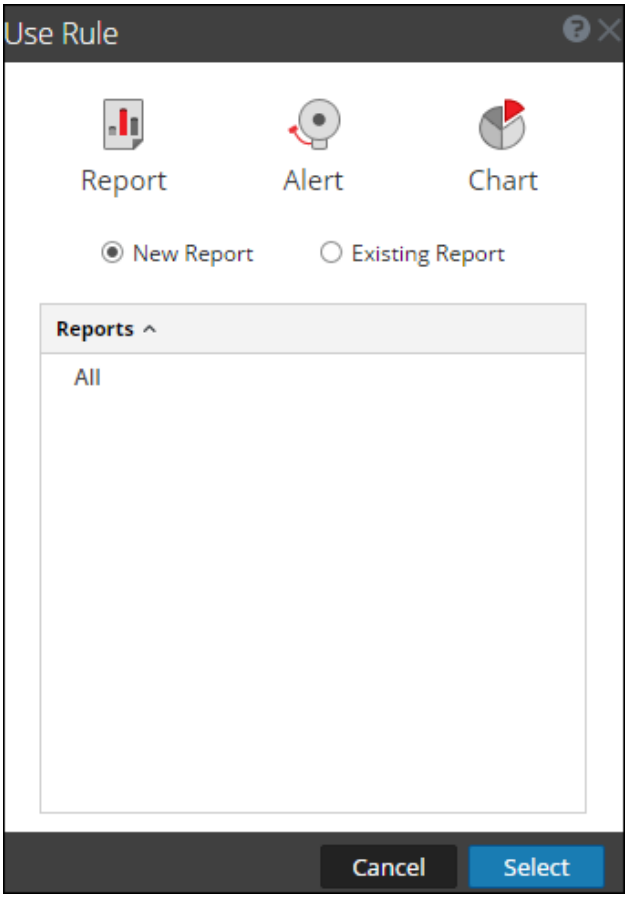
Procedimiento

Realice los siguientes pasos para programar un informe:

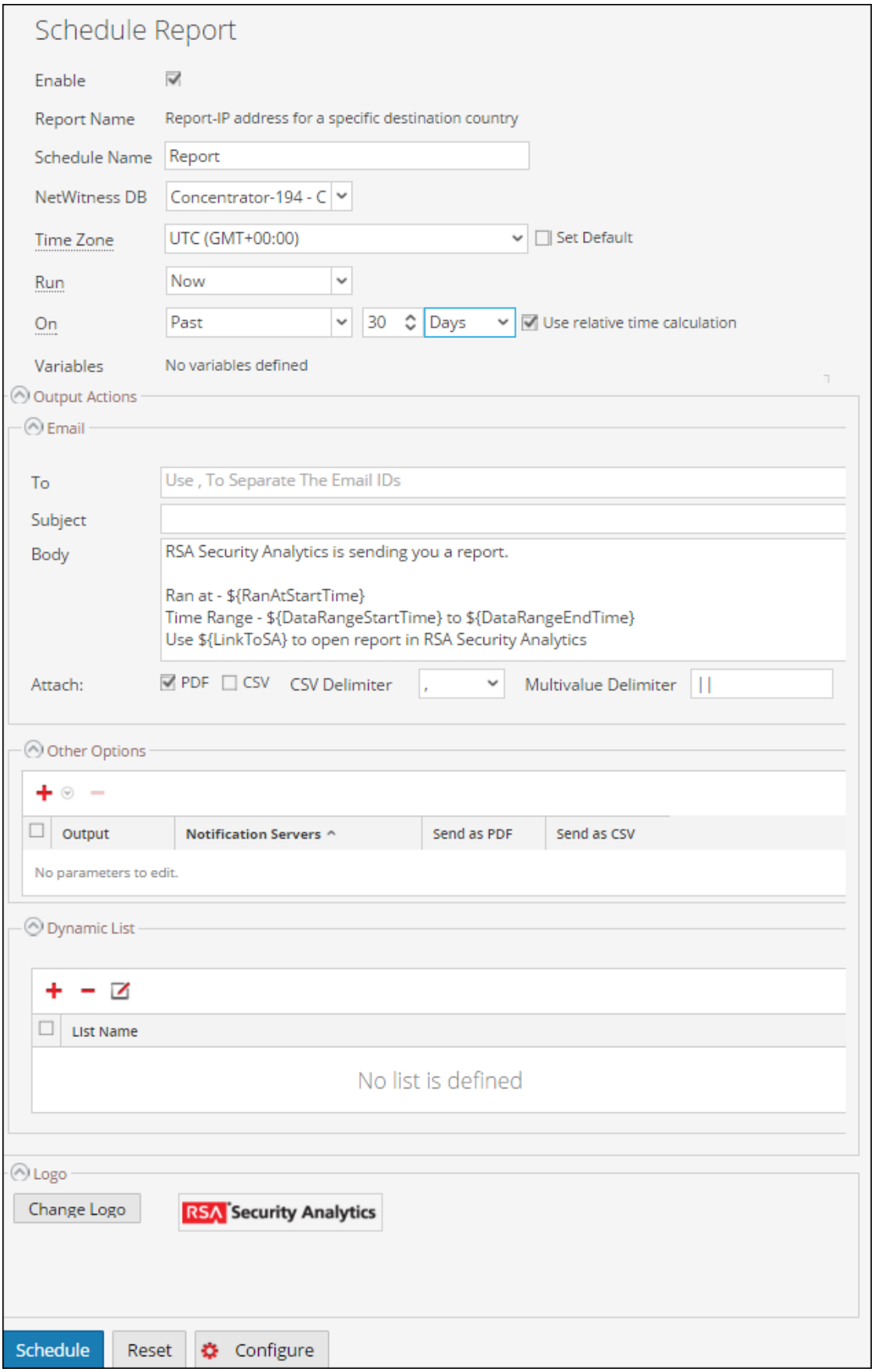
1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Informes**.
   Se muestra la vista Informe.
3. En la página **Crear regla**, haga clic en + para crear una regla.
4. Haga clic en **Guardar**.
5. Haga clic en **Usar**.



6. Seleccione **Nuevo informe** o **Informe existente**.



7. Seleccione un grupo de informes y haga clic en **Seleccionar**.
8. Ingrese el nombre del informe y seleccione la regla.
9. Haga clic en **Schedule**.
   Se muestra la vista Calendarizar informe.


Schedule Report
Enable
Report Name
Report-IP address for a specific destination country
Schedule Name
Report
NetWitness DB
Concentrator-194 - C
Time Zone
UTC (GMT+00:00)
Set Default
Run
Now
On
Past
30
Days
Use relative time calculation
Variables
No variables defined
Output Actions
Email
To
Use , To Separate The Email IDs
Subject
Body
RSA Security Analytics is sending you a report.
Ran at - ${RanAtStartTime}
Time Range - ${DataRangeStartTime} to ${DataRangeEndTime}
Use ${LinkToSA} to open report in RSA Security Analytics
Attach:
PDF
CSV
CSV Delimiter
,
Multivalue Delimiter
||
Other Options
Output
Notification Servers
Send as PDF
Send as CSV
No parameters to edit.
Dynamic List
List Name
No list is defined
Logo
Change Logo
RSA Security Analytics
Schedule
Reset
Configure

Nota: Si proporciona permisos de acceso a un informe a otro usuario, también debe proporcionar permisos para el grupo de informes, las reglas utilizadas en el informe y los grupos de reglas, de lo contrario se mostrará un mensaje de error.

8. Para ejecutar los informes según el programa, seleccione la casilla de verificación **Habilitar**.
9. En el campo **Nombre de calendario**, escriba un nombre para la configuración del informe del calendario.
10. En el campo Origen de datos, seleccione un origen de datos.

    Nota: Si el origen de datos no se muestra, asegúrese de tener permisos de **lectura** configurados para el origen de datos. Esto se aplica a los orígenes de datos NWDB y Warehouse. Para obtener más información, consulte el tema Configurar permisos de orígenes de datos en la *Guía de configuración de hosts y servicios*.

11. (Opcional) En el menú desplegable **Pool de recursos de Warehouse**, seleccione los pools o las líneas de espera disponibles en el clúster para programar el informe a ejecutar en el pool o en la línea de espera. Este menú desplegable está disponible solo si selecciona un informe de base de datos de Warehouse.

    Nota: Se enumeran todas las colas o los pools que ha especificado en la página Explorar para Reporting Engine. Si no se configuran pools o líneas de espera en la página Explorador, este menú desplegable se inhabilita y los trabajos se presentan a los clústeres sin ningún nombre de línea de espera o pool.

    Nota: Si el pool o la línea de espera configurados en el calendario de informes se retira del clúster, en el Programador de capacidad, el nombre de la línea de espera permanece sin definir. Sin embargo, en el programador justo, el nombre del pool especificado se creará mediante property mapred.fairscheduler.allow.undeclared.pool.

12. En el menú desplegable Zona horaria, seleccione una zona horaria para mostrar todos los datos relacionados con tiempo en una salida de informe en el formato especificado. Este ajuste se puede configurar en la vista Explorar de Reporting Engine (/com.rsa.soc.re/configuration/reportoutputformatterconfig/reportoutputformatterconfig).
13. En el campo **Ejecutar**, seleccione el tipo de calendario de ejecución. (Por ejemplo, Ahora o Cada una hora).

    Según el tipo de calendario de ejecución, realice una de las siguientes acciones:

- Si selecciona un calendario de ejecución **Después** o **Mensual**, debe proporcionar un valor para el día y la hora en el campo respectivo que se proporciona.
- Si selecciona un calendario de ejecución **Por hora**, debe especificar los minutos en el campo **En el minuto**.
- Si selecciona un calendario de ejecución **Diario**, debe ingresar un valor en el campo **A las**.
- Si selecciona un programa que se ejecute **Semanalmente**, debe ingresar un valor en el campo **A las** y, además, seleccionar los días de la semana.

Nota: Durante la programación de un informe, si selecciona la opción **Pasado** o la opción **Rango (específico/genérico)** o un rango de horas de finalización muy cerca de la hora actual, debe asegurarse de que se devuelvan los datos agregados en el origen de datos. Si hay una demora de agregación en el origen de datos, la hora de finalización que elige debe tener en cuenta la demora, de lo contrario, los informes pierden datos no agregados para ese rango de horas.

Para obtener información sobre cómo generar un informe con variables, consulte Usar variables para creación de informes con parámetros.

14. (Opcional) En el panel Acciones de salida, realice lo siguiente:

    a. Escriba la dirección y el asunto del correo electrónico.
    b. Edite el cuerpo del mensaje del informe.
    c. Seleccione el formato del archivo adjunto.
    d. Escriba un valor para los delimitadores CSV y Valores múltiples.
    e. (Opcional) En el campo Otras opciones, realice lo siguiente:

        i. Haga clic en  y seleccione SFTP, URL o la acción de salida Recurso compartido de red.
        Se agrega una fila con la acción de salida seleccionada.

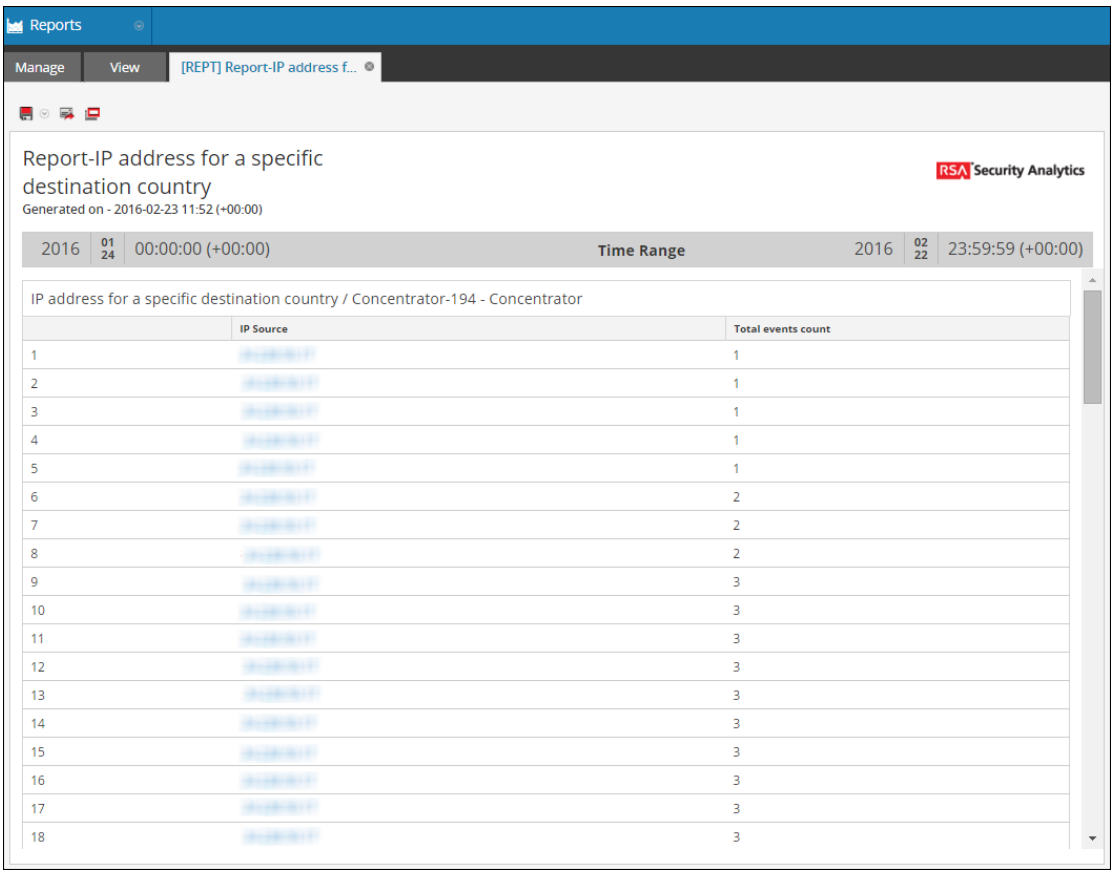
ii. Seleccione las opciones adecuadas para enviar el informe en formato PDF, CSV o ambos a la acción de salida SFTP, URL o Recurso compartido de red configurada para RE.

15. (Opcional) Para agregar una lista en el panel Lista dinámica, consulte la sección Requisitos previos .

16. (Opcional) Para seleccionar un logotipo en el panel Logotipo, consulte la sección Administrar y seleccionar un logotipo de informe .

> **Nota:** Si no especifica un logotipo, se usará el logotipo predeterminado de RSA.

17. Haga clic en **Schedule**.
El informe programado se ejecuta según lo programado y proporciona las salidas configuradas.



Los próximos pasos

Realice las siguientes tareas:

1. Puede notificar al destinatario de correo electrónico cuando la ejecución del informe termine y enviar informes en formato PDF y CSV como archivos adjuntos en el correo electrónico.
2. Puede generar una lista en función del informe programado y verla en el módulo **Listas**.
3. Puede enviar un informe calendarizado en formato PDF o CSV, o ambos al SFTP, la ubicación, o la URL, o un recurso compartido de red configurados de RE.
4. Puede cambiar el logotipo predeterminado y verlo en el informe calendarizado.
5. Puede modificar los detalles de configuración de Security Analytics Reporting Engine, para lo cual debe navegar a la pestaña General de Reporting Engine. Consulte el tema Pestaña General de Reporting Engine en la *Guía de configuración de hosts y servicios*.

Ejemplos

Cuando calendariza informes en la vista Calendarizar informe, de forma predeterminada, los resultados de la opción **Pasado** se presentan en función de la zona horaria especificada por el usuario. Los siguientes ejemplos proporcionan una idea clara sobre qué resultados puede esperar cuando selecciona **horas**, **días**, **semanas**, **meses** o **años** para la opción **Pasado** en función de la duración absoluta o relativa.

Nota: De forma predeterminada, la casilla de verificación Duración relativa está deseleccionada. Esto implica que los resultados de la opción **Pasado** se presentan en función de la duración absoluta.

Basada en la duración absoluta:

La Duración absoluta permite programar un informe en un tiempo absoluto con respecto a la hora actual, excluidos los segundos; se debe tener en cuenta el intervalo de tiempo como un todo. Por ejemplo, las 12:00 h es la hora absoluta con respecto a la hora actual (12:45 h).

Horas

Suponga que selecciona Horas y especifica una hora. Si la hora actual especificada por el usuario es 4:20 h, el informe se genera para el rango de tiempo 3:00 h a 4:00 h.

Días

Suponga que selecciona Días y especifica un día. Si la fecha actual es 27 de agosto de 2014, y la hora actual especificada por el usuario es 10:15 h, el informe se genera para el rango: 26 de agosto de 2014, 00:00 h a 27 de agosto de 2014, 00:00 h.

Semanas

Suponga que selecciona Semanas y especifica una semana. Si la fecha actual es 27 de agosto de 2014, 14:30 h, y el día es miércoles, el informe se genera para el rango: sábado 16 de agosto de 2014, 00:00 h al sábado 23 de agosto de 2014, 00:00 h.

Meses

Suponga que selecciona Meses y especifica un mes. Si la fecha actual es 27 de agosto de 2014, 14:30 h, el informe se genera para el rango:
1 de julio de 2014, 00:00 h al 31 de julio de 2014, 00:00 h.

Años

Suponga que selecciona años y especifica un año. Si la fecha actual es 27 de agosto de 2014, 14:30 h, el informe se genera para el rango:
1 de enero de 2013, 00:00 h al 31 de diciembre de 2013, 00:00 h.

Basada en la duración relativa:

La duración relativa permite programar un informe a una hora relativa a la hora actual, lo cual podría variar en función de la hora actual. Por ejemplo, las 12:45 h es la hora relativa con respecto a la hora actual (12:45 h).

Horas

Suponga que selecciona Horas y especifica una hora. Si la hora actual especificada por el usuario es 16:20 h, el informe se genera para el rango de tiempo 15:20 h a 16:20 h.

Días

Suponga que selecciona Días y especifica un día. Si la fecha actual es 27 de agosto de 2014, y la hora actual especificada por el usuario es 10:15 h, el informe se genera para el rango: 26 de agosto de 2014, 10:15 h a 27 de agosto de 2014, 10:15 h.

Semanas

Suponga que selecciona Semanas y especifica una semana. Si la fecha actual es 27 de agosto de 2014, 12:30 h, y el día es miércoles, el informe se genera para el rango: Jueves 21 de agosto de 2014, 12:30 h al miércoles 27 de agosto de 2014, 12:30 h.

Meses

Suponga que selecciona Meses y especifica un mes. Si la fecha actual es 27 de agosto de 2014, 14:30 h, el informe se genera para el rango:
27 de julio de 2014, 14:30 h a 27 de agosto de 2014, 14:30 h.

Años

Suponga que selecciona años y especifica un año. Si la fecha actual es 27 de agosto de 2014, 14:30 h, el informe se genera para el rango: 27 de agosto de 2013, 14:30 h a 27 de agosto de 2014, 14:30 h.

Activar o desactivar un informe programado

En este tema se proporcionan instrucciones para activar o desactivar un informe calendarizado.

Requisitos previos

Asegúrese de:

- Haber comprendido los componentes de la vista Informe. Para obtener más información, consulte Vista Informe.
- Haber comprendido los componentes de la vista Informes calendarizados. Para obtener más información, consulte Características.

Procedimiento

Realice los siguientes pasos para habilitar o inhabilitar un informe calendarizado desde el panel Lista de informes calendarizados:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Informes**.
   Se muestra la vista Informe.
3. En el panel **Lista de informes**, seleccione un informe y haga clic en  > **Ver informes calendarizados**.
   Se muestra la vista Ver informes calendarizados.
4. Seleccione un informe en el panel Lista de informes calendarizados.
5. Haga clic en  > **Habilitar**.
   El estado del informe cambia a “En ejecución” si el informe está calendarizado para ejecutarse de inmediato.
6. Haga clic en  > **Desactivar**.
   El estado del informe cambia a “Inactivo”.

Generar una lista desde el informe programado

En este tema se proporcionan instrucciones para generar una lista a partir de la salida del informe calendarizado.

Requisitos previos

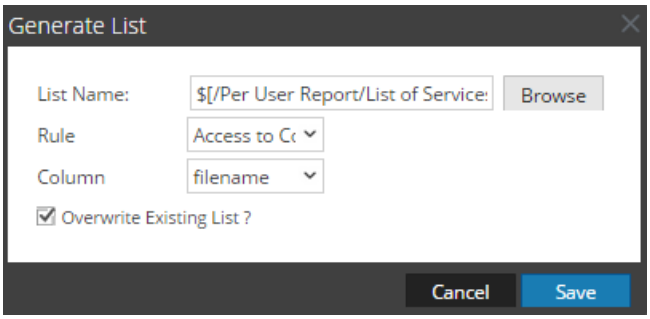
Asegúrese de:

- Que se hayan creado listas en Security Analytics con anterioridad a la generación de una lista para programar un informe.
- Haber comprendido los componentes de la vista Programar un informe. Para obtener más información, consulte Características.
- Haber comprendido los componentes del panel Lista dinámica. Para obtener más información, consulte Características.

Procedimiento

Realice los siguientes pasos para generar una lista desde la vista Crear informe:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Informes**.
   Se muestra la vista Informe.
3. En el panel **Lista de informes**, seleccione un informe y haga clic en  > **Calendarizar informe**.
   Se muestra la pestaña de la vista Programar un informe.
4. En el panel **Lista dinámica**, haga clic en  .
   Se abre el cuadro de diálogo Generar lista.
5. Haga clic en **Navegar**.
   Se muestra el panel Selección de lista.
6. Elija un elemento de la lista y haga clic en **Seleccionar**.
   El nombre de la lista se completa en el campo Nombre de lista.
7. Seleccione una regla válida para filtrar más los resultados del informe según la definición de la regla.
8. Seleccione un valor para el campo **Columna**.
   La columna forma los valores para la lista que se crea.
9. Si desea sobrescribir la lista existente, seleccione la casilla de verificación **¿Desea sobrescribir la lista existente?**.
10. Haga clic en **Guardar**.
    El nombre de la lista se completa en el panel Generar lista.



11. (Opcional) Seleccione una lista en el panel Generar lista y haga clic en para eliminar la lista seleccionada.
12. (Opcional) Seleccione una lista en el panel Generar lista y haga clic en para editar los detalles de la lista.

Los próximos pasos

Puede programar un informe en el panel **Calendarizar informe**. Para obtener más información, consulte Características.

Iniciar o detener un informe programado

En este tema se proporcionan instrucciones para iniciar o detener un informe calendarizado.

Requisitos previos

Asegúrese de:

- Haber comprendido los componentes de la vista Informe. Para obtener más información, consulte Vista Informe.
- Haber comprendido los componentes del panel Calendarizar informe. Para obtener más información, consulte Características.

Procedimiento

Realice los siguientes pasos para iniciar o detener un informe calendarizado:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Informes**.
   Se muestra la vista Informe.

3. En el panel **Lista de informes**, seleccione un informe y haga clic en  > **Ver informes calendarizados**.
   Se muestra la vista Ver informes calendarizados.
4. Seleccione un informe en el panel Lista de informes calendarizados.
5. Haga clic en  > **Iniciar**.
   El estado del informe cambia a "En ejecución" si el informe está calendarizado para ejecutarse de inmediato.
6. Haga clic en  > **Detener**.
   El estado del informe cambia a "Completado".

Ver un historial de ejecución de un informe programado

En este tema se proporcionan instrucciones para ver el historial de ejecución de un informe calendarizado. Puede ver el historial de un informe calendarizado que está en ejecución. Puede ver el historial basado en los siguientes criterios:

- Cantidad de calendarios pasados ejecutados
- Fecha inicial y fecha de finalización para el rango de fechas

Puede ver los detalles como cuántas veces se ejecutó el informe calendarizado, el tiempo de ejecución (segundos), el estado de ejecución. También puede ver el informe generado en pantalla completa.

Requisitos previos

Asegúrese de haber comprendido los componentes del panel Historial de ejecución. Para obtener más información, consulte Características.

Procedimiento

Realice lo siguiente para ver el historial de ejecución de un informe calendarizado:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Informes**.
   Se muestra la vista Informe.

3. En el panel **Lista de informes**, realice una de las siguientes acciones:
   - Haga clic en  > **Ver informes calendarizados**.
   - Haga clic en la columna **N.º de calendarios**.
     La pestaña de la vista Calendarizar informes se muestra con el estado de cada uno de los informes calendarizados.
4. Realice una de las siguientes acciones
   - Seleccione un informe programado y haga clic en  > **Historial de ejecución**.
   - Seleccione un informe programado y haga clic en  .
     Se muestra la vista Historial de ejecución.

> **Nota:** De manera predeterminada, puede ver 10 historiales de ejecución de un informe calendarizado. El historial de ejecución que se muestra depende de la configuración de Conservar historial de informes establecida en la pestaña **General** de la vista **Administration > Servicios > Configuración de Reporting Engine**.
> Por ejemplo, si establece la configuración de Conservar historial de informes en 100 días, los datos que se muestran en la vista Historial de ejecución corresponden a los detalles del historial de ejecución de los últimos 100 días de acuerdo con la información de la fecha actual.

5. Para el campo **Obtener historial por:**, seleccione el tipo de historial que se obtendrá. (Por ejemplo, Pasado o Rango [específico])
6. En el campo **Conteo**, ingrese la cantidad de ejecuciones que se mostrarán.
7. Haga clic en **Mostrar historial**.
   Se muestra el historial de ejecución del informe calendarizado.

Ver informes calendarizados

En este tema se proporcionan instrucciones para ver informes calendarizados. Debe ver los informes calendarizados para conocer su estado. Si el informe calendarizado está en un estado detenido o desactivado, puede iniciarlo o activarlo.

Requisitos previos

Asegúrese de:

- Haber comprendido los componentes de la vista Informe. Para obtener más información, consulte Vista Informe.

- Haber comprendido los componentes de la vista Informes calendarizados. Para obtener más información, consulte Características.

Procedimiento

Realice lo siguiente para ver los informes calendarizados:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.

   Se muestra la pestaña Administrar.

2. Haga clic en **Informes**.

   Se muestra la vista Informe.

3. En el panel **Lista de informes**, realice una de las siguientes acciones:

   - Haga clic en  > **Ver informes calendarizados**.
   - Haga clic en la columna **N.º de calendarios**.

   La pestaña de la vista Calendarizar informes se muestra con el estado de cada uno de los informes calendarizados.

Nota: Si el estado del informe es parcial o completo, los valores de "registro de fecha y hora de última ejecución" y "última ejecución (segundos)" se actualizan. Sin embargo, el tiempo promedio que tardó la ejecución del informe se actualiza solo cuando el estado del informe es completo y no cuando es parcial.

Próximos pasos

Realice las siguientes tareas:

1. Puede agregar, editar, eliminar, iniciar o detener el informe calendarizado.
2. Puede ver todos los informes que se ejecutaron correctamente. Para obtener más información, consulte Panel Ver todos los informes.

Eliminar un informe programado

En este tema se proporcionan instrucciones para eliminar un informe calendarizado.

Requisitos previos

Asegúrese de:

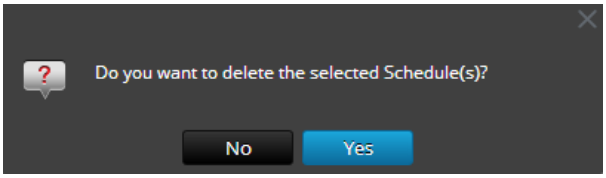
- Haber comprendido los componentes de la vista Informe. Para obtener más información, consulte Vista Informe.

- Haber comprendido los componentes del panel Calendarizar informe. Para obtener más información, consulte Características.

Procedimiento

Realice los siguientes pasos para eliminar un informe calendarizado desde el panel Lista de informes calendarizados:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Informes**.
   Se muestra la vista Informe.
3. En la barra de herramientas **Informe**, haga clic en **Ver todos los calendarios**.
   Se muestra la vista Ver informes calendarizados.
4. En el panel **Lista de informes calendarizados**, seleccione el informe.
5. Haga clic en  >**Eliminar calendario**.
   Se muestra un cuadro de diálogo de confirmación.



5. Haga clic en **Sí** para eliminar el informe programado.
   Se muestra un mensaje que confirma la correcta eliminación del informe calendarizado y el calendario seleccionado se elimina del panel Lista de informes calendarizados.

Editar un informe programado

En este tema se proporcionan instrucciones para editar un informe calendarizado.

Requisitos previos

Asegúrese de:

- Haber comprendido los componentes de la vista Informe. Para obtener más información, consulte Vista Informe.

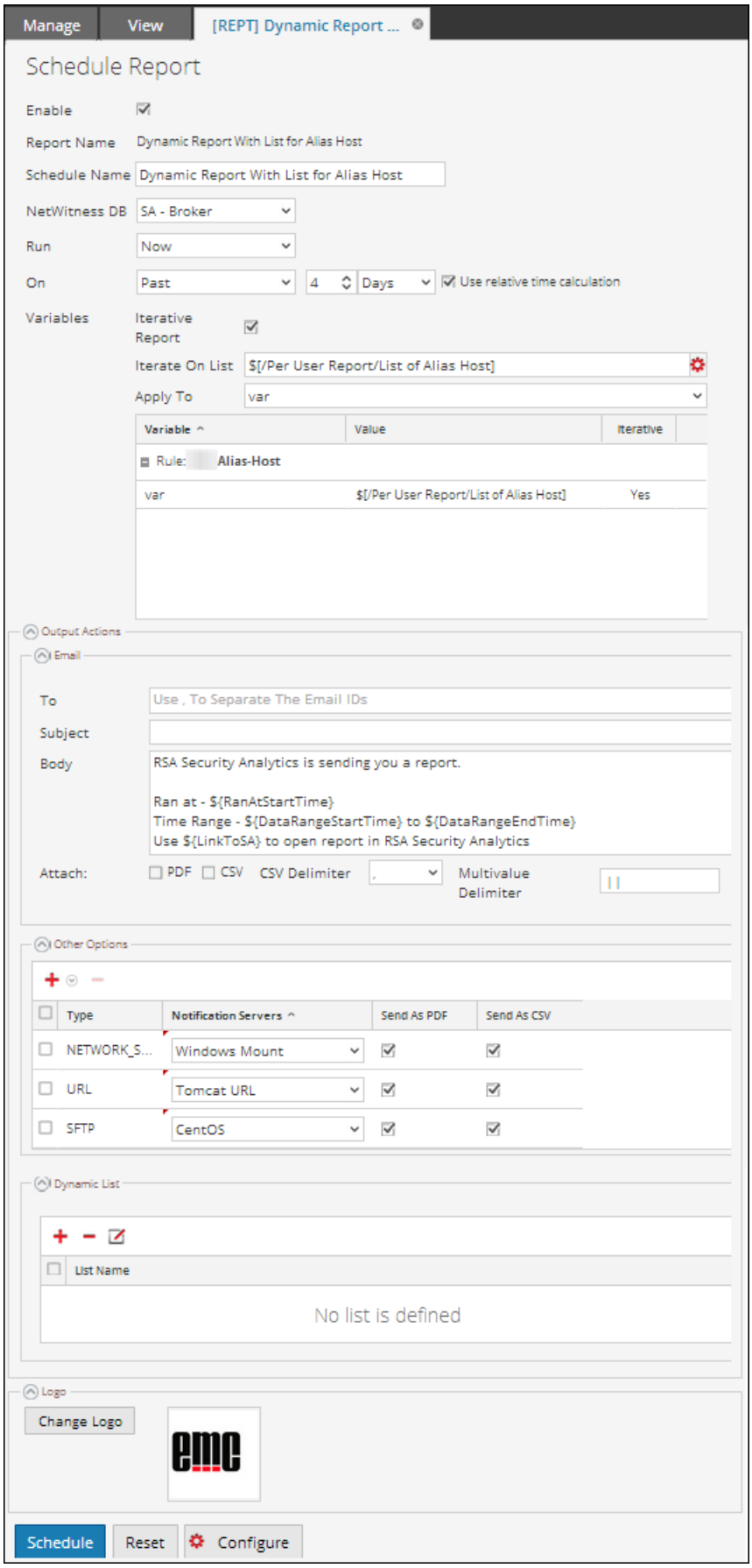
- Haber comprendido los componentes del panel Calendarizar informe. Para obtener más información, consulte Características.

Procedimiento

Realice los siguientes pasos para editar un informe calendarizado desde el panel Lista de informes calendarizados:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Informes**.
   Se muestra la vista Informe.
3. En el panel **Lista de informes**, seleccione un informe y haga clic en  > **Ver informes calendarizados**.
   Se muestra la pestaña Ver informes calendarizados.
4. En el panel **Lista de informes calendarizados**, realice una de las siguientes acciones:
   - Seleccione un informe y haga clic en  .
   - Seleccione un informe y haga clic en  > **Editar calendario**.

Se muestra la pestaña Calendarizar informe.


Manage
View
[REPT] Dynamic Report ...
Schedule Report
Enable
Report Name
Dynamic Report With List for Alias Host
Schedule Name
Dynamic Report With List for Alias Host
NetWitness DB
SA - Broker
Run
Now
On
Past
4
Days
Use relative time calculation
Variables
Iterative Report
Iterate On List
$[/Per User Report/List of Alias Host]
Apply To
var
Variable
Value
Iterative
Rule:
Alias-Host
var
$[/Per User Report/List of Alias Host]
Yes
Output Actions
Email
To
Use , To Separate The Email IDs
Subject
Body
RSA Security Analytics is sending you a report.
Ran at - ${RanAtStartTime}
Time Range - ${DataRangeStartTime} to ${DataRangeEndTime}
Use ${LinkToSA} to open report in RSA Security Analytics
Attach:
PDF
CSV
CSV Delimiter
Multivalue Delimiter
Other Options
Type
Notification Servers
Send As PDF
Send As CSV
NETWORK_S...
Windows Mount
URL
Tomcat URL
SFTP
CentOS
Dynamic List
List Name
No list is defined
Logo
Change Logo
Schedule
Reset
Configure

5. En la pestaña Calendarizar informe, realice lo siguiente:
   a. En el campo **Nombre de calendario**, modifique el nombre de la configuración del informe del calendario.
   b. Para ejecutar los informes según el calendario, seleccione la casilla de verificación **Habilitar**.
   c. En el campo **Origen de datos**, seleccione la base de datos.

   Nota: si el origen de datos no se muestra, asegúrese de tener permisos de **lectura** configurados para el origen de datos. Esto se aplica a los orígenes de datos NWDB y Warehouse. Para obtener más información, consulte el tema Configurar permisos de orígenes de datos en la *Guía de configuración de hosts y servicios*.

6. (Opcional) En la lista desplegable **Pool de recursos de Warehouse**, seleccione el pool o la línea de espera para el informe.

   Nota: La lista desplegable **Pool de recursos de Warehouse** se muestra solo si se selecciona la regla de Warehouse. Si no se ingresan pools o líneas de espera para el Reporting Engine, este campo estará inhabilitado.

7. En el campo **Ejecutar**, seleccione el tipo de calendario de ejecución. (Por ejemplo, Ahora o Cada una hora).
8. Seleccione el rango de fechas para ejecutar la consulta en función de una duración absoluta, o seleccione la casilla de verificación **Usar duración de tiempo relativo** para ejecutarla de acuerdo con una duración relativa.
9. (Opcional) En el panel Acciones de salida, realice lo siguiente:
   i. Escriba la dirección y el asunto del correo electrónico.
   ii. Edite el cuerpo del mensaje del informe.
   iii. Seleccione el formato del archivo adjunto.
   iv. Escriba un valor para los delimitadores CSV y Varios valores.
10. (Opcional) En el campo Otras opciones, realice lo siguiente:
    i. Haga clic en  > **SFTP**, **URL** o **Recurso compartido de red**. De acuerdo con la opción seleccionada, se agrega una fila en el campo Otras opciones.
    ii. Seleccione las opciones adecuadas para enviar el informe en formato PDF o CSV al SFTP, la URL o el recurso compartido de red configurados.
11. (Opcional) Para agregar una lista en el panel Lista dinámica, consulte la sección Requisitos previos .

12. (Opcional) Para seleccionar otro logotipo en el panel Logotipo, consulte la sección Administrar y seleccionar un logotipo de informe .

    Nota: Si no especifica un logotipo, se usa el logotipo predeterminado de RSA.

13. Haga clic en **Schedule**.
    El informe programado se ejecuta según lo programado y proporciona las salidas configuradas.

Administrar el acceso para un informe o un grupo de informes

En esta sección se describen los permisos de acceso que tiene el usuario según la función del usuario para administrar un informe y un grupo de informes. El módulo Reporting proporciona un control de acceso en el nivel de informe y de grupo de informes. El usuario que tiene el conjunto correcto de permisos puede ejecutar las tareas en el módulo Reporting. El administrador administra el control de acceso desde la pestaña **Administration > Seguridad > Funciones**.

Cuando crea usuarios y funciones de usuario, el administrador debe asegurarse de que las funciones creadas para tareas específicas tengan acceso a todos los permisos más altos en la jerarquía de funciones.

Los informes y los grupos de informes se pueden vincular a un conjunto específico de funciones de usuario de modo que, cuando un usuario inicie sesión en Security Analytics, se puedan ver los informes con derechos de acceso para la función de usuario específica. Los usuarios que pertenecen a una función de usuario con el permiso de acceso “Lectura y escritura” pueden definir informes. Además, el acceso se puede restringir de modo que solo accedan a los informes quienes tengan el acceso de “Solo lectura”.

Nota: debe tener permiso de “Solo lectura” en un grupo para ver los informes dentro de ese grupo.

En el nivel del informe, puede establecer los siguientes permisos de acceso para las funciones de usuario en Security Analytics:

- Lectura y escritura
- Solo lectura
- Sin acceso

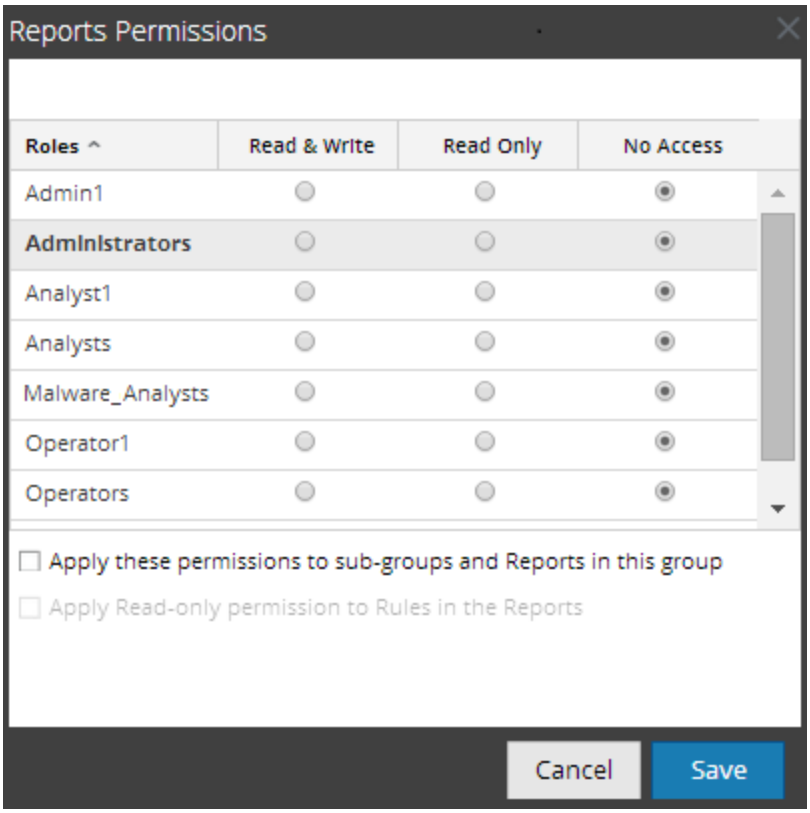
Suponga que desea que los **analistas de seguridad** tengan acceso a todos los informes de un grupo de informes. Para esto, puede configurar el permiso “**Lectura y escritura**” en el nivel del grupo de informes. Y si no desea que la función **Operador** tenga acceso a un conjunto específico de informes en un grupo de informes, puede configurar el permiso “**Sin acceso**” en el nivel del grupo de informes.

El permiso se configura solo para el grupo de informes, pero no para los informes, las reglas ni los subgrupos del grupo de informes.

Control de acceso para un grupo de informes

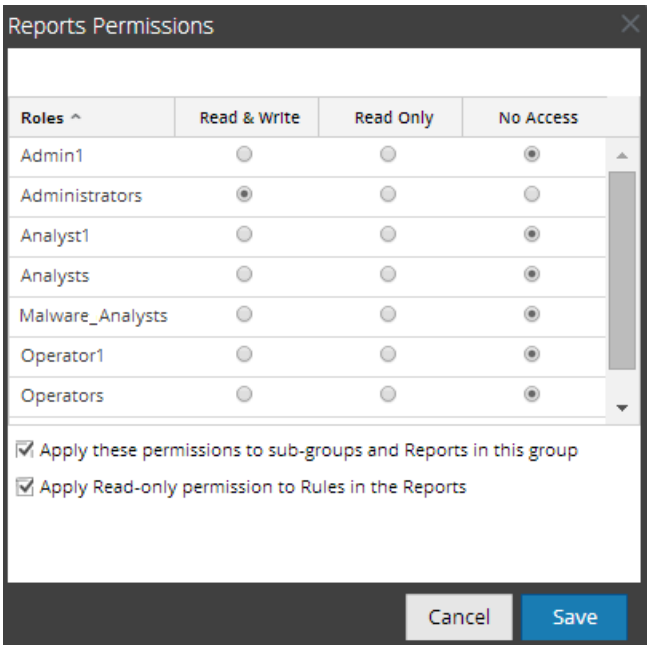
Cuando desea cambiar los permisos del grupo de informes, debe seleccionar un grupo de informes y configurar sus permisos de acceso en el panel Permisos de informes.

Antes de aplicar permisos del grupo de informes, el permiso predeterminado configurado para todas las funciones de usuario es el permiso "Sin acceso", excepto para los administradores, como se muestra en la figura.



Si desea cambiar el permiso de acceso para una función de usuario específica, debe configurarlo en el nivel del grupo de informes, como se muestra en la figura. Suponga que desea que los administradores tengan acceso a todos los informes de un grupo de informes. Para esto, puede configurar el permiso "**Lectura y escritura**" en el panel Permisos de grupo de informes.

También puede aplicar permisos a los subgrupos y a los informes del grupo, como también aplicar permisos de solo lectura a reglas en los informes si selecciona la casilla de verificación apropiada, como se muestra en la figura.



Los tres escenarios se explican de forma resumida:

- Escenario 1: Permisos aplicados a grupo de informes/subgrupo/informe según la función de usuario.
- Escenario 2: Permisos aplicados a subgrupo e informe del grupo.
- Escenario 3: Permiso de solo lectura aplicado a las reglas del informe.

Función (analista)	Permisos aplicados a grupo de informes/-subgrupo/informe según la función de usuario.	Permisos aplicados a subgrupo e informes del grupo.	Permiso (de solo lectura) aplicado a las reglas del informe

Grupo	Lectura y escritura	**Lectura y escritura**	**Lectura y escritura**	Lectura y escritura
Subgrupo	Lectura	**Lectura**	**Lectura y escritura: heredados**	Lectura y escritura
Informe	Lectura	**Lectura**	**Lectura y escritura: heredados**	Lectura y escritura
Reglas	Lectura	**Lectura**	Lectura	**Lectura**

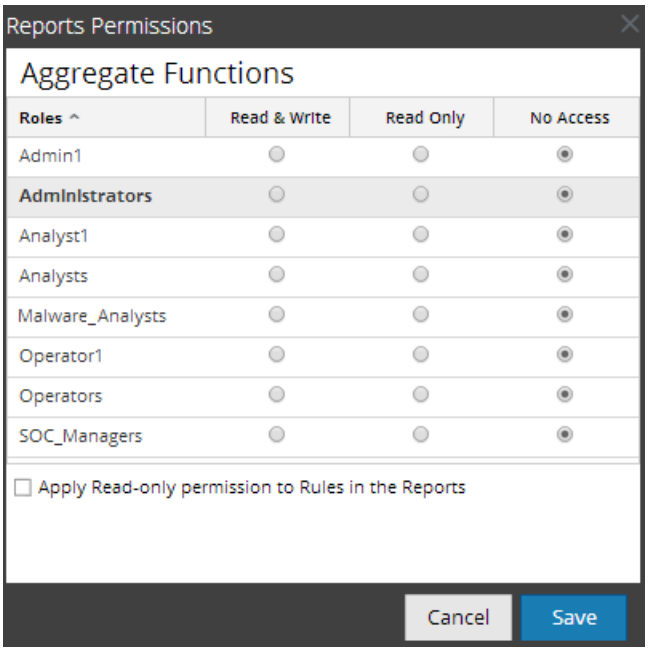
Al grupo de informes se asignará la función de un **analista de seguridad** y los permisos se configuran en **Lectura y escritura** para el grupo de informes.

En el escenario 1, cada uno de los niveles tiene un permiso configurado de acuerdo con la función del usuario. En el escenario 2, el subgrupo y los informes del grupo heredan el permiso en el nivel del grupo de informes (lectura y escritura). En el escenario 3 se configura el permiso de lectura para las reglas, salvo que el permiso configurado para las reglas no puede ser mayor que los permisos configurados para el grupo de informes.

Control de acceso para un informe

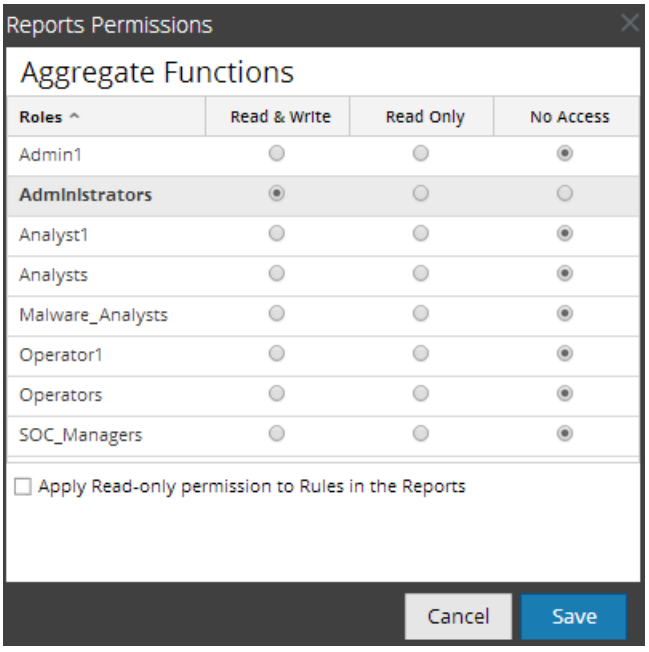
Cuando desea cambiar los permisos del informe, debe seleccionar un informe y configurar sus permisos de acceso en el panel Permisos de informes.

Antes de aplicar permisos de informes, el permiso predeterminado configurado para todas las funciones de usuario es el permiso “Sin acceso” y la casilla de verificación está deseleccionada, como se muestra en la figura.



Si desea cambiar el permiso de acceso para una función de usuario específica, debe configurarlo en el nivel de informe, como se muestra en la figura. Suponga que desea que los **administradores** tengan acceso a un informe específico. Para esto, puede configurar el permiso "**Lectura y escritura**" en el panel Permisos de informe.

Y, puede aplicar permisos de solo lectura a las reglas de los informes si selecciona la casilla de verificación, como se muestra en la figura.



Los dos escenarios se explican de forma resumida:

- Escenario 1: Permisos aplicados a un grupo de informes/subgrupo/informe/reglas.
- Escenario 2: Permiso de solo lectura aplicado a las reglas del informe.

	Función (analistas)	Permisos aplicados a grupo de informes/subgrupo/informe/reglas según la función de usuario.	Permiso (de solo lectura) aplicado a las reglas del informe
Grupo	Lectura y escritura	**Lectura y escritura**	Lectura y escritura
Subgrupo	Lectura	**Lectura**	Lectura y escritura
Informe	Lectura	**Lectura**	Lectura y escritura
Reglas	Lectura	**Lectura**	**Lectura**

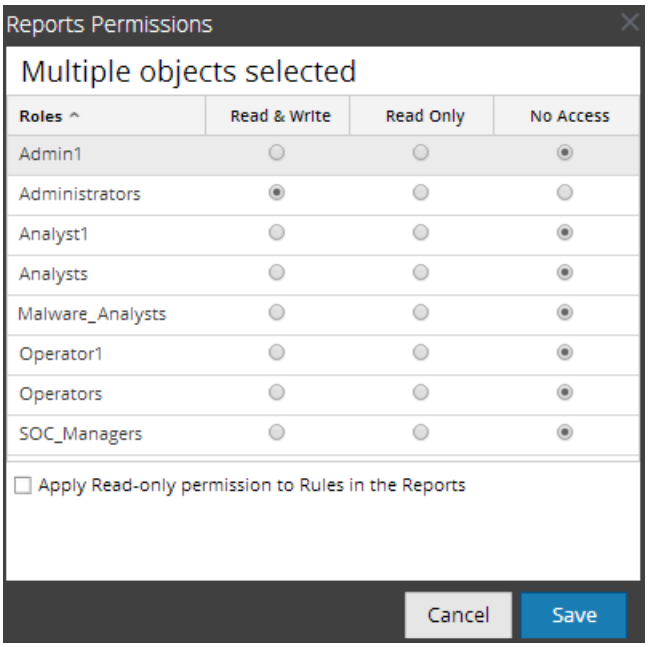
Al informe se asignará la función de un **analista de seguridad** y los permisos se configuran en **Lectura y escritura** para los informes.

En el escenario 1, cada uno de los niveles tiene un permiso configurado según la función del usuario. En el escenario 2 se configura el permiso de lectura para las reglas, salvo que el permiso para las reglas no puede ser mayor que el permiso para los informes.

Nota: si el permiso para las reglas es mayor que el permiso para los informes, el permiso no se aplica. Por ejemplo, si configura los permisos para el grupo de informes como **Sin acceso** y especifica la opción *Aplicar permisos de solo lectura a las reglas de los informes*, el permiso de solo lectura no se configura para las reglas.

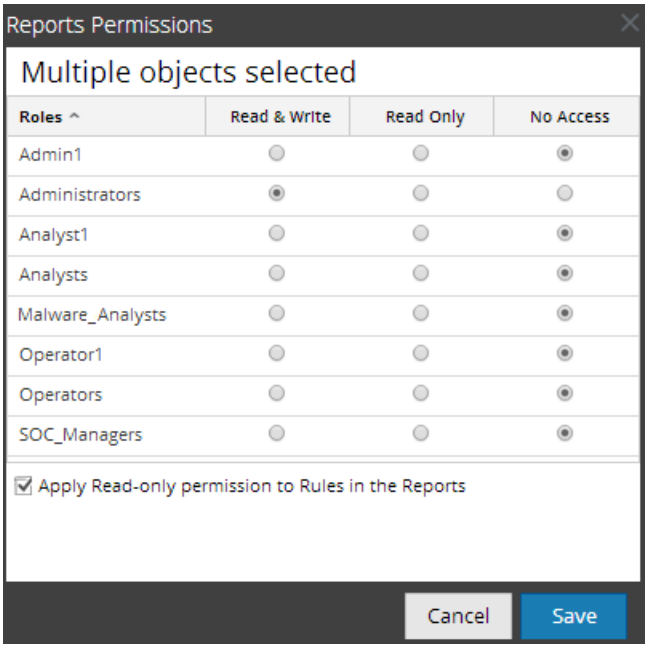
Control de acceso para un informe cuando se seleccionan múltiples informes

Cuando desea cambiar los permisos de varios informes, debe seleccionarlos y configurar sus permisos de acceso en el panel Permisos de informes. El permiso de acceso que elige se aplica a todos los informes seleccionados.



Control de acceso para un informe cuando se seleccionan múltiples informes con varias reglas

Cuando desea cambiar los permisos y están seleccionados múltiples informes con varias reglas, debe seleccionar la casilla de verificación del panel Permisos de informes, como se muestra en la figura. El permiso de acceso de solo lectura se aplica a todas las reglas de los informes seleccionados, siempre que el permiso de las reglas sea menor que el permiso de los informes.

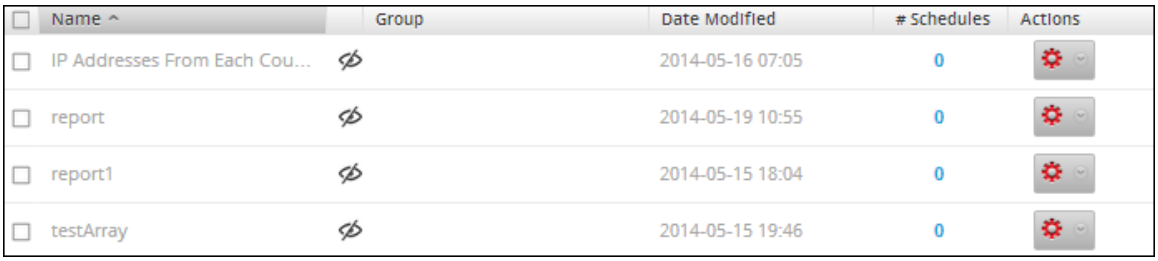


Inicie sesión como un usuario específico y vea los detalles de acceso

Cuando inicia sesión en la interfaz del usuario de Security Analytics como un usuario que tiene el permiso "Acceso de lectura", todos los informes se marcan con el símbolo (📖) y cuando hace clic en el símbolo, se muestra la leyenda "Solo lectura" en el panel Lista de informes.

Cuando inicia sesión en la interfaz del usuario de Security Analytics como un usuario que no tiene el permiso de acceso "Lectura y escritura" en un informe, todos los informes se marcan con el símbolo (👁) y aparecen en gris en el panel Lista de informes.

En la siguiente figura se muestra el panel Lista de informes cuando se inicia sesión con un permiso de acceso de "Lectura y escritura" mínimo.



Nota: Si un usuario (que no sea el superusuario) crea un informe, no habrá acceso al informe para el superusuario.

Lista tabular

En la siguiente tabla se indican las diversas columnas del panel Permisos de informes:

Columna	Descripción
Funciones	La función del usuario que inició sesión en la interfaz del usuario de Security Analytics.
Lectura y escritura	El usuario puede acceder, ver, editar, importar, exportar y eliminar el informe en la página Informes. El usuario también puede cambiar el permiso en el informe.
Solo lectura	El usuario solo puede acceder al informe y verlo en la vista Informes.
Sin acceso	El usuario no puede acceder a un informe ni verlo cuando tiene configurado este permiso.

Columna	Descripción
Aplicar estos permisos a subgrupos e informes en este grupo	Seleccione la casilla de verificación para aplicar los permisos seleccionados al grupo de informes, subgrupos en el grupo e informes en el grupo. **Nota:** Esta casilla de verificación solo se completa cuando se establece permisos de acceso para un grupo de informes.
Aplicar permisos de solo lectura a las reglas de los informes	Seleccione la casilla de verificación para aplicar permisos a las reglas de los informes de forma automática.

Temas:

- Establecer el control de acceso para un informe
- Establecer el control de acceso para un grupo de informes

Establecer el control de acceso para un informe

En este tema se proporcionan instrucciones para configurar el control de acceso para un informe.

Requisitos previos

Asegúrese de:

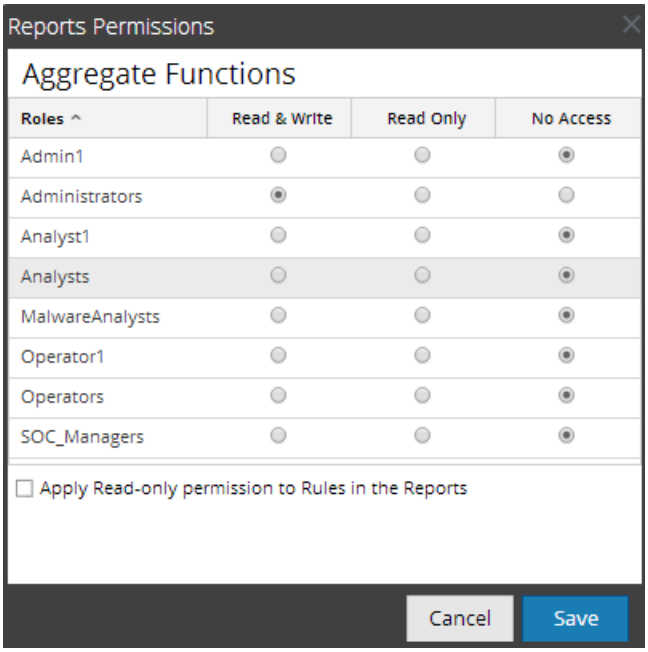
- Haber comprendido los componentes de la vista Informe. Para obtener más información, consulte Vista Informe.
- Haber comprendido los permisos de acceso que tendrá el usuario según la función de usuario. Para obtener más información, consulte Administrar el acceso para un informe o un grupo de informes.

- Tener un permiso de acceso de “Lectura y escritura” mínimo para establecer permisos de acceso para un informe.

Procedimiento

Realice los siguientes pasos para establecer permisos de acceso para un informe:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Informes**.
   Se muestra la vista Informe.
3. En el panel **Lista de informes**, seleccione un informe.
4. Haga clic en  > **Permisos**.
   Aparece el cuadro de diálogo Permisos de informes.



4. Según la función de usuario, seleccione los botones que correspondan.
5. (Opcional) Seleccione la casilla de verificación si desea otorgar permiso de acceso de lectura a reglas en los informes.

Nota: Cuando se selecciona la casilla de verificación, se otorga permiso de acceso de LECTURA a todas las reglas dependientes, siempre que los permisos para el informe sean más altos que los permisos de las reglas.

6. Haga clic en **Guardar**.
   Se muestra un mensaje de confirmación que indica que el permiso se estableció para el informe seleccionado.

Establecer el control de acceso para un grupo de informes

En este tema se proporcionan instrucciones para establecer permisos para un grupo de informes.

Requisitos previos

Asegúrese de:

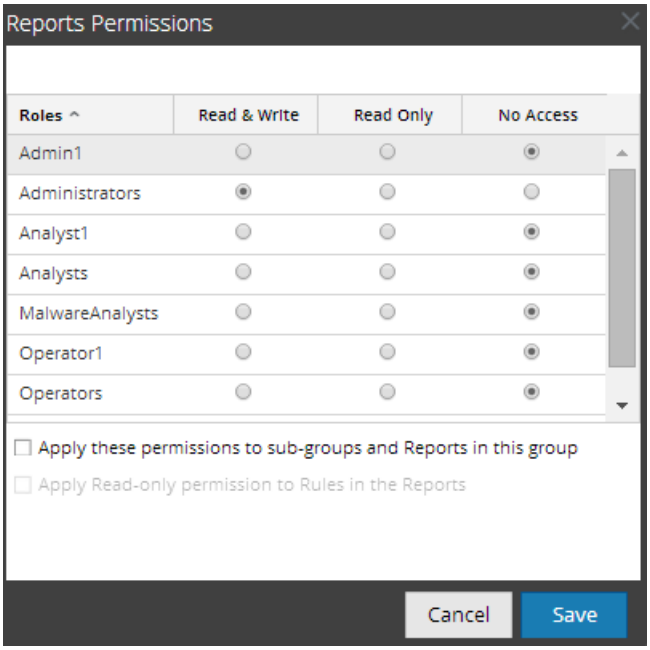
- Haber comprendido los componentes de la vista Informe. Para obtener más información, consulte Vista Informe.
- Haber comprendido los permisos de acceso que tendrá el usuario según la función de usuario. Para obtener más información, consulte Administrar el acceso para un informe o un grupo de informes
- Tener un permiso de acceso de "Lectura y escritura" mínimo para establecer permisos de acceso para un grupo de informes.

Procedimiento

Realice los siguientes pasos para establecer permisos de acceso para un grupo de informes:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Informes**.
   Se muestra la vista Informe.
3. En el panel **Grupos de informes**, seleccione o haga clic con el botón secundario en un grupo de informes.
4. Haga clic en  > **Permisos**.

Aparece el cuadro de diálogo Permisos de informes.



4. Según la función de usuario, seleccione los botones que correspondan.
5. (Opcional) Seleccione la casilla de verificación apropiada para aplicar los permisos seleccionados a subgrupos e informes en el grupo.
6. (Opcional) Seleccione la casilla de verificación apropiada para otorgar permiso de acceso de lectura a reglas en los informes.

Nota: cuando se selecciona la casilla de verificación, se otorga permiso de acceso de LECTURA a todas las reglas dependientes, siempre que los permisos para el informe sean más altos que los permisos de las reglas.

7. Haga clic en **Guardar**.
   Se muestra un mensaje de confirmación que indica que el permiso se estableció correctamente para el grupo de informes seleccionado.

Investigar un informe

En este tema se proporcionan instrucciones para investigar un informe. Puede investigar un informe, para lo cual debe navegar directamente hacia el módulo Investigation desde el informe. Con la opción Investigar un informe, puede investigar cada evento mencionado en el informe.

En este tema se proporcionan instrucciones para investigar un informe. Puede investigar un informe, para lo cual debe navegar directamente hacia el módulo Investigation desde el informe. Con la opción Investigar un informe, puede investigar cada evento mencionado en el informe.

Requisitos previos

Asegúrese de:

- Haber comprendido los componentes de la vista Informe. Para obtener más información, consulte Vista Informe.
- Haber comprendido los componentes del panel Ver todos los informes. Para obtener más información, consulte Panel Ver todos los informes.

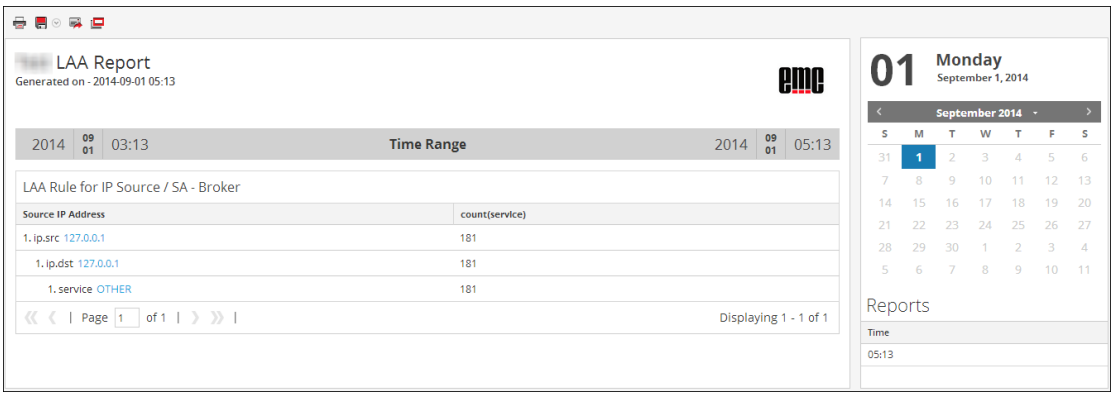
Procedimiento

Realice los siguientes pasos para investigar un informe:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Informes**.
   Se muestra la vista Informe.
3. En la barra de herramientas **Informe**, haga clic en **Ver todos los informes**.
   Se muestra la pestaña Ver todos los informes.

   Nota: Si no se muestran informes en Ver todos los informes, seleccione una fecha para la cual desea mostrar los informes.

4. Haga doble clic en el nombre del informe para ver sus detalles.
   Aparece la pantalla de detalles del informe.



5. Haga clic en una dirección ip.src en el informe para verlo en el módulo Investigation.

Nota: si desea copiar manualmente los datos de los resultados y usarlos para una investigación, asegúrese de que los valores binarios tengan el prefijo “hex:”.

Los próximos pasos

Realice las siguientes tareas:

1. Puede imprimir, guardar, enviar por correo electrónico y ver informes en pantalla completa.
2. Puede seleccionar una fecha del calendario para ver una lista de los informes que se ejecutaron correctamente para la fecha seleccionada.

Administrar y seleccionar un logotipo de informe

En este tema se proporcionan instrucciones para seleccionar y administrar logotipos en la vista de configuración de servicios de Reporting Engine.

Requisitos previos

Asegúrese de tener definido el servicio de RE antes de administrar un logotipo.

Administrar logotipos de informe

Para administrar logotipos:

1. En el menú de **Security Analytics**, seleccione **Administration** > **Servicios**.

   Se muestra la vista Servicios.
2. En el panel **Lista de servicios**, seleccione un servicio de RE y haga clic en **Ver** > **Configuración**.

   Se muestra la vista Configuración de servicios.
3. Seleccione la pestaña **Administrar logotipos**.

   Se muestran todos los logotipos disponibles.

Para agregar un logotipo:

1. En la pestaña **Administrar logotipos**, haga clic en  .

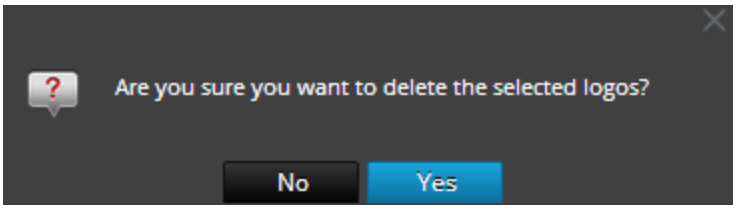
   Se abre un navegador de archivos donde puede elegir el archivo en la unidad local.
2. Seleccione el logotipo y haga clic en **Seleccionar**.

   El logotipo seleccionado se agrega a la sección Administrar logotipos.

Para eliminar un logotipo:

1. En la pestaña **Administrar logotipos**, realice una de las siguientes acciones:
   - Seleccione el logotipo y haga clic en .
   - Mediante (Ctrl+clic), seleccione varios logotipos y haga clic en .

   Se muestra un cuadro de diálogo de confirmación.



2. Si desea eliminar el logotipo, haga clic en **Sí**.

   El logotipo seleccionado se elimina de la sección Administrar logotipos.

Para configurar un logotipo predeterminado:

En la pestaña **Administrar logotipos**, seleccione el logotipo y haga clic en Set default.

El logotipo seleccionado se establece como el logotipo predeterminado para el servicio de RE.

Seleccionar un logotipo

En esta sección se proporcionan instrucciones para elegir logotipos en la vista Programar un informe.

Requisitos previos

- Haber comprendido los componentes del panel Calendarizar informe. Para obtener más información, consulte Características.
- Haber comprendido los componentes de la vista Informes calendarizados. Para obtener más información, consulte Características.
- Haber comprendido los campos del panel Cambiar un logotipo. Para obtener más información, consulte Cuadro de diálogo Seleccionar un logotipo.

Procedimiento

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.

   Se muestra la pestaña Administrar.

2. Haga clic en **Informes**.

   Se muestra la vista Informe.

3. En el panel **Lista de informes**, seleccione un informe.
4. Haga clic en  > **Ver informes calendarizados**.
   Se muestra la pestaña de la vista Ver informes calendarizados.
5. Seleccione un informe programado y haga clic en  > **Editar calendario**.
   Se muestra la pestaña de la vista Programar un informe.
6. En el panel Logotipo, haga clic en **Cambiar logotipo**.
   Se abre el cuadro de diálogo Cambiar un logotipo.
7. Realice una de las siguientes acciones
   - Haga clic en **Cargar nuevo logotipo** para cargar otro logotipo.
   - Seleccione un logotipo de la lista.
8. Haga clic en **Seleccionar**.
   El logotipo seleccionado está disponible en el panel Logotipo.

Usar variables para creación de informes con parámetros

En este tema se suministra información sobre el uso de variables para crear informes en el módulo Reporting de RSA Security Analytics. La creación de informes con parámetros permite especificar valores dinámicamente en el tiempo de ejecución sin cambiar la definición de la regla, de modo que pueda ver los resultados de acuerdo con un valor particular. Puede lograr la creación de informes con parámetros si usa variables en la consulta o la regla. Para obtener información sobre la adición de una regla, consulte Definir una regla. En la hora de ejecución, puede ingresar el valor de la variable o seleccionarlo en la lista de acuerdo con el conjunto de resultados que se muestra.

La sintaxis para especificar la variable es la siguiente:

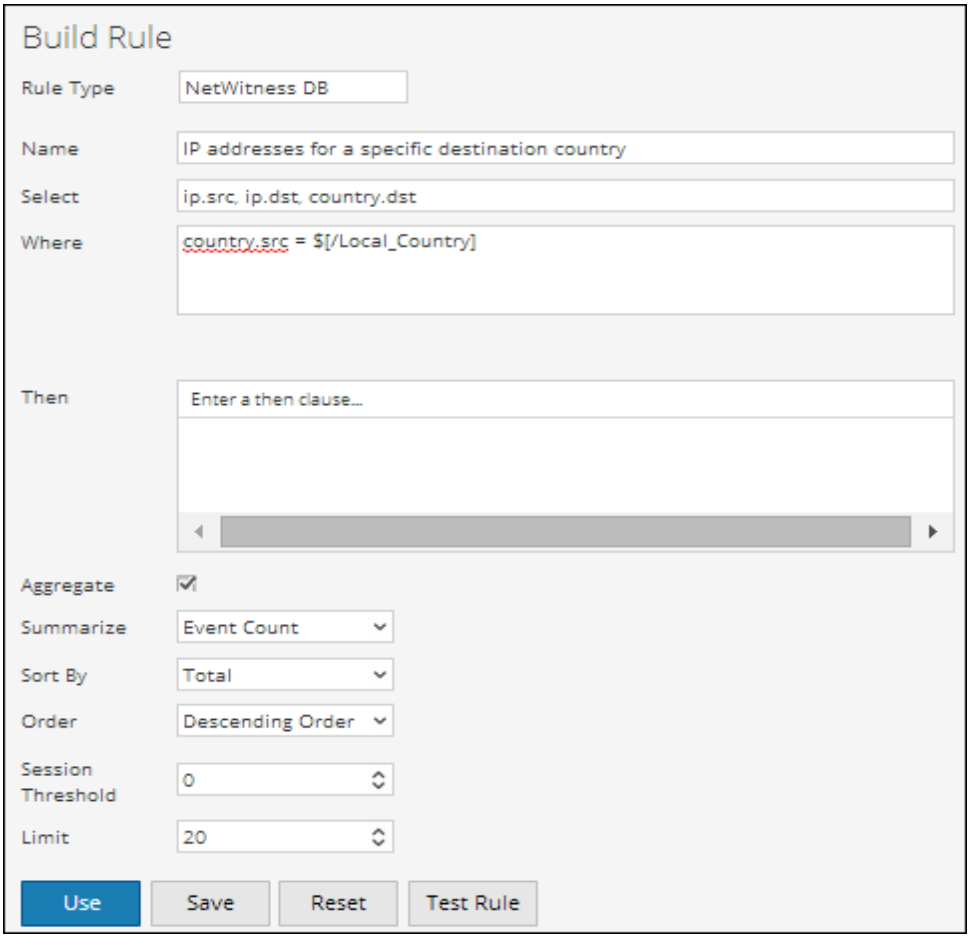
Descripción	Ejemplos de sintaxis compatible
Inserte `$` antes de una variable. Encierre una variable en llaves.	`columnname=${<variable>}`

La sintaxis para definir la variable es la misma para orígenes de datos de la base de datos NetWitness, IPBD y la base de datos de Warehouse. Cuando asigna el valor de la variable en una configuración de ejecución, debe ingresar el valor entre comillas simples: `'<value>'`.

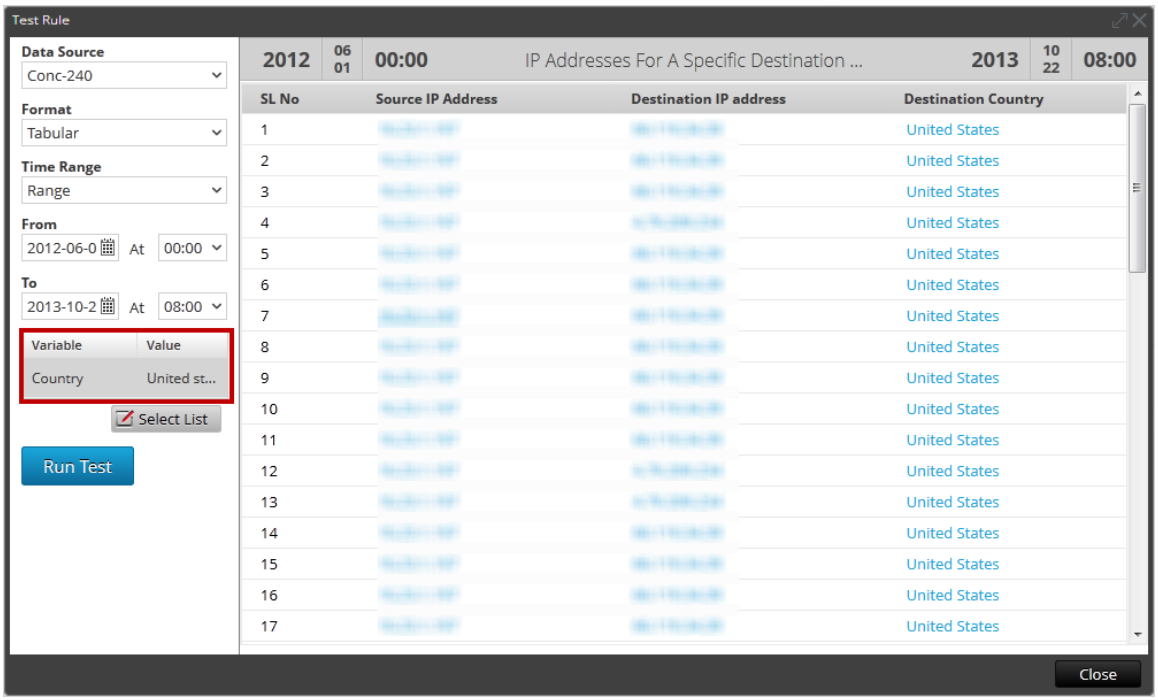
En esa sección se proporcionan algunos ejemplos donde se puede usar una variable.

Ver las direcciones IP de origen para un país de destino específico

El siguiente es un ejemplo de regla de la base de datos NetWitness para ver las direcciones IP de origen y destino de un país de destino específico. Aquí, el país de origen se define como una variable `${local_Country}`.



En el tiempo de ejecución, se le solicitará ingresar el valor para la variable. En la figura siguiente se muestra la variable `local_Country`, donde puede ingresar el valor. Si ingresa el valor como **Estados Unidos**, se enumeran todas las direcciones IP de origen y destino con Estados Unidos como país de destino.



Puede usar la regla anterior para programar un informe. Para obtener más información, consulte Requisitos previos. Puede programar dos tipos de informes:

- Informe con variables dinámicas
- Informe iterativo

Informe con variables dinámicas

Las variables dinámicas permiten que el usuario especifique los valores de una variable definida en una regla durante la programación de un informe.

Para programar un informe con una variable dinámica:

1. En el menú de Security Analytics, haga clic en **Administration > Informes**.

   Se muestra la pestaña Administrar.

2. Haga clic en **Informes**.

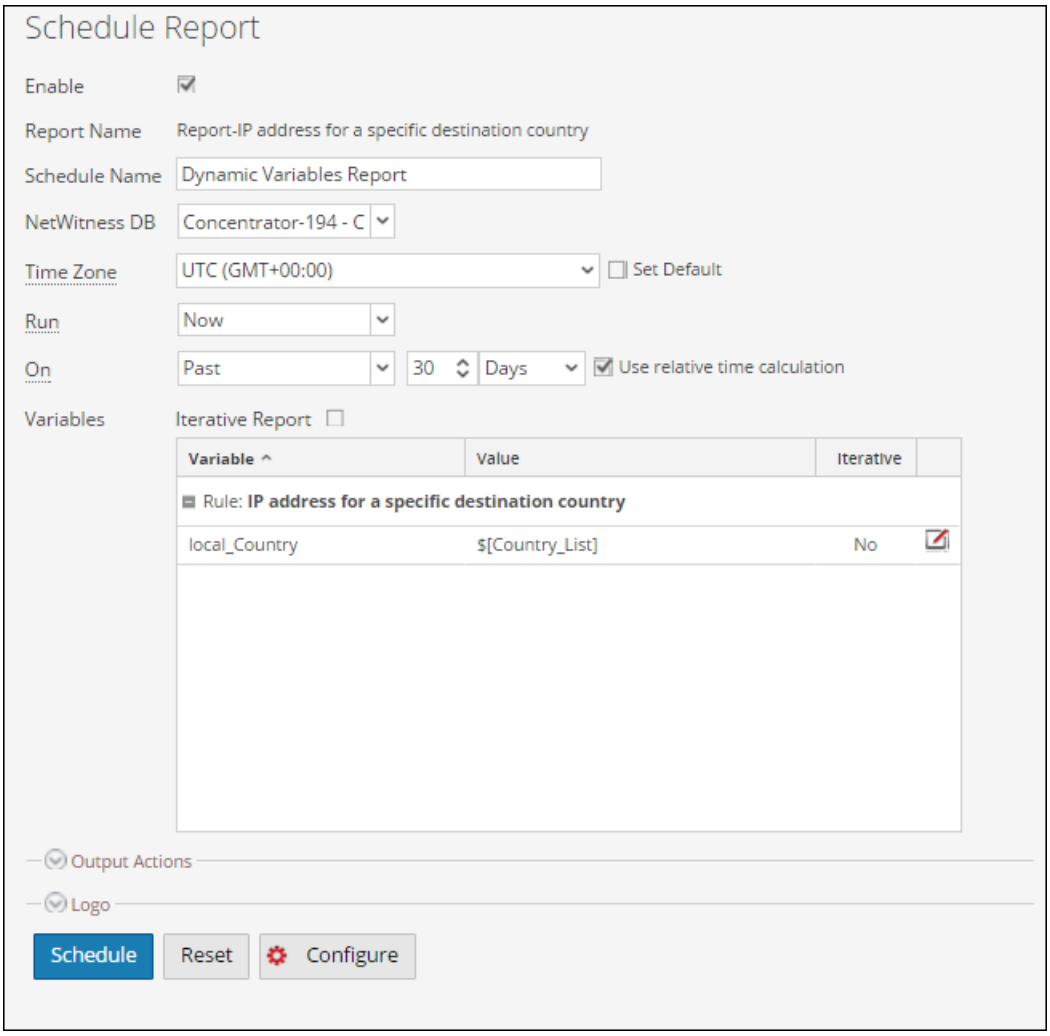
   Se muestra la vista Informe.

3. En la página **Crear informe**, haga clic en + para crear un informe.

4. Agregue la regla que tiene la variable definida por el usuario desde la pestaña Reglas.

5. Haga clic en **Schedule**.

   Se muestra la pestaña de la vista Calendarizar informe.



6. Para ejecutar los informes según el calendario, seleccione la casilla de verificación **Habilitar**.
7. En el campo **Nombre de calendario**, escriba un nombre para la configuración del informe del calendario.
8. En el campo **Origen de datos**, seleccione un origen de datos.

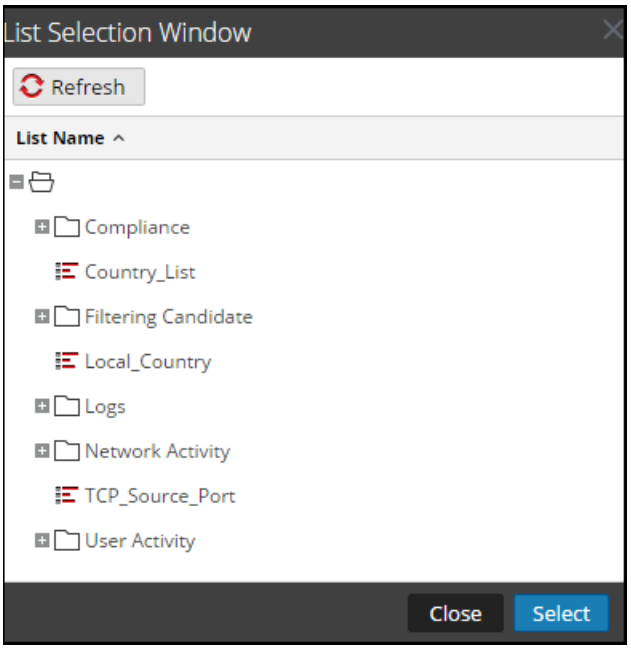
   Nota: si el origen de datos no se muestra, asegúrese de tener permisos de **lectura** configurados para el origen de datos. Esto se aplica a los orígenes de datos NWDB y Warehouse. Para obtener más información, consulte **Configurar permisos de orígenes de datos** en la *Guía de configuración de Reporting Engine*.
9. (Opcional) En el menú desplegable **Pool de recursos de Warehouse**, seleccione los pools o las líneas de espera disponibles en el clúster para programar el informe de modo que se ejecute en el pool o en la línea de espera. Este menú desplegable está disponible solo si selecciona un informe de base de datos de Warehouse.

Nota: Se enumeran todas las colas o los pools que ha especificado en la página Explorar para Reporting Engine. Si no se configuran pools o líneas de espera en la página Explorador, este menú desplegable se inhabilita y los trabajos se presentan a los clústeres sin ningún nombre de línea de espera o pool.

Nota: Si el pool o la línea de espera configurados en el calendario de informes se retira del clúster, en el Programador de capacidad, el nombre de la línea de espera permanece sin definir. Sin embargo, en el programador justo, el nombre del pool especificado se creará mediante la propiedad `mapred.fairscheduler.allow.undeclared.pool`.

10. En el menú desplegable Zona horaria, seleccione una zona horaria para mostrar todos los datos relacionados con tiempo en una salida de informe en el formato especificado. Este ajuste se puede configurar en la vista Explorar de Reporting Engine (/com.rsa.soc.re/configuration/reportoutputformatterconfig/reportoutputformatterconfig).
11. En el campo **Ejecutar**, seleccione el tipo de calendario de ejecución. (Por ejemplo, Ahora o Cada una hora). Según el tipo de calendario de ejecución, realice una de las siguientes acciones:
    - Si selecciona un calendario de ejecución **Después** o **Mensual**, debe proporcionar un valor para el día y la hora en el campo respectivo que se proporciona.
    - Si selecciona un calendario de ejecución **Por hora**, debe especificar los minutos en el campo **En el minuto**.
    - Si selecciona un programa que se ejecute **Diariamente**, debe ingresar un valor de hora en el campo **A las**.
    - Si selecciona un calendario de ejecución **Semanal**, debe ingresar un valor en el campo **A las** y, además, seleccionar los días de la semana.

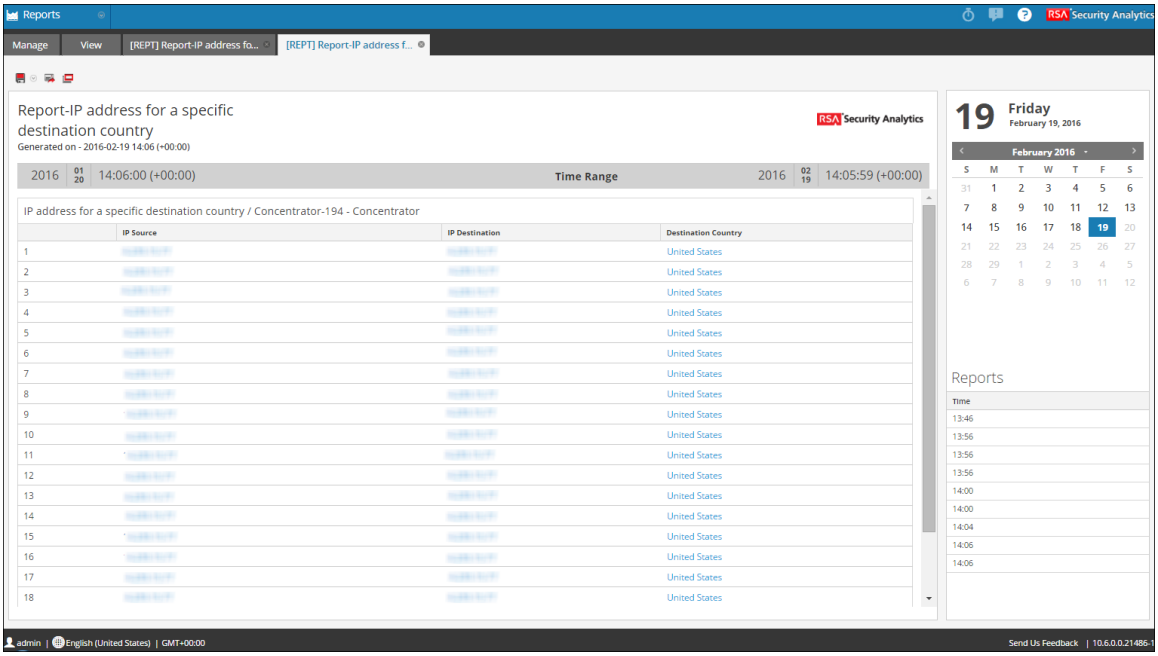
    Nota: Durante la programación de un informe, si selecciona la opción **Pasado**, la opción **Rango (específico/genérico)** o un rango de horas de finalización muy cercano a la hora actual, debe asegurarse de que se devuelvan los datos agregados en el origen de datos. Si hay una demora en la agregación en el origen de datos, esta se debe considerar en la hora de finalización que se selecciona o, de lo contrario, los informes pierden datos no agregados para ese rango de tiempo.
12. En el campo Variables, haga clic en  .
13. Realice una de las siguientes acciones
    - Ingrese el valor para la variable, o
    - Elija el valor de la lista para la variable.



14. Haga clic en **Seleccionar**.
15. Haga clic en **Schedule**.

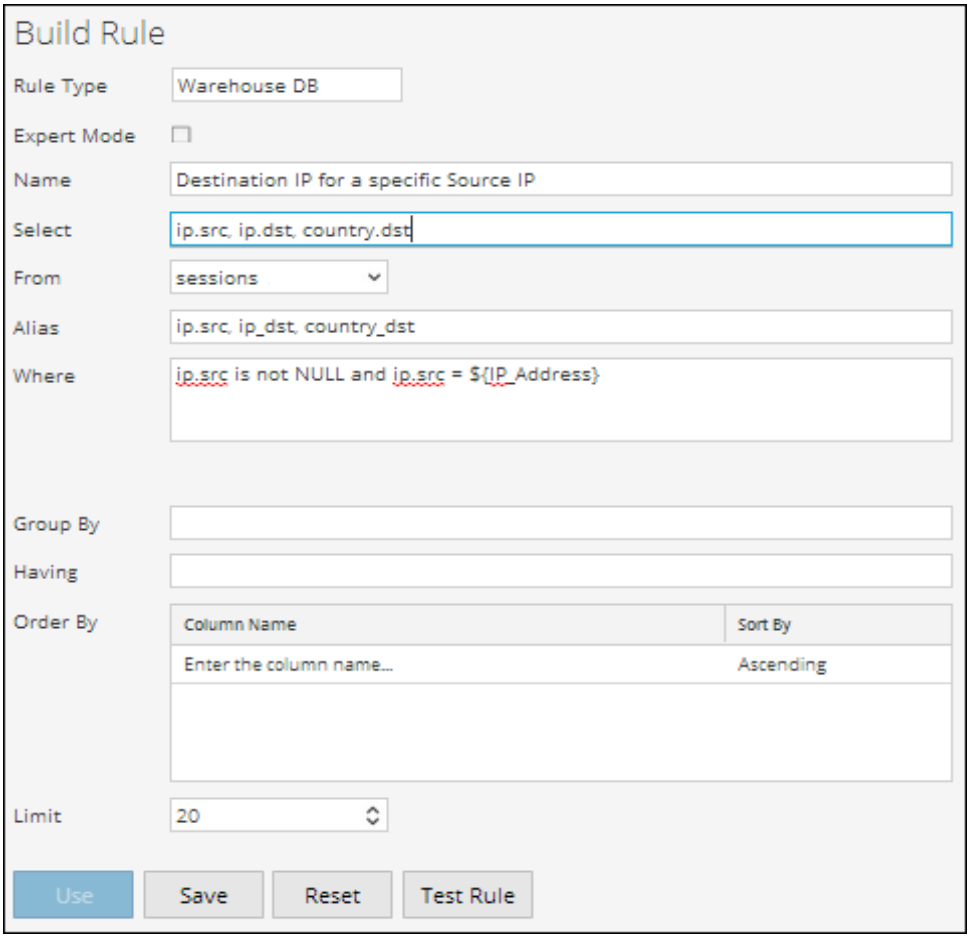
    El informe programado se ejecuta según lo programado y proporciona las salidas configuradas.

El informe programado se ejecuta según lo programado y proporciona las salidas configuradas.

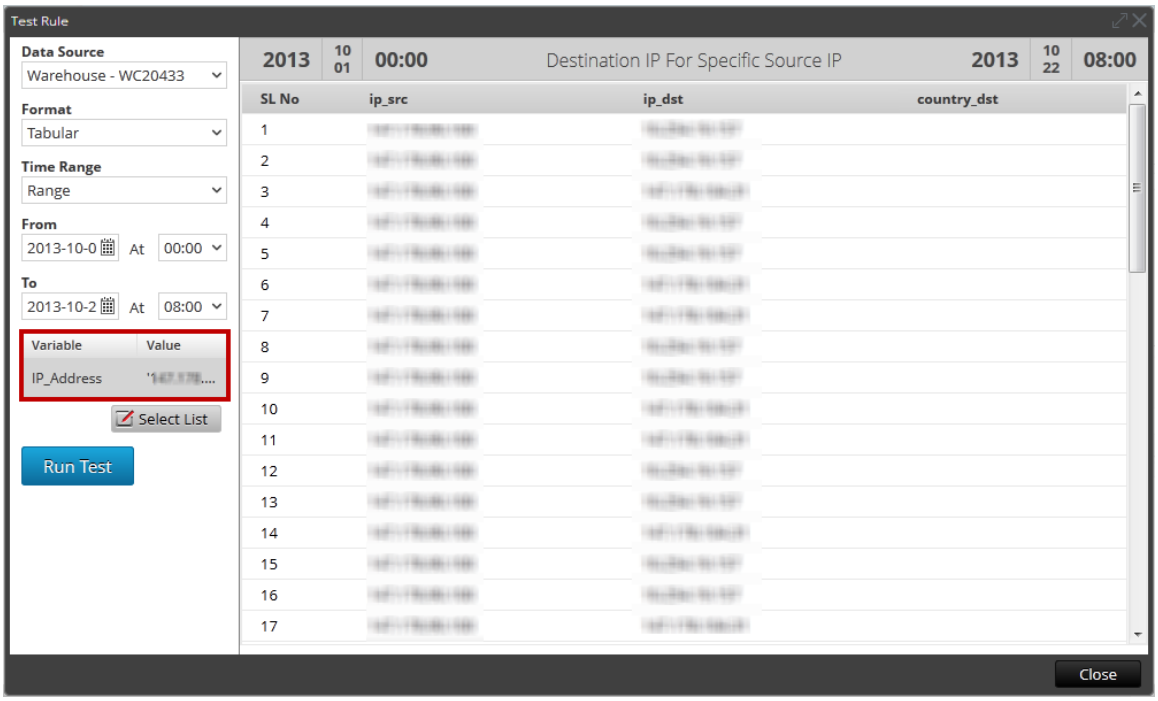


Ver todas las direcciones IP de destino para una dirección IP de origen

A continuación se incluye un ejemplo de regla de Warehouse para ver todas las direcciones IP de destino para un origen IP específico. La dirección IP de origen `ip_src` se define como una variable `${IP_Address}`.

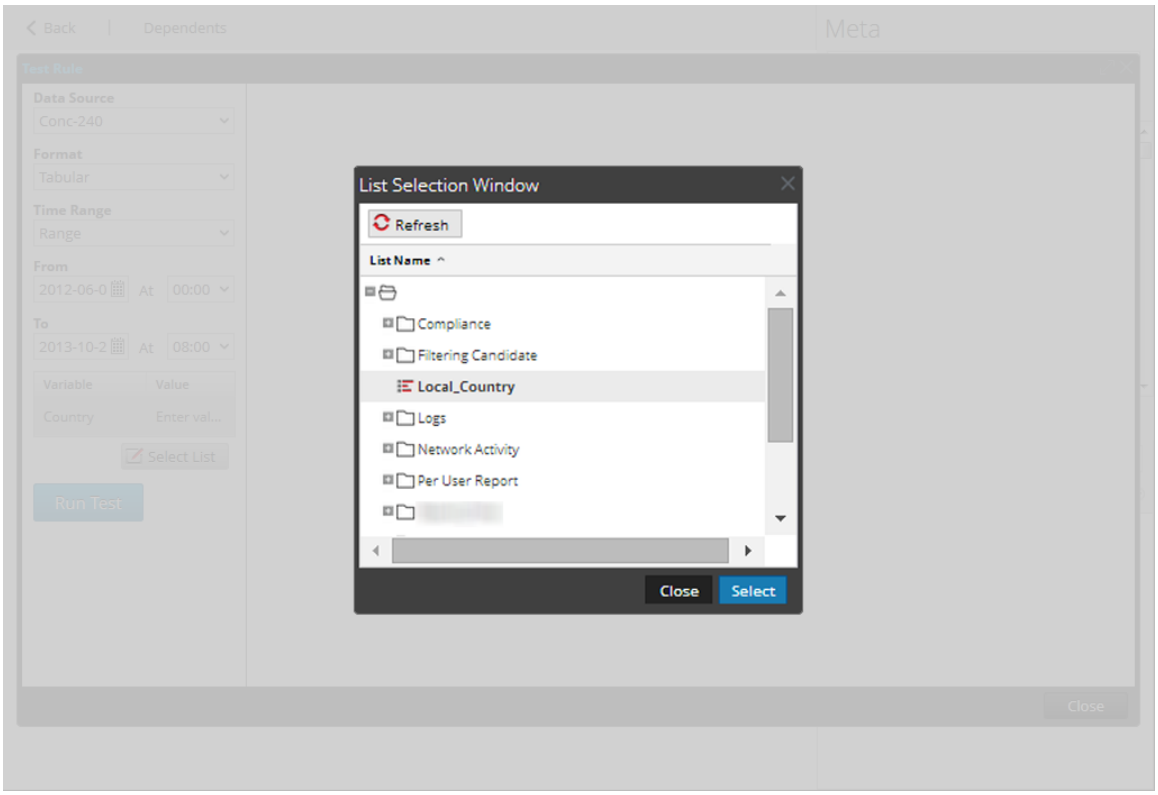


En el tiempo de ejecución, se le solicita ingresar la dirección IP de origen. En la siguiente figura se muestra la variable `IP_Address` y es posible ingresar una dirección IP de origen válida. Se enumeran todas las direcciones IP de destino con la IP de origen especificada.



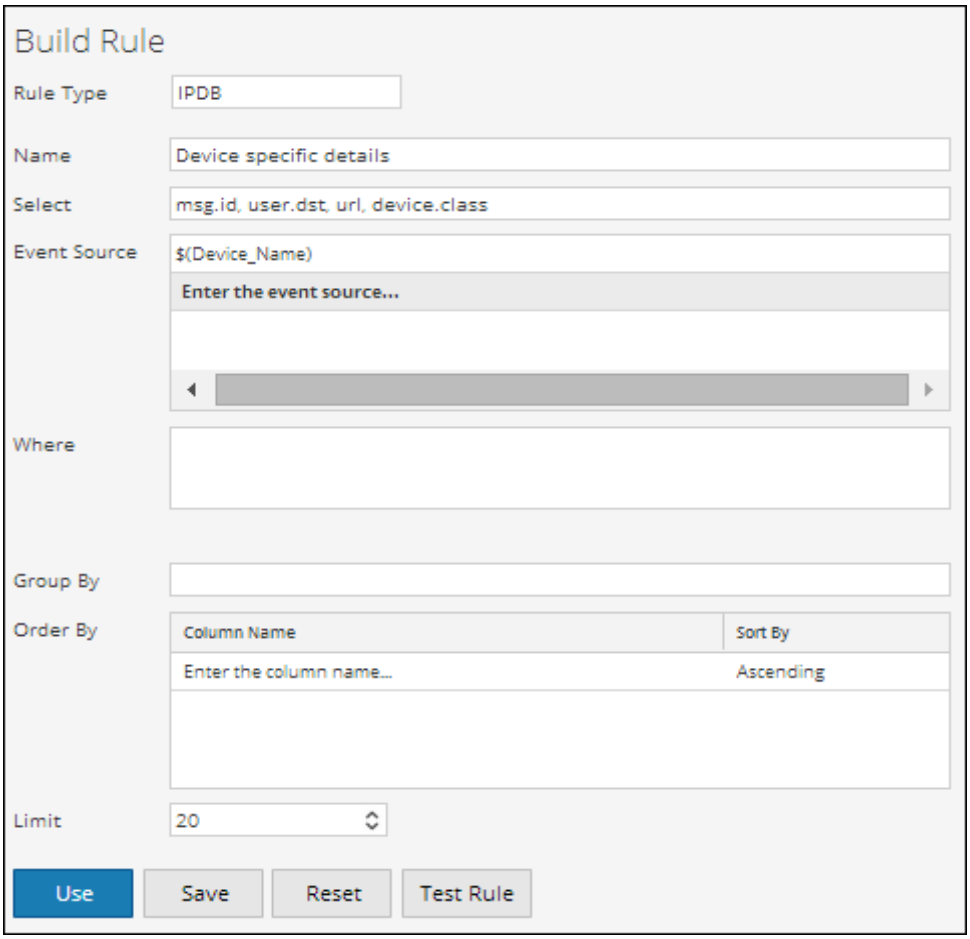
Asociar una variable a una lista de valores

Puede asociar la variable a una lista. Por ejemplo, puede crear una lista denominada `Local_Country` e ingresar todos los nombres de países como valores. Puede seleccionar la lista `Local_Country` como el valor para la variable `Local_Country`. En Configuración de ejecución, la lista `Local_Country` se completa y se puede seleccionar el país en función del cual se mostrarán los resultados.

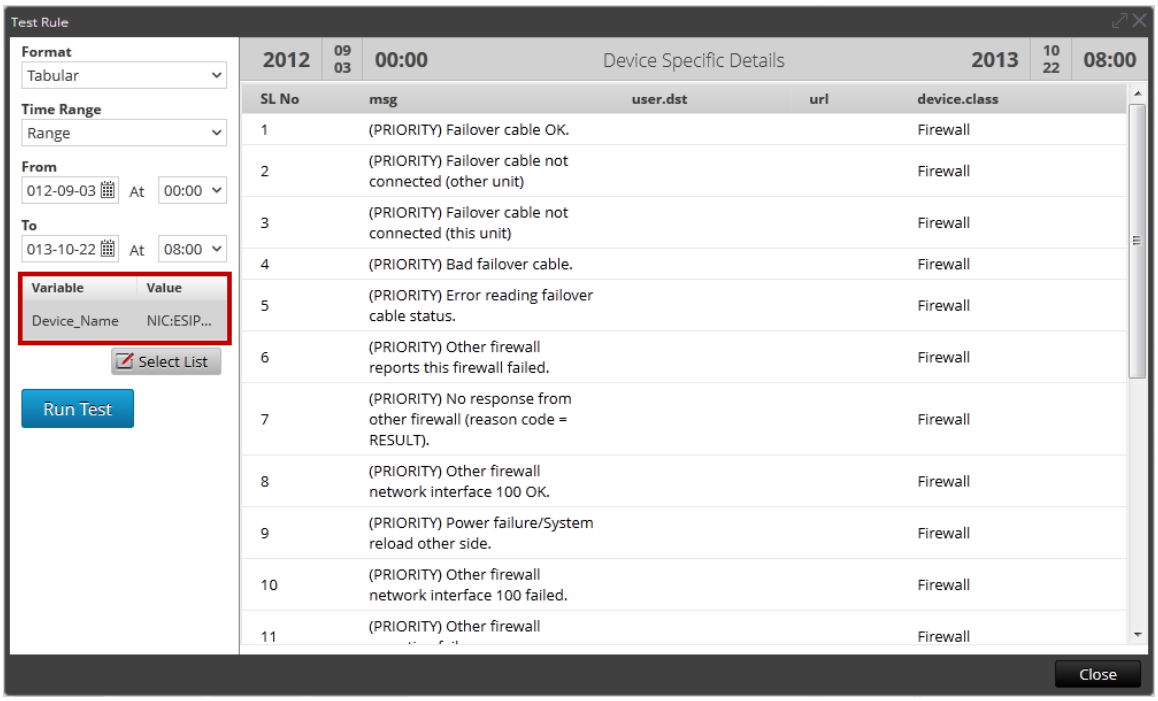


Regla de IPDB para ver los detalles de un dispositivo de acuerdo con el nombre del dispositivo

A continuación, se incluye un ejemplo de regla de IPDB para ver los detalles de un dispositivo de acuerdo con el nombre del dispositivo. En la especificación del origen de eventos, se especifica el nombre del dispositivo como una variable `${Device_Name}`.



En la hora de ejecución, se le solicita ingresar el nombre del dispositivo `Device_Name`. En la siguiente figura se muestra la variable `Device_Name` y puede ingresar la especificación de origen de eventos, por ejemplo, `NIC:ESIPDB:ESIPDB-ES:ciscopix:111.111.111.25`. Se muestran todos los detalles de los dispositivos.



Informe iterativo

Un informe iterativo genera un informe para cada valor de la lista.

Para programar un informe iterativo:

1. En el menú de Security Analytics, haga clic en **Administration > Informes**.

   Se muestra la pestaña Administrar.

2. Haga clic en **Informes**.

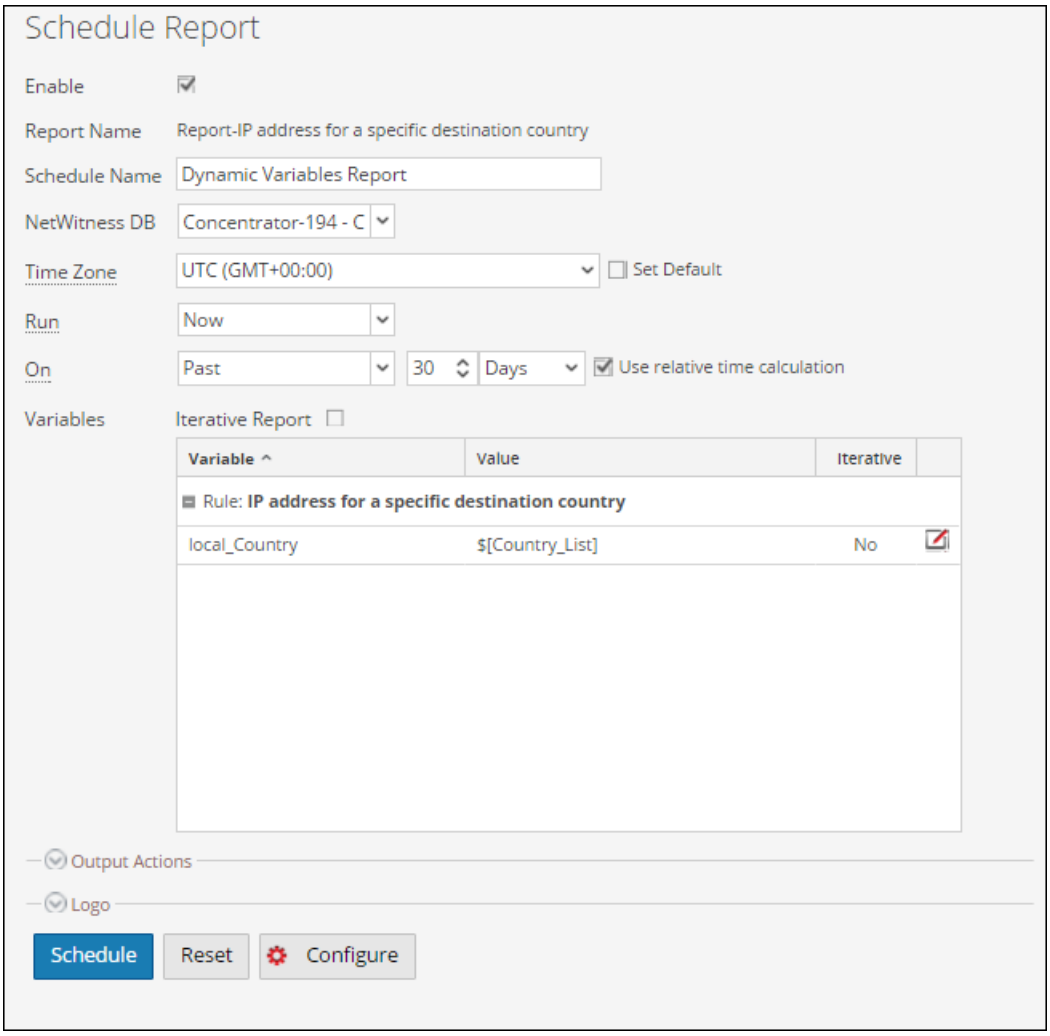
   Se muestra la vista Informe.

3. En la página **Crear informe**, haga clic en + para crear un informe.

4. Agregue la regla que tiene la variable definida por el usuario desde la pestaña Reglas.

5. Haga clic en **Schedule**.

   Se muestra la pestaña de la vista Calendarizar informe.



6. Para ejecutar los informes según el calendario, seleccione la casilla de verificación **Habilitar**.
7. En el campo **Nombre de calendario**, escriba un nombre para la configuración del informe del calendario.
8. En el campo **Origen de datos**, seleccione un origen de datos.

   Nota: si el origen de datos no se muestra, asegúrese de tener permisos de **lectura** configurados para el origen de datos. Esto se aplica a los orígenes de datos NWDB y Warehouse. Para obtener más información, consulte **Configurar permisos de orígenes de datos** en la *Guía de configuración de Reporting Engine*.
9. (Opcional) En el menú desplegable **Pool de recursos de Warehouse**, seleccione los pools o las líneas de espera disponibles en el clúster para programar el informe de modo que se ejecute en el pool o en la línea de espera. Este menú desplegable está disponible solo si selecciona un informe de base de datos de Warehouse.

Nota: Se enumeran todas las colas o los pools que ha especificado en la página Explorar para Reporting Engine. Si no se configuran pools o líneas de espera en la página Explorador, este menú desplegable se inhabilita y los trabajos se presentan a los clústeres sin ningún nombre de línea de espera o pool.

Nota: Si el pool o la línea de espera configurados en el calendario de informes se retira del clúster, en el Programador de capacidad, el nombre de la línea de espera permanece sin definir. Sin embargo, en el programador justo, el nombre del pool especificado se creará mediante la propiedad `mapred.fairscheduler.allow.undeclared.pool`.

10. En el menú desplegable Zona horaria, seleccione una zona horaria para mostrar todos los datos relacionados con tiempo en una salida de informe en el formato especificado. Este ajuste se puede configurar en la vista Explorar de Reporting Engine (/com.rsa.soc.re/configuration/reportoutputformatterconfig/reportoutputformatterconfig).
11. En el campo **Ejecutar**, seleccione el tipo de calendario de ejecución. (Por ejemplo, Ahora o Cada una hora). Según el tipo de calendario de ejecución, realice una de las siguientes acciones:
    - Si selecciona un calendario de ejecución **Después** o **Mensual**, debe proporcionar un valor para el día y la hora en el campo respectivo que se proporciona.
    - Si selecciona un calendario de ejecución **Por hora**, debe especificar los minutos en el campo **En el minuto**.
    - Si selecciona un programa que se ejecute **Diariamente**, debe ingresar un valor de hora en el campo **A las**.
    - Si selecciona un calendario de ejecución **Semanal**, debe ingresar un valor en el campo **A las** y, además, seleccionar los días de la semana.

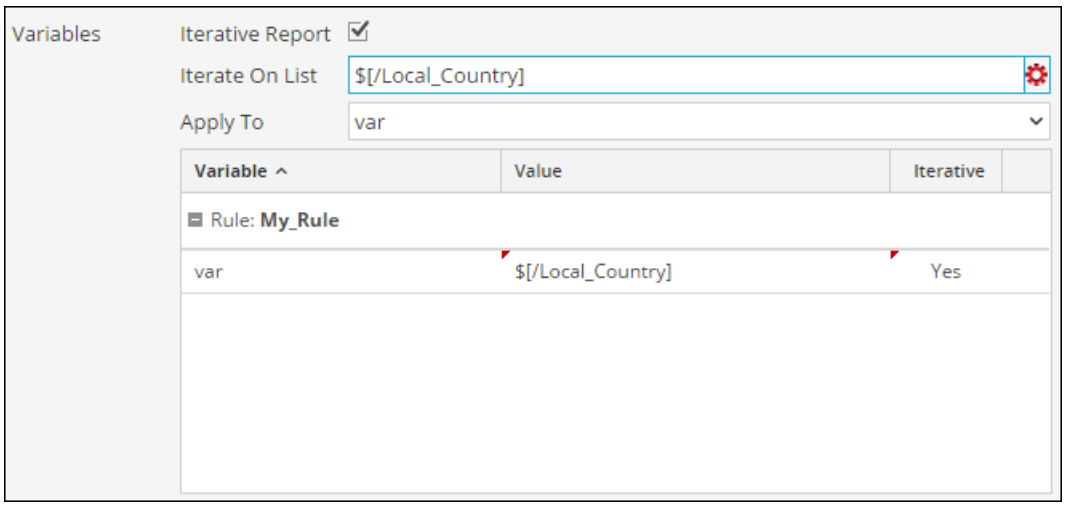
    Nota: Durante la programación de un informe, si selecciona la opción **Pasado**, la opción **Rango (específico/genérico)** o un rango de horas de finalización muy cercano a la hora actual, debe asegurarse de que se devuelvan los datos agregados en el origen de datos. Si hay una demora en la agregación en el origen de datos, esta se debe considerar en la hora de finalización que se selecciona o, de lo contrario, los informes pierden datos no agregados para ese rango de tiempo.
12. En el campo Variables, realice lo siguiente:
    a. Para ejecutar informes iterativos, seleccione la casilla de verificación **Informe iterativo**.
    b. Para el valor Iterar en lista, haga clic en  .

       Se abre la ventana Selección de lista.

c. Seleccione una lista y haga clic en **Seleccionar**.

   El elemento de lista seleccionado se agrega al campo **Iterar en lista**.

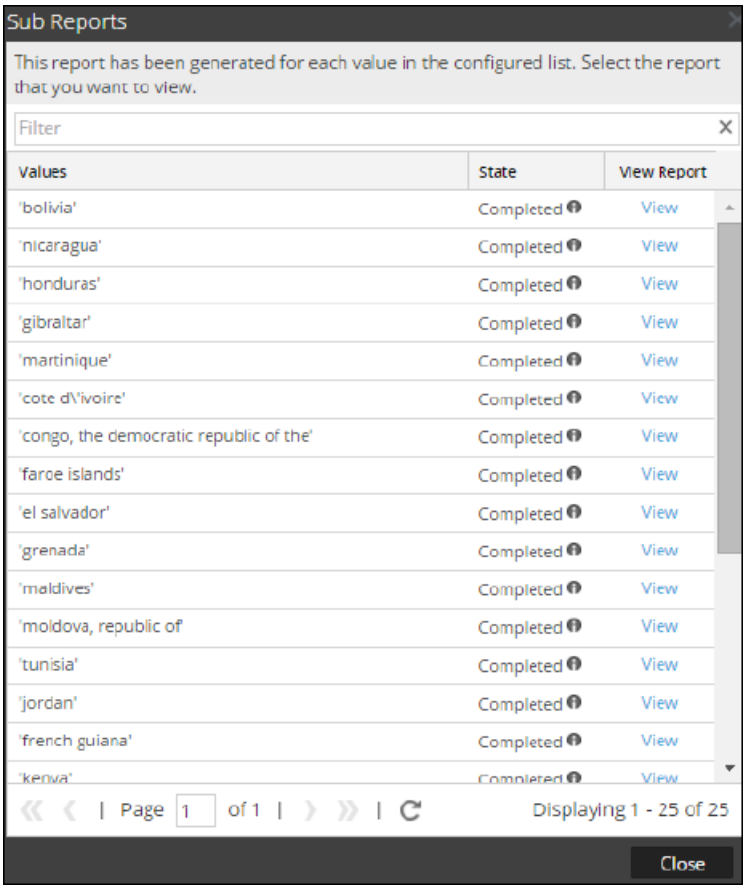
d. Seleccione la variable en la cual se debe aplicar el valor de lista seleccionado.

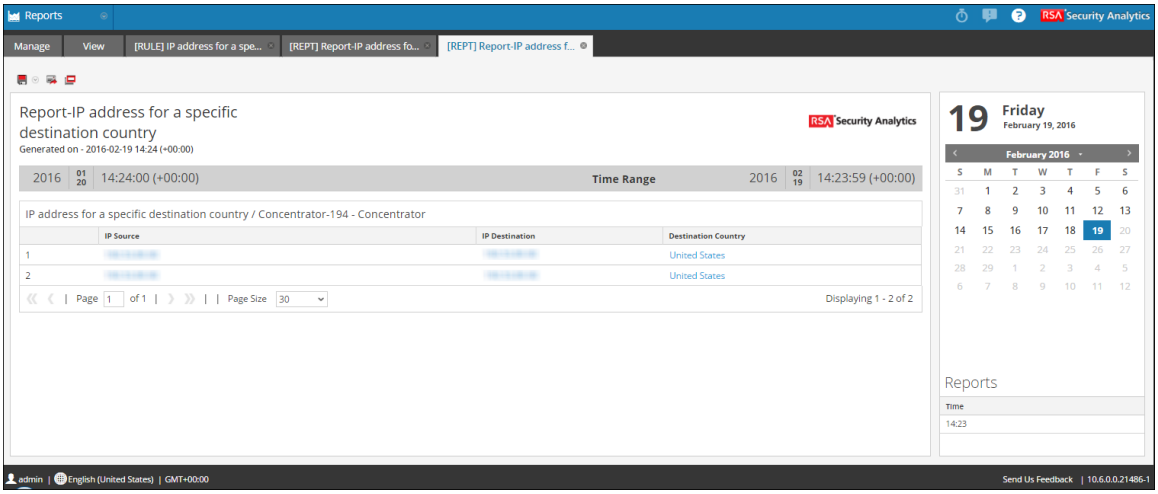


13. Haga clic en **Schedule**.

    El informe programado se ejecuta según lo programado y proporciona las salidas configuradas.

En la siguiente figura se muestra la vista Informe iterativo.


Sub Reports
This report has been generated for each value in the configured list. Select the report that you want to view.
Filter
Values
State
View Report
'bolivia' Completed View
'nicaragua' Completed View
'honduras' Completed View
'gibraltar' Completed View
'martinique' Completed View
'cote d\'ivoire' Completed View
'congo, the democratic republic of the' Completed View
'faroe islands' Completed View
'el salvador' Completed View
'grenada' Completed View
'maldives' Completed View
'moldova, republic of' Completed View
'tunisia' Completed View
'jordan' Completed View
'french guiana' Completed View
'kenya' Completed View
Page 1 of 1
Displaying 1 - 25 of 25
Close


Reports
RSA Security Analytics
Manage
View
[RULE] IP address for a spe...
[REPT] Report-IP address fo...
[REPT] Report-IP address f...
Report-IP address for a specific destination country
Generated on - 2016-02-19 14:24 (+00:00)
RSA Security Analytics
2016 01 20 14:24:00 (+00:00)
Time Range
2016 02 19 14:23:59 (+00:00)
IP address for a specific destination country / Concentrator-194 - Concentrator
IP Source
IP Destination
Destination Country
1
United States
2
United States
Page 1 of 1
Page Size 30
Displaying 1 - 2 of 2
19 Friday
February 19, 2016
February 2016
Reports
Time
14:23
admin
English (United States)
GMT+00:00
Send Us Feedback
10.6.0.0.21486-1

Trabajar con gráficos en el módulo Reporting

El módulo Gráficos se usa para definir y ver gráficos.

Temas

- Descripción general de un gráfico
- Definir grupos de gráficos y gráficos
- Administrar el acceso para un gráfico o un grupo de gráficos
- Probar un gráfico
- Investigar un gráfico

Descripción general de un gráfico

Cualquier regla en el sistema Security Analytics que no se ordena por nada se puede utilizar para crear instantáneamente un gráfico. En Security Analytics, el intervalo de gráfico se puede ajustar desde el panel de definición de gráfico mismo. Cada vez que se ejecuta un gráfico, almacena sus datos de resultados de manera lógica en el Reporting Engine, de modo que se puede revisar en la vista Tablero o la vista Gráfico sin ninguna consideración de rendimiento. En la siguiente sección se detalla cómo se crean, se configuran y se agregan gráficos a la línea de espera de gráficos global para generar datos.

Un gráfico consta de lo siguiente:

Propiedad	Descripción	Ejemplo
Nombre del gráfico **Nota:** En el campo **Nombre**, el ícono para expandir el tamaño de la columna no se muestra al final del campo de la columna. Debe mover el mouse un poco hacia la izquierda para ver el ícono que permite ampliar la columna.	Se usa para identificar el gráfico.	Chart1
Base de la regla	Identifica la ruta de regla elegida para la jerarquía de carpeta.	

Nota: En la interfaz del usuario de Reporting, la salida del campo donde se muestra la fecha y la hora está siempre de acuerdo con el perfil de zona horaria que seleccionó el usuario.

Definir grupos de gráficos y gráficos

Este tema es un conjunto de tareas para configurar grupos de gráficos y gráficos. Puede definir, eliminar, editar, importar y exportar gráficos en Security Analytics. Cada tema describe los procedimientos pertinentes.

Temas:

- Agregar un gráfico
- Agregar un grupo de gráficos
- Eliminar un gráfico
- Eliminar un grupo de gráficos
- Desactivar un gráfico
- Arrastrar y soltar un gráfico en un grupo
- Duplicar un gráfico
- Editar un gráfico
- Activar un gráfico
- Exportar un gráfico
- Exportar un grupo de gráficos
- Importar gráficos y grupos de gráficos
- Actualizar grupo o lista de gráficos
- Buscar un gráfico existente
- Ver la lista de todos los gráficos
- Ver un gráfico

Agregar un gráfico

Usar variables para creación de informes con parámetros

En este tema se proporcionan instrucciones para agregar gráficos a un grupo o subgrupo.

Requisitos previos

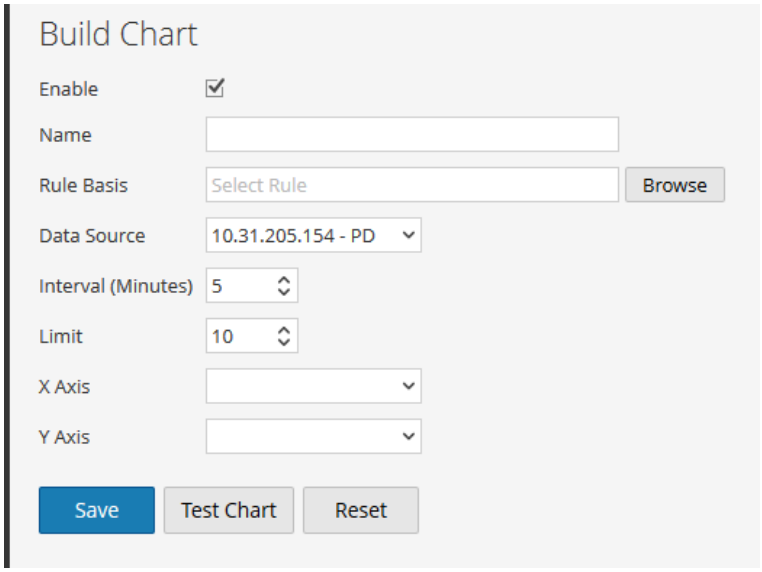
Asegúrese de:

- Haber definido reglas antes de agregar un gráfico.
- Haber comprendido los componentes de la vista Crear gráfico. Para obtener más información, consulte Vista Crear gráfico.

Procedimiento

Realice los siguientes pasos para agregar gráficos a un grupo o subgrupo:

1. En el menú de **Security Analytics**, seleccione **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Gráficos** para mostrar la vista Gráfico.
3. En la barra de herramientas **Gráfico**, haga clic en .
   Se muestra la pestaña de la vista Crear gráfico.



4. Ingrese el nombre del gráfico.
5. Para que Reporting Engine recopile los datos y genere resultados de gráficos, seleccione la casilla de verificación **Activar**.
6. En el campo Base de la regla, realice lo siguiente:

   Nota: Si la regla contiene la acción de regla lookup_and_add, sum_count o sum_values, el gráfico asociado no incluye datos.

   a. Haga clic en **Navegar**. Se muestra el cuadro de diálogo Agregar regla.

b. Navegue al árbol Regla y seleccione una regla.

c. Haga clic en **Seleccionar**.

7. La Regla aparece en el campo Base de la regla.
8. Seleccione el origen de datos en la lista desplegable **Origen de datos**.

> **Nota:** Si el origen de datos no se muestra, asegúrese de tener permisos de **lectura** configurados para el origen de datos. Esto se aplica a los orígenes de datos NWDB y Warehouse. Para obtener más información, consulte el tema Configurar permisos de orígenes de datos en la *Guía de configuración de hosts y servicios*.

9. (Opcional) Para modificar el valor del intervalo, haga clic en la flecha hacia arriba o hacia abajo.
   El valor del intervalo es el intervalo en minutos en el cual la regla que forma la base del gráfico se ejecuta para recopilar datos.
10. Seleccione el valor **Límite** para limitar la cantidad de registros que se mostrarán.
11. **Eje X** y **Eje Y** se usan para especificar los metadatos que se trazarán en los gráficos.
    En **Eje X** se muestran los metadatos de la regla "Group by". En **Eje Y** se muestran las funciones de agregado que se usan en la regla.

> **Nota:** Sum, Count, Countdistinct y Average son las funciones de agregado compatibles con el gráfico. De manera predeterminada, para las reglas personalizadas con múltiples "Group by", puede seleccionar solo los primeros metadatos en el **Eje X**.

12. Haga clic en **Guardar**.
    Se muestra un mensaje de confirmación que indica que el gráfico se guardó correctamente.

Los próximos pasos

Realice las siguientes tareas:

- Puede editar, eliminar o actualizar un gráfico en el panel Gráficos.
- Puede probar un gráfico en la Vista Probar un gráfico.

Agregar un grupo de gráficos

En este tema se proporcionan instrucciones para agregar grupos a la carpeta predeterminada o agregar subgrupos bajo un grupo de gráficos. Puede organizar los gráficos en estas carpetas y subcarpetas.

Requisitos previos

Asegúrese de haber comprendido los componentes de la vista Gráfico. Para obtener más información, consulte Vista Gráfico.

Procedimiento

Realice los siguientes pasos para agregar grupos a la carpeta predeterminada o agregar subgrupos en un grupo de gráficos:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Gráficos**.
   Se muestra la vista Gráfico.
3. En el panel **Grupos de gráficos**, haga clic en  .
   Se agrega un grupo predeterminado en el panel Grupos de gráficos.
4. Ingrese el nombre del nuevo grupo.
5. Presione **Enter**.
   El grupo se agrega al panel Grupos de gráficos.

Los próximos pasos

Puede agregar gráficos al grupo de gráficos.

Eliminar un gráfico

En este tema se proporcionan instrucciones para eliminar gráficos en un grupo o subgrupo.

Requisitos previos

Asegúrese de haber comprendido los componentes de la vista Gráfico. Para obtener más información, consulte Vista Gráfico.

Procedimiento

Realice los siguientes pasos para eliminar gráficos en un grupo o un subgrupo:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Gráficos**.
   Se muestra la vista Gráfico.

3. En el panel **Lista de gráficos**, realice una de las siguientes acciones:

   - Seleccione los gráficos y haga clic en .
   - Haga clic en > **Eliminar**.

     Una confirmación le preguntará si desea eliminar el gráfico seleccionado.

4. Haga clic en **Sí** para eliminar el gráfico.

   Se muestra un mensaje que confirma la correcta eliminación del gráfico y el gráfico seleccionado se elimina del panel Lista de gráficos.

Eliminar un grupo de gráficos

En este tema se proporcionan instrucciones para eliminar grupos de gráficos de la carpeta predeterminada o subgrupos bajo un grupo de gráficos.

Requisitos previos

Asegúrese de:

- Que no haya gráficos asociados al grupo de gráficos.
- Haber comprendido la vista Gráfico. Para obtener más información, consulte Vista Gráfico.

Procedimiento

Realice los siguientes pasos para eliminar grupos de gráficos de la carpeta predeterminada o subgrupos bajo un grupo de gráficos:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.

   Se muestra la pestaña Administrar.

2. Haga clic en **Gráficos**.

   Se muestra la vista Gráfico.

3. En el panel **Grupos de gráficos**, seleccione el grupo y haga clic en .

   Un cuadro de diálogo de confirmación solicita confirmar que desea eliminar el grupo seleccionado.

4. Haga clic en **Sí** para eliminar el grupo.

   El grupo seleccionado se elimina del panel Grupos de gráficos.

Desactivar un gráfico

En este tema se proporcionan instrucciones para desactivar un gráfico. Si se desactiva un gráfico, el gráfico calendarizado se desactiva con un mensaje de confirmación y el estado del gráfico se cambia a “Cerrado”.

Requisitos previos

Asegúrese de haber comprendido los componentes de la vista Gráfico. Para obtener más información, consulte Vista Gráfico.

Procedimiento

Realice los siguientes pasos para inhabilitar un gráfico:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Gráficos**.
   Se muestra la vista Gráfico.
3. En el panel **Lista de gráficos**, seleccione uno o varios gráficos que muestran ● en la columna **Activado**.
4. Haga clic en ○.
   Un mensaje de confirmación indica que el estado del gráfico se cambió exitosamente.

Arrastrar y soltar un gráfico en un grupo

En este tema se proporcionan instrucciones para arrastrar y soltar un gráfico desde el panel Lista de gráficos en un grupo del panel Grupos de gráficos.

Requisitos previos

Asegúrese de haber comprendido los componentes de la vista Gráfico. Para obtener más información, consulte Vista Gráfico.

Procedimiento

Realice los siguientes pasos para arrastrar y soltar un gráfico desde el panel Lista de gráficos en un grupo en el panel Grupos de gráficos:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Gráficos**.
   Se muestra la vista Gráfico.

3. Seleccione un gráfico en el panel **Lista de gráficos** y arrástrelo y suéltelo a un grupo en el panel **Grupos de gráficos**.
   El gráfico se copia al grupo en el panel Grupos de gráficos.

Duplicar un gráfico

En este tema se proporcionan instrucciones para duplicar un gráfico existente. El gráfico duplicado se muestra en el panel Lista de gráficos con sufijos. Por ejemplo, Chart(1).

Requisitos previos

Asegúrese de haber comprendido los componentes de la vista Gráfico. Para obtener más información, consulte Vista Gráfico.

Procedimiento

Realice los siguientes pasos para duplicar un gráfico existente:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Gráficos**.
   Se muestra la vista Gráfico.
3. En el panel **Lista de gráficos**, seleccione un gráfico para duplicar.
4. En la barra de herramientas **Gráfico**, haga clic en  .
   El gráfico se duplica y se agrega al panel Lista de gráficos.

Los próximos pasos

Puede transferir el gráfico duplicado a otro grupo. Para obtener más información, consulte Arrastrar y soltar un gráfico en un grupo.

Editar un gráfico

En este tema se proporcionan instrucciones para editar gráficos en un grupo o un subgrupo.

Requisitos previos

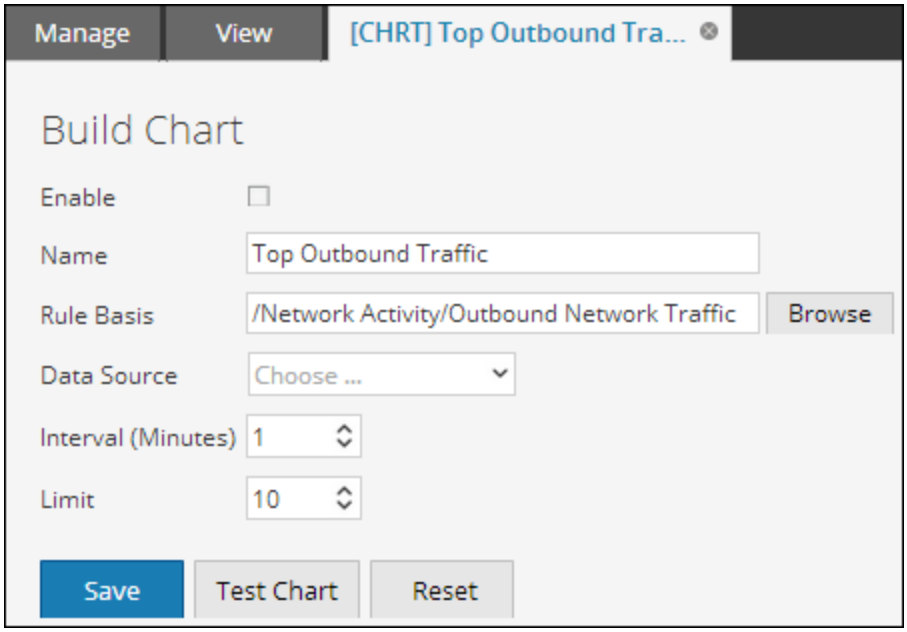
Asegúrese de haber comprendido los componentes de la vista Crear gráfico. Para obtener más información, consulte Vista Crear gráfico.

Procedimiento

Realice los siguientes pasos para editar gráficos en un grupo o un subgrupo:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.

2. Haga clic en **Gráficos**.
   Se muestra la vista Gráfico.
3. En el panel **Lista de gráficos**, realice una de las siguientes acciones:
   - Haga doble clic en un gráfico o seleccione uno y haga clic en .
   - Seleccione un gráfico y haga clic en > **Editar**.
     Se muestra la pestaña de la vista Crear gráfico.



4. Modifique el nombre del gráfico.
5. Para que Reporting Engine recopile los datos y genere resultados de gráficos, seleccione la casilla de verificación **Activar**.
6. (Opcional) En el campo **Base de la regla**, realice lo siguiente:
   a. Haga clic en **Navegar**.
      Se muestra el cuadro de diálogo Agregar regla.
   b. Navegue al árbol Regla y seleccione una regla.
   c. Haga clic en **Seleccionar**.
      La Regla aparece en el campo Base de la regla.
7. Seleccione el origen de datos en la lista desplegable **Origen de datos**.

Nota: si el origen de datos no se muestra, asegúrese de tener permisos de **lectura** configurados para el origen de datos. Esto se aplica a los orígenes de datos NWDB y Warehouse. Para obtener más información, consulte el tema Configurar permisos de orígenes de datos en la *Guía de configuración de hosts y servicios*.

8. (Opcional) Para modificar el valor del intervalo, haga clic en las flechas hacia arriba o hacia abajo.
9. Seleccione el valor límite para limitar la cantidad de registros que se mostrarán.
10. Haga clic en **Guardar**.
    Se muestra un mensaje de confirmación que indica que el gráfico se editó correctamente.

Activar un gráfico

En este tema se proporcionan instrucciones para activar un gráfico. Al activar un gráfico, el gráfico se ejecuta según lo calendarizado y proporciona el resultado configurado mientras que el estado del gráfico se cambia a “En ejecución”.

Nota: De manera predeterminada, el gráfico se activa cuando se agrega al panel Lista de gráficos.

Requisitos previos

Asegúrese de haber comprendido los componentes de la vista Gráfico. Para obtener más información, consulte Vista Gráfico

Procedimiento

Realice los siguientes pasos para habilitar un gráfico:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Gráficos**.
   Se muestra la vista Gráfico.
3. En el panel **Lista de gráficos**, seleccione uno o varios gráficos que muestran ○ en la columna **Activado**.
4. Haga clic en ●.
   Un mensaje de confirmación indica que el estado de los gráficos se cambió exitosamente.

Exportar un gráfico

En este tema se proporcionan instrucciones para exportar gráficos seleccionados a un archivo externo que posteriormente se puede importar en otro ambiente de Security Analytics.

Requisitos previos

Asegúrese de que haya gráficos enumerados en el grupo de gráficos.

Procedimiento

Realice los siguientes pasos para exportar los gráficos seleccionados a un archivo externo:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Gráficos**.
   Se muestra la vista Gráfico.
3. En el panel **Lista de gráficos**, realice una de las siguientes acciones:

   - Seleccione un gráfico y haga clic en  > **Exportar**.
   - Haga clic en  > **Exportar**.
     El archivo exportado se guarda en la unidad local.

Exportar un grupo de gráficos

En este tema se proporcionan instrucciones para exportar grupos de gráficos seleccionados a un archivo externo que pueda importarse posteriormente a otro ambiente de Security Analytics.

Requisitos previos

Asegúrese de que haya gráficos enumerados en el grupo de gráficos.

Procedimiento

Realice los siguientes pasos para exportar grupos de gráficos seleccionados

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Gráficos**.
   Se muestra la vista Gráfico.
3. En el panel **Grupos de gráficos**, seleccione un grupo de gráficos y haga clic en 
   > **Exportar**.
   El archivo exportado se guarda en la unidad local.

Importar gráficos y grupos de gráficos

En este tema se proporcionan instrucciones para importar gráficos que contienen subgrupos y gráficos de otras instancias de Security Analytics en el panel Grupos de gráficos. Los gráficos deben estar en un archivo binario válido que se haya exportado desde otra instancia de Security Analytics.

Durante el proceso de importación, debe seleccionar el archivo binario y especificar si los gráficos existentes se deben sobrescribir con gráficos del mismo nombre incluidos en el archivo binario de importación.

- Si decide sobrescribirlos, todas las reglas, las listas y los gráficos duplicados se sobrescribirán con los contenidos del archivo binario de importación.
- Si decide no sobrescribirlos y existe una regla, una lista o un gráfico duplicados en la carpeta de destino, la importación se realizará y no se mostrará ningún mensaje acerca de los gráficos duplicados.

Requisitos previos

Asegúrese de disponer de gráficos o grupos de gráficos exportados desde otras instancias de Security Analytics.

Procedimiento

Realice los siguientes pasos para importar gráficos desde otras instancias de Security Analytics:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Gráficos**.
   Se muestra la vista Gráfico.
3. En el panel **Grupos de gráficos**, seleccione una carpeta para importar el archivo.
4. Realice una de las siguientes acciones

   - En el panel Grupos de gráficos, haga clic en  > **Importar**.
   - En la barra de herramientas Gráfico, haga clic en  > **Importar**.
     Se muestra el cuadro de diálogo **Importar gráfico**.
5. Haga clic en **Navegar** para seleccionar el archivo binario.
   Security Analytics proporciona una vista del sistema de archivos de los archivos.
6. Busque el archivo binario y haga clic en **Abrir**.
   El archivo se agrega a la lista Importar gráfico.

7. (Opcional) Para sobrescribir cualquier regla existente en la biblioteca con una regla de nombre idéntico en el archivo binario cuando se realiza la importación, seleccione la casilla de verificación **Regla**. Si no selecciona la opción Sobrescribir y se encuentra una regla idéntica en el archivo binario, este archivo se importa y no se muestra ningún mensaje de error.
8. (Opcional) Para sobrescribir cualquier lista existente en la biblioteca con una lista de nombre idéntico en el archivo binario, seleccione la casilla de verificación **Lista**. Si no selecciona la opción Sobrescribir y se encuentra una lista idéntica en el archivo binario, este archivo se importa y no se muestra ningún mensaje de error.
9. (Opcional) Para sobrescribir cualquier gráfico existente en la biblioteca con un gráfico de nombre idéntico en el archivo binario cuando se realiza la importación, seleccione la casilla de verificación **Gráfico**. Si no selecciona la opción Sobrescribir y se encuentra un gráfico idéntico en el archivo binario, este archivo se importa y no se muestra ningún mensaje de error.
10. Haga clic en **Importar** para importar el archivo binario.

Actualizar grupo o lista de gráficos

En este tema se proporcionan instrucciones sobre cómo actualizar un grupo de gráficos o gráficos individuales para ver la nueva disposición de grupos o gráficos.

Procedimiento

Realice los siguientes pasos para actualizar un grupo de gráficos o gráficos individuales:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Gráficos**.
   Se muestra la vista Gráfico.
3. Siga uno de los procedimientos que se presentan a continuación:

   - En el panel **Grupos de gráficos**, arrastre y suelte el grupo.
     El grupo de gráficos se transfiere a la ubicación nueva.
   - En el panel **Lista de gráficos**, arrastre y suelte los gráficos en el grupo deseado del panel Grupos de gráficos.
     Los gráficos se transfieren a la nueva ubicación.

4. Haga lo siguiente:

   - En el panel **Grupos de gráficos**, haga clic en .
     El grupo de gráficos se actualiza.
   - En el panel **Lista de gráficos**, haga clic en .
   - En el panel de la **barra de herramientas Gráfico**, seleccione **Actualización automática**.
     La lista de gráficos se actualiza.

Buscar un gráfico existente

En este tema se proporcionan instrucciones para buscar un gráfico existente mediante el ingreso de texto como una subcadena en el cuadro de búsqueda de la barra de herramientas Gráfico.

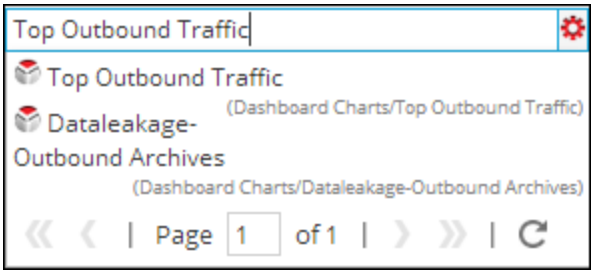
Requisitos previos

Asegúrese de haber definido gráficos antes de realizar esta tarea.

Procedimiento

Realice los siguientes pasos para buscar un gráfico existente:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Gráficos**.
   Se muestra la vista Gráfico.
3. En la barra de herramientas **Gráfico**, ingrese texto en el cuadro de texto Buscar.
4. Haga clic en > **Gráfico**.
   Los gráficos con la subcadena en su nombre aparecen en la lista desplegable de búsqueda.



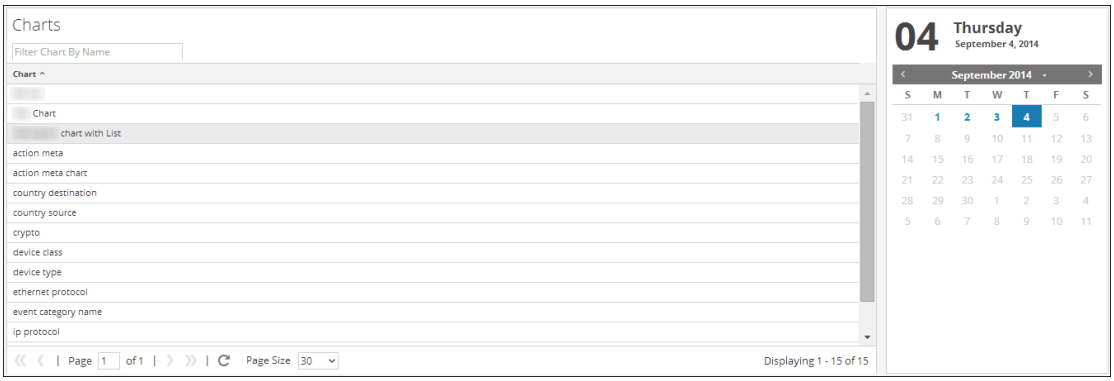
Ver la lista de todos los gráficos

En este tema se proporcionan instrucciones para ver la lista de todos los gráficos.

Procedimiento

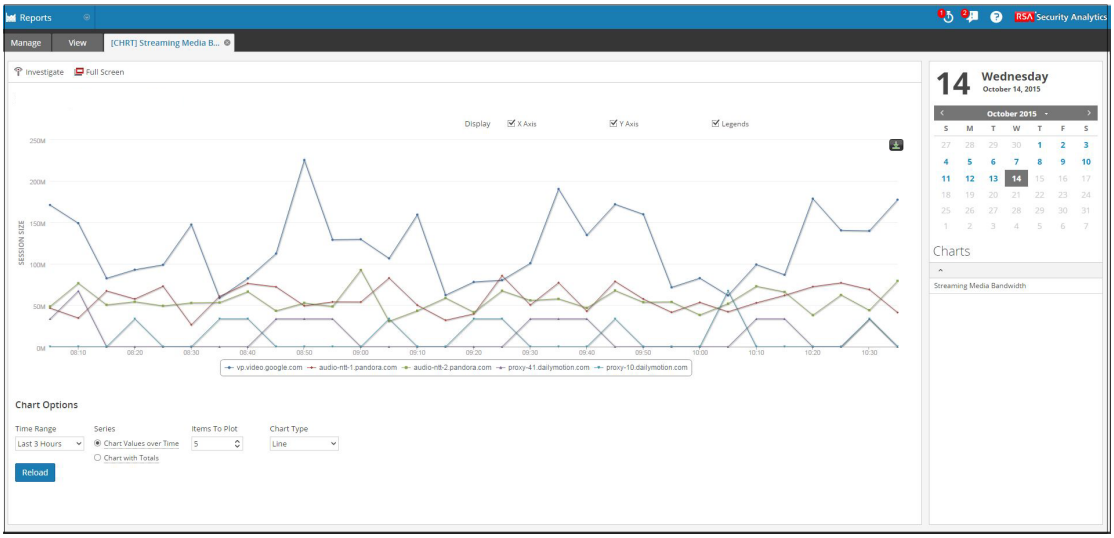
Realice los siguientes pasos para ver la lista de todos los gráficos:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Gráficos**.
   Se muestra la vista Gráfico.
3. En la barra de herramientas **Gráfico**, haga clic en **Ver todos los gráficos**.
   Todos los gráficos ejecutados para la fecha seleccionada se muestran en una nueva pestaña.



Nota:
* Si no se muestra ninguna lista, seleccione una fecha del calendario para ver una lista de gráficos.
*Si desea ver un gráfico específico, ingrese el nombre del gráfico en los criterios de búsqueda.

4. Haga clic en el nombre del gráfico para ver sus detalles para esa fecha.



Ver un gráfico

En este tema se proporcionan instrucciones para ver un gráfico.

Requisitos previos

Asegúrese de haber comprendido los componentes del panel Ver un gráfico. Para obtener más información, consulte Panel Ver un gráfico.

Procedimiento

Realice los siguientes pasos para ver un gráfico:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Gráficos**.
   Se muestra la vista Gráfico.
3. En el panel **Lista de gráficos**, realice una de las siguientes acciones:

   - Seleccione un gráfico y haga clic en  > **Ver**.
   - Seleccione un gráfico y haga clic en **Ver** en la columna Ver gráfico.
     Se muestra la pestaña de la vista Ver gráfico.

4. En **Opciones de gráficos**, realice lo siguiente:

   a. Seleccione el rango de tiempo.

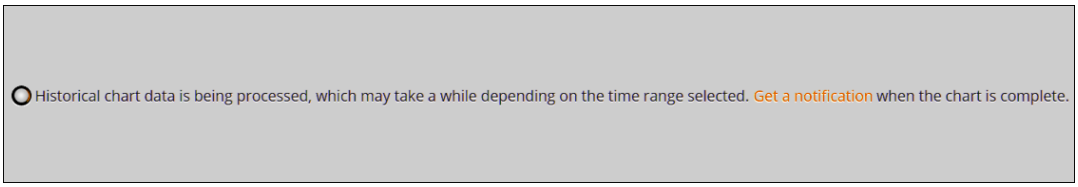
Nota: Cuando selecciona la opción Rango de tiempo, puede seleccionar un rango de tiempo predefinido, por ejemplo, última hora, últimas 3 horas y así sucesivamente, o puede personalizar la selección, para lo cual debe elegir Últimos n días o Personalizado. Si selecciona la opción Últimos n días, puede ver los datos históricos para un máximo de 15 días. Mientras que, si selecciona la opción Personalizado, puede seleccionar una fecha de inicio y una fecha de finalización para ver los datos del rango de fechas seleccionado.

   b. Seleccione la serie: Valores del gráfico en el tiempo o Gráfico con totales.
      Cuando selecciona Valores del gráfico en el tiempo, el gráfico muestra el cambio en los valores durante el tiempo seleccionado. Cuando selecciona Gráfico con totales, el gráfico muestra un total para cada valor agregado durante el tiempo seleccionado.

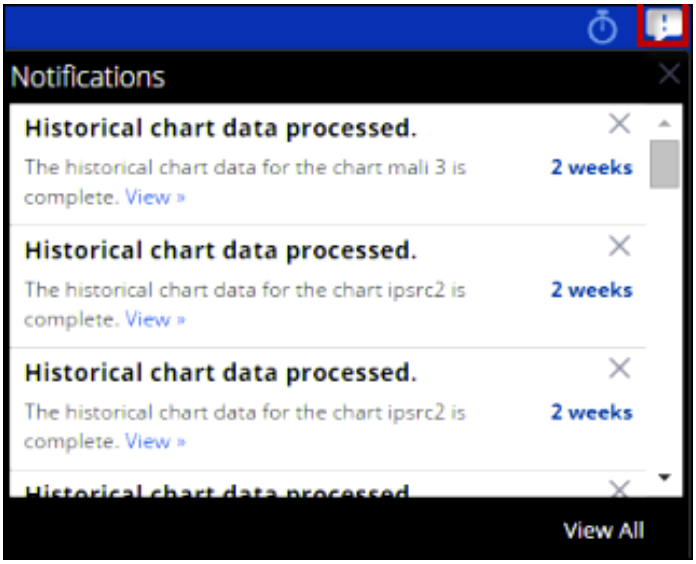
   c. Seleccione los elementos para trazar.
      La cantidad de eventos que desea ver en el gráfico.

   d. En la lista desplegable Tipo de gráfico, seleccione el tipo de gráfico.

   e. Haga clic en **Volver a cargar** para volver a cargar el gráfico seleccionado.
      Si existe una demora en la recuperación de los datos históricos para el rango de tiempo seleccionado, aparece un mensaje.



Después de que se genera el gráfico, se muestra una notificación en la bandeja de notificaciones disponible en la barra de herramientas de Security Analytics. Para obtener más información sobre la barra de herramientas de Security Analytics, consulte el tema Ventana del navegador en la *Guía de introducción de Security Analytics*.



Administrar el acceso para un gráfico o un grupo de gráficos

En esta guía se describe la función Alerta del módulo Reporting. El módulo Alertas se usa para definir y ver alertas.

En esta sección se describen los permisos de acceso que tiene el usuario según la función del usuario para administrar un gráfico y un grupo de gráficos. El módulo Reporting proporciona un control de acceso en el nivel de gráfico y de grupo de gráficos. El usuario que tiene el conjunto correcto de permisos puede ejecutar las tareas en el módulo Reporting. El administrador administra el control de acceso desde la pestaña **Administration > Seguridad > Funciones**.

Cuando el administrador crea usuarios y funciones de usuario, debe asegurarse de que las funciones creadas para tareas específicas tengan acceso a todos los permisos más altos en la jerarquía de funciones.

Los gráficos y los grupos de gráficos se pueden vincular a un conjunto específico de funciones de usuario de modo que, cuando un usuario inicie sesión en Security Analytics, se puedan ver los gráficos con derechos de acceso para la función de usuario específica. Los usuarios que pertenecen a una función de usuario con el permiso de acceso “Lectura y escritura” pueden definir gráficos. Además, el acceso se puede restringir de modo que solo accedan a los gráficos quienes tengan el acceso de “Solo lectura”.

Nota: debe tener permiso de “Solo lectura” en un grupo para ver los gráficos dentro de ese grupo.

En el nivel del gráfico, puede establecer los siguientes permisos de acceso para las funciones de usuario en Security Analytics:

- Lectura y escritura
- Solo lectura
- Sin acceso

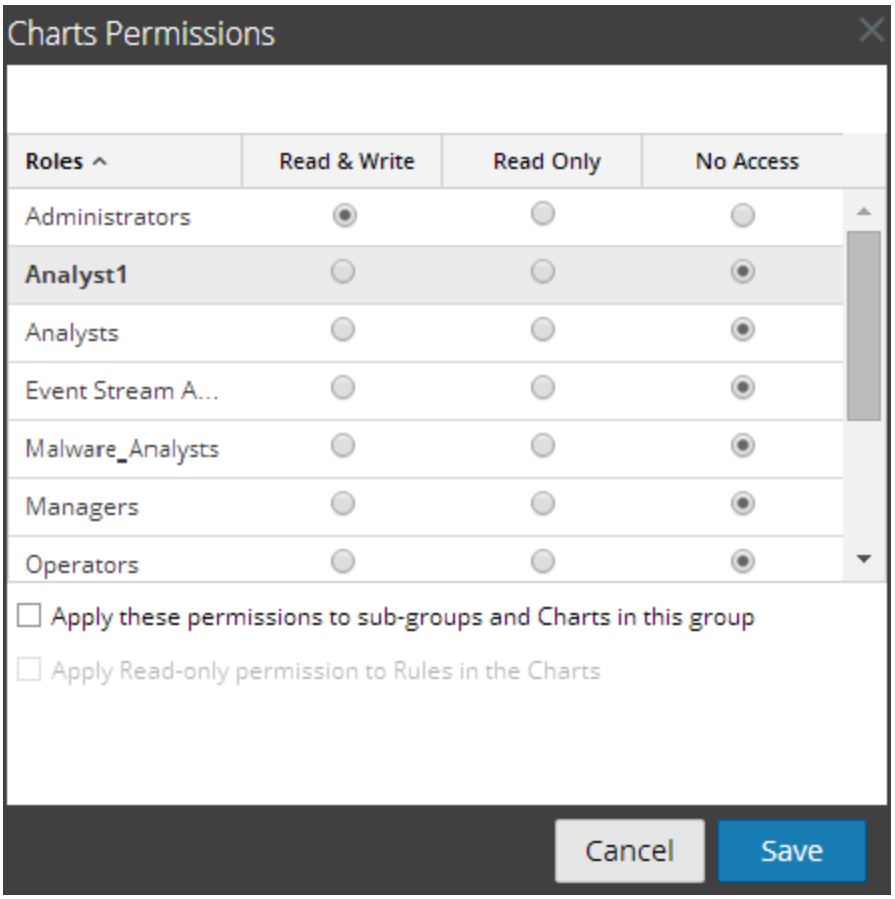
Suponga que desea que los **analistas de seguridad** tengan acceso a todos los gráficos de un grupo de gráficos. Para esto, puede configurar el permiso **"Lectura y escritura"** en el nivel del grupo de gráficos. Y si no desea que la función **Operador** tenga acceso a un conjunto específico de gráficos en un grupo de gráficos, puede configurar el permiso "**Sin acceso**" en el nivel del grupo de gráficos.

El permiso se configura solo para el grupo de gráficos, pero no para los gráficos, las reglas ni los subgrupos del grupo de gráficos.

Control de acceso para un grupo de gráficos

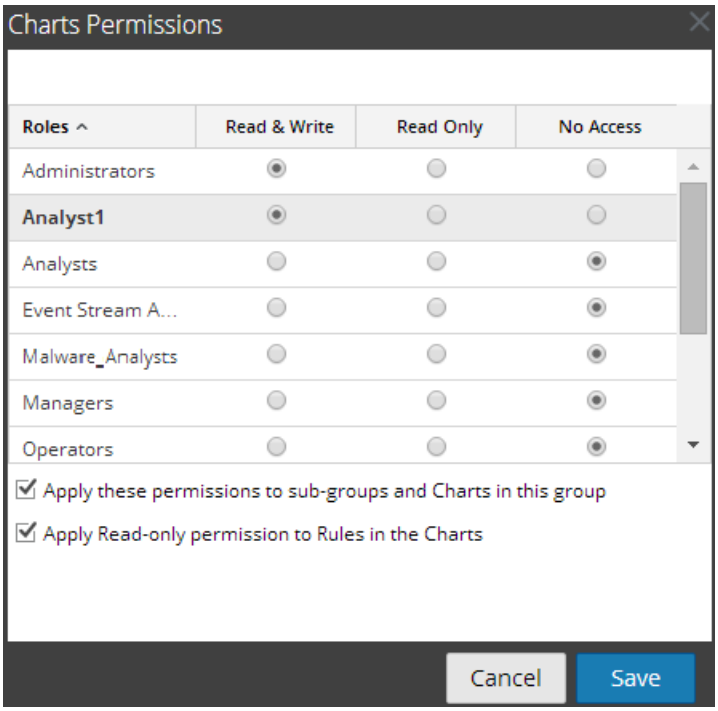
Cuando desea cambiar los permisos del grupo de gráficos, debe seleccionar un grupo de gráficos y configurar sus permisos de acceso en el panel Permisos de gráficos.

Antes de aplicar permisos del grupo de gráficos, el conjunto de permisos predeterminado para todas las funciones de usuario es el permiso "Sin acceso" y las casillas de verificación están deseleccionadas.



Si desea cambiar el permiso de acceso para una función de usuario específica, debe configurarlo en el nivel del grupo de gráficos, como se muestra en la figura. Suponga que desea que los **administradores** tengan acceso a todos los gráficos de un grupo de gráficos. Para esto, puede configurar el permiso "**Lectura y escritura**" en el panel Permisos de grupo de gráficos.

También puede aplicar permisos a los subgrupos y a los gráficos del grupo, así como permisos de solo lectura a reglas en los gráficos si selecciona las casillas de verificación apropiadas.



Los tres escenarios se explican de forma resumida:

- Escenario 1: Permisos aplicados a grupo de gráficos/subgrupo/gráfico según la función de usuario.
- Escenario 2: Permisos aplicados a subgrupo y gráfico del grupo.
- Escenario 3: Permiso de solo lectura aplicado a reglas en el gráfico.

	Función (Analista)	Permisos aplicados a grupo de gráficos/subgrupo/gráfico según la función de usuario	Permisos aplicados a subgrupo y gráficos del grupo	Permiso (de solo lectura) aplicado a reglas en el gráfico
Grupo	Lectura y escritura	**Lectura y escritura**	**Lectura y escritura**	Lectura y escritura
Subgrupo	Lectura	**Lectura**	**Lectura y escritura: heredados**	Lectura y escritura

Gráfico	Lectura	**Lectura**	**Lectura y escritura: heredados**	Lectura y escritura
Reglas	Lectura	**Lectura**	Lectura	**Lectura**

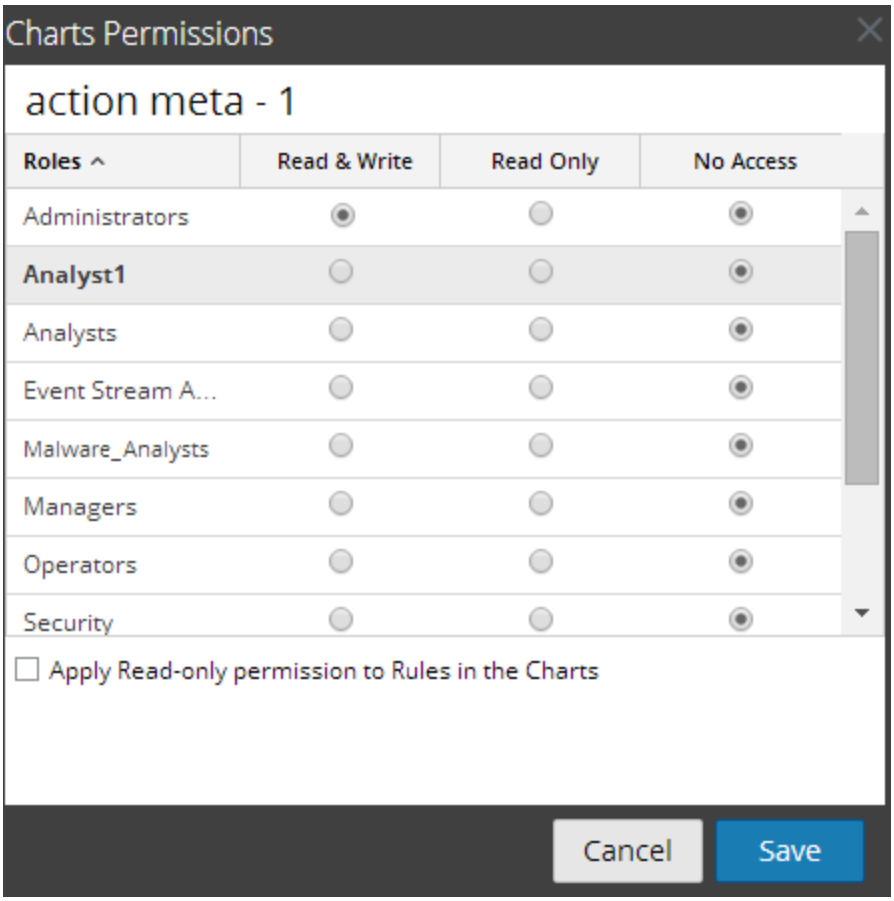
Al grupo de gráficos se asigna la función de un **analista de seguridad** y los permisos se configuran en **Lectura y escritura** en el grupo de gráficos.

En el escenario 1, cada uno de los niveles tendrá un permiso configurado de acuerdo con la función del usuario. En el escenario 2, el subgrupo y los gráficos del grupo heredarán el permiso en el nivel del grupo de gráficos. En el escenario 3 se configura el permiso de lectura para las reglas, salvo que el permiso configurado para las reglas no puede ser mayor que los permisos configurados para el grupo de gráficos.

Control de acceso para un gráfico

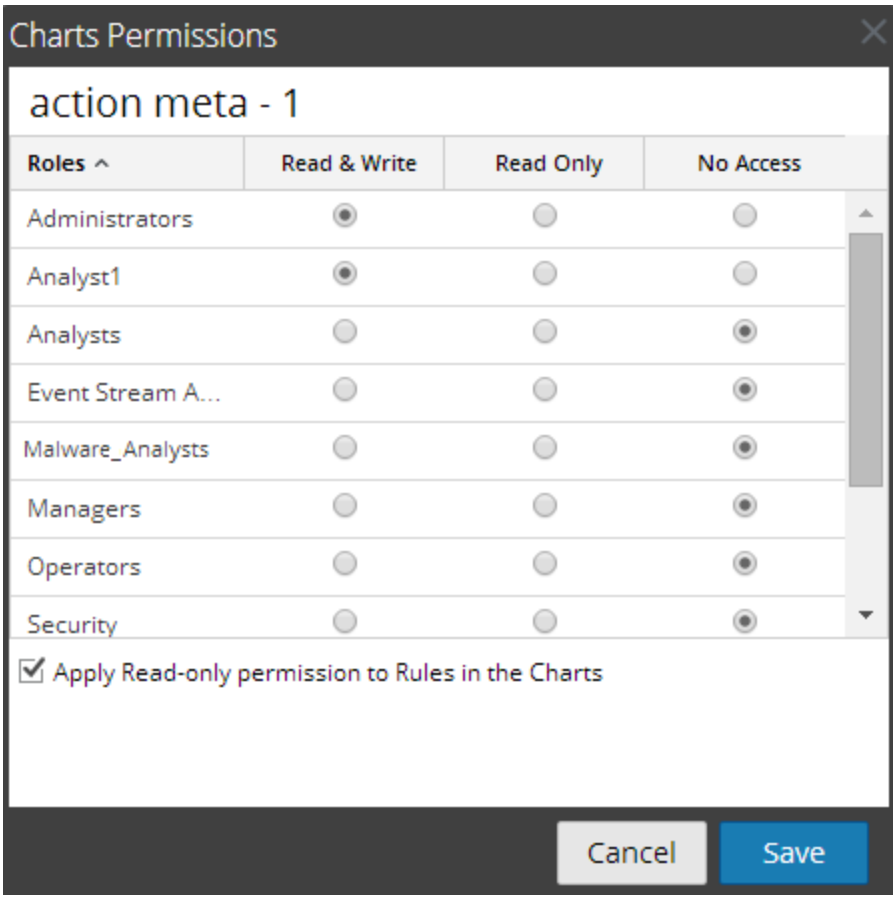
Cuando desea cambiar los permisos de los gráficos, debe seleccionar un gráfico y configurar sus permisos de acceso en el panel Permisos de gráficos.

Antes de aplicar permisos de gráficos, el conjunto de permisos predeterminado para todas las funciones de usuario es el permiso “Sin acceso” y la casilla de verificación está deseleccionada.



Si desea cambiar el permiso de acceso para una función de usuario específica, debe configurarlo en el nivel de gráfico, como se muestra en la figura. Suponga que desea que los **administradores** tengan acceso a un gráfico específico. Para esto, puede configurar el permiso "**Lectura y escritura**" en el panel Permisos de gráficos.

Además, puede aplicar permisos de solo lectura a las reglas de los gráficos si selecciona la casilla de verificación.



Los dos escenarios se explican de forma resumida:

- Escenario 1: Permisos aplicados a grupo de gráficos/subgrupo/gráfico/reglas según la función de usuario.
- Escenario 2: Permiso de solo lectura aplicado a reglas en el gráfico.

	Función (Analista)	Permisos aplicados a grupo de gráficos/subgrupo/gráfico/reglas según la función de usuario	Permiso (de solo lectura) aplicado a reglas en el gráfico
Grupo	Lectura y escritura	**Lectura y escritura**	Lectura y escritura
Subgrupo	Lectura	**Lectura**	Lectura y escritura

Gráfico	Lectura	**Lectura**	Lectura y escritura
Reglas	Lectura	**Lectura**	**Lectura**

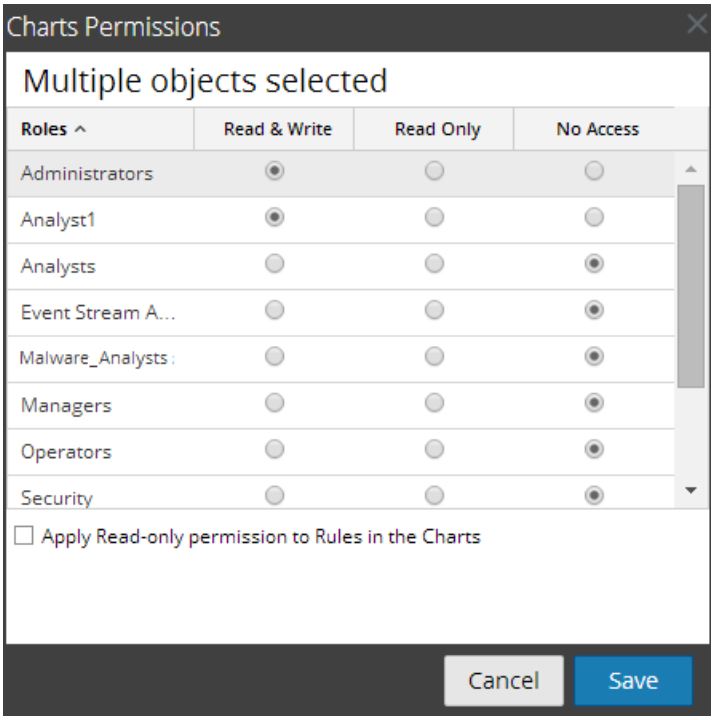
Al gráfico se asignará la función de un **analista de seguridad** y los permisos se configuran en **Lectura y escritura** para los gráficos.

En el escenario 1, cada uno de los niveles tiene un permiso configurado según la función del usuario. En el escenario 2 se configura el permiso de lectura para las reglas, salvo que el permiso para las reglas no puede ser mayor que el permiso para los gráficos.

Nota: Si el permiso para las reglas es mayor que el permiso para el gráfico, el permiso no se aplica. Por ejemplo, si configura los permisos para el grupo de informes como **Sin acceso** y especifica la opción *Aplicar permisos de solo lectura a las reglas de los informes*, el permiso de solo lectura no se configura para las reglas.

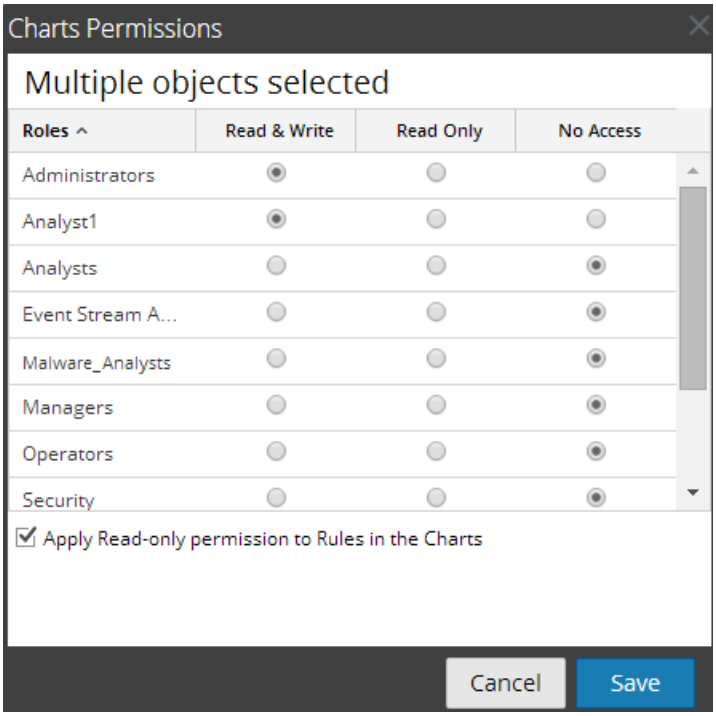
Control de acceso para un gráfico cuando se seleccionan múltiples gráficos

Cuando desea cambiar los permisos de varios gráficos, debe seleccionarlos y configurar sus permisos de acceso en el panel Permisos de gráficos. El permiso de acceso que elige se aplica a todos los gráficos seleccionados.



Control de acceso para un gráfico cuando se seleccionan múltiples gráficos con varias reglas

Cuando desea cambiar los permisos y están seleccionados múltiples gráficos con varias reglas, debe seleccionar la casilla de verificación del panel Permisos de gráficos.



El permiso de acceso de solo lectura se aplica a todas las reglas de los gráficos seleccionados, siempre que el permiso de las reglas sea menor que el permiso de los gráficos.

Nota: si un usuario (distinto del superusuario) crea un gráfico, el superusuario no puede acceder a él.

Lista tabular

En la siguiente tabla se indican las diversas columnas del panel Permisos de gráficos.

Columna	Descripción
Funciones	La función del usuario que inició sesión en la interfaz del usuario de Security Analytics.
Lectura y escritura	El usuario puede acceder, ver, editar, importar, exportar y eliminar el gráfico en la página Gráficos. El usuario también puede cambiar el permiso en el gráfico.

Columna	Descripción
Solo lectura	El usuario solo puede acceder al gráfico y verlo en la vista Gráficos.
Sin acceso	El usuario no puede acceder a un gráfico ni verlo cuando tiene configurado este permiso.
Aplicar estos permisos a subgrupos y gráficos en este grupo	Seleccione la casilla de verificación para aplicar los permisos seleccionados al grupo de gráficos, subgrupos en el grupo y gráficos en el grupo. **Nota:** Esta casilla de verificación solo se completa cuando se establece permisos de acceso para un grupo de gráficos.
Aplicar permisos de solo lectura a las reglas de los gráficos	Seleccione la casilla de verificación para aplicar permisos a las reglas de los gráficos de forma automática.

Temas

- Establecer el control de acceso para un gráfico
- Establecer el control de acceso para un grupo de gráficos

Establecer el control de acceso para un gráfico

En este tema se proporcionan instrucciones para establecer un control de acceso a un gráfico.

Requisitos previos

Asegúrese de:

- Haber comprendido los permisos de acceso que tendrá el usuario según la función de usuario. Para obtener más información, consulte Administrar el acceso para un gráfico o un grupo de

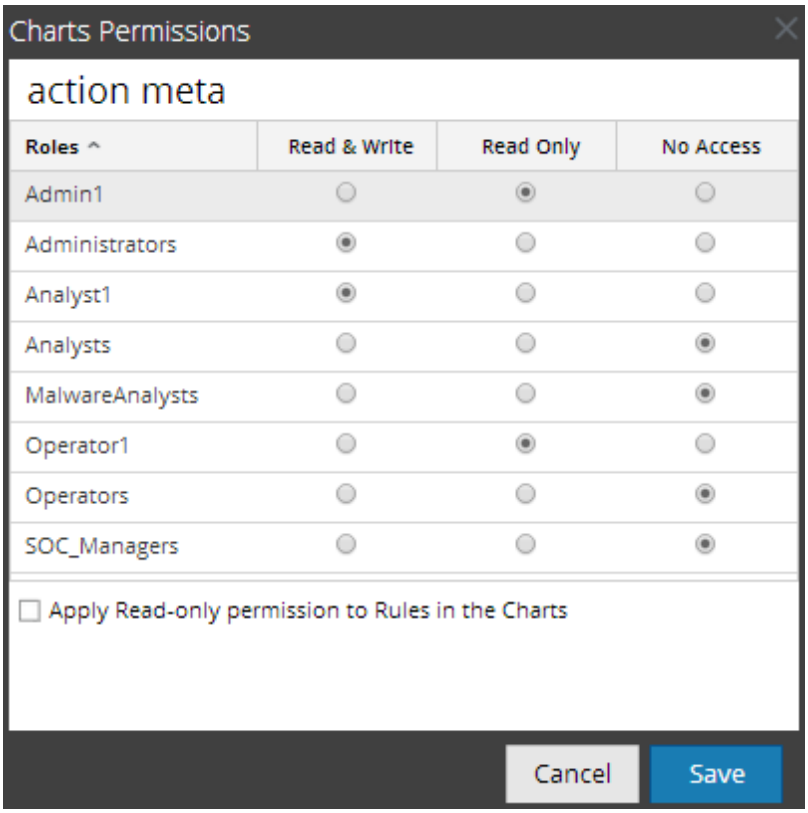
gráficos.

- Tener un permiso de acceso de “Lectura y escritura” mínimo para establecer los permisos de acceso de un gráfico.

Procedimiento

Realice los siguientes pasos para establecer permisos de acceso para un gráfico:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Gráficos**.
   Se muestra la vista Gráfico.
3. En el panel **Lista de gráficos**, seleccione un gráfico.
4. Haga clic en > **Permisos**.
   Aparece el cuadro de diálogo Permisos de gráficos.



5. Según la función de usuario, seleccione los botones que correspondan.
6. (Opcional) Seleccione la casilla de verificación si desea brindar permiso de acceso de lectura a reglas dependientes.

Nota: cuando se selecciona la casilla de verificación, a todas las reglas dependientes con permiso Sin acceso se les otorga permiso de acceso de LECTURA.

6. Haga clic en **Guardar**.
   Se muestra un mensaje de confirmación que indica que el permiso se estableció correctamente para el gráfico seleccionado.

Establecer el control de acceso para un grupo de gráficos

En este tema se proporcionan instrucciones para establecer permisos para un grupo de gráficos.

Requisitos previos

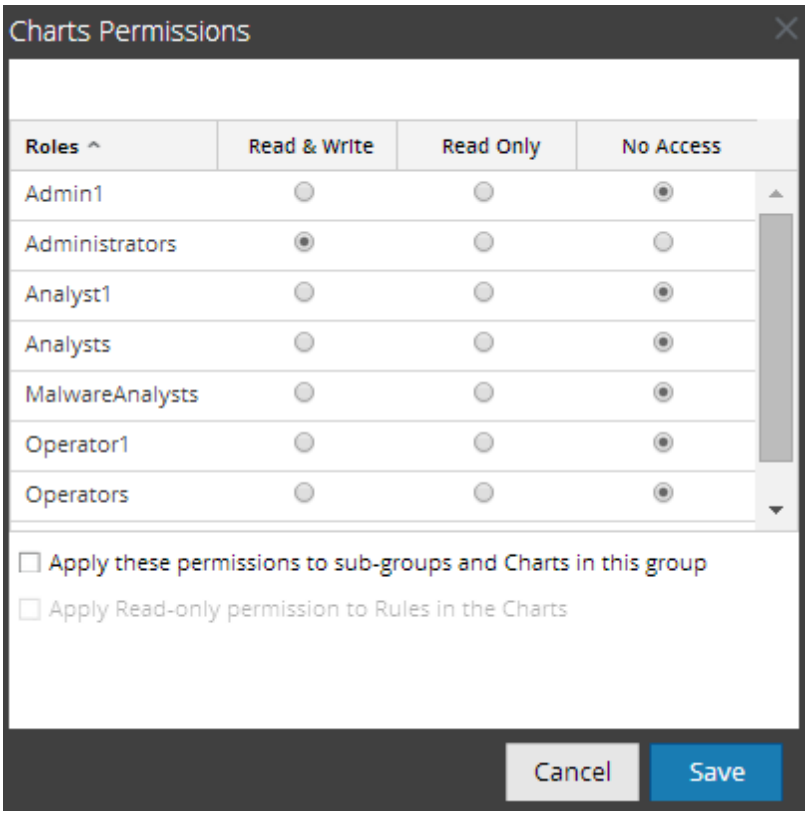
Asegúrese de:

- Haber comprendido los permisos de acceso que tendrá el usuario según la función de usuario. Para obtener más información, consulte Administrar el acceso para un gráfico o un grupo de gráficos.
- Tener un permiso de acceso de “Lectura y escritura” mínimo para establecer permisos de acceso para un grupo de gráficos.

Procedimiento

Realice los siguientes pasos para establecer permisos de acceso para un grupo de gráficos:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Gráficos**.
   Se muestra la vista Gráfico.
3. En el panel **Grupos de gráficos**, seleccione un grupo de gráficos.
4. Haga clic en  > **Permisos**.
   Aparece el cuadro de diálogo Permisos de gráficos.



5. Según la función de usuario, seleccione los botones que correspondan.
6. (Opcional) Seleccione la casilla de verificación apropiada para aplicar estos permisos a subgrupos y gráficos en el grupo.
7. (Opcional) Seleccione la casilla de verificación apropiada para otorgar permiso de acceso de lectura a reglas dependientes.

Nota: cuando se selecciona la casilla de verificación, a todas las reglas dependientes con permiso Sin acceso se les otorga permiso de acceso de LECTURA.

7. Haga clic en **Guardar**.
   Se muestra un mensaje de confirmación que indica “El permiso se estableció correctamente para el grupo de gráficos seleccionado”.

Probar un gráfico

En este tema se proporcionan instrucciones para probar un gráfico basado en el rango de tiempo y el tipo de gráfico seleccionado.

Requisitos previos

Asegúrese de haber comprendido los componentes de la vista **Probar un gráfico**. Para obtener más información, consulte Vista Probar un gráfico.

Procedimiento

Realice los siguientes pasos para probar un gráfico:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Gráficos**.
   Se muestra la vista Gráfico.
3. Realice una de las siguientes acciones

   - En la barra de herramientas **Gráfico**, haga clic en  .
   - En el panel **Gráfico**, haga doble clic en un gráfico o seleccione un gráfico y haga clic en  .
   - En el panel **Lista de gráficos**, haga clic en  > **Editar**.
     Se muestra la pestaña de la vista Crear gráfico.
4. Haga clic en **Probar gráfico** para ver el gráfico.
   Se muestra la pestaña de la vista Ver gráfico.
5. Seleccione los rangos de fechas **Desde** y **Hasta**.
6. Seleccione la **serie**, ya sea Serie temporal o Resumen.
7. En la lista desplegable **Tipo de gráfico**, seleccione el tipo de gráfico.
8. Haga clic en **Ejecutar prueba** para ejecutar la prueba.
   Se muestran los datos de gráfico (si los hay) para el rango de tiempo.

Investigar un gráfico

En este tema se proporcionan instrucciones para investigar un gráfico. Puede investigar un gráfico navegando directamente al módulo Investigation desde el gráfico. Puede usar la función Investigar un gráfico para investigar un evento en un punto de tiempo específico o en todo el rango de tiempo para el cual se generó el gráfico.

La vista Ver gráfico cuenta con un calendario para seleccionar la fecha para la cual se desea recuperar la lista de los gráficos ejecutados. Según la fecha seleccionada en el calendario, se completa una lista de los gráficos ejecutados en la fecha seleccionada. Puede hacer doble clic en el nombre del gráfico para ver sus detalles.

Mediante las opciones de gráfico, puede cambiar el intervalo de tiempo o el formato del gráfico, como Área escalonada, Línea, Barra, etc., para otro rango de fechas.

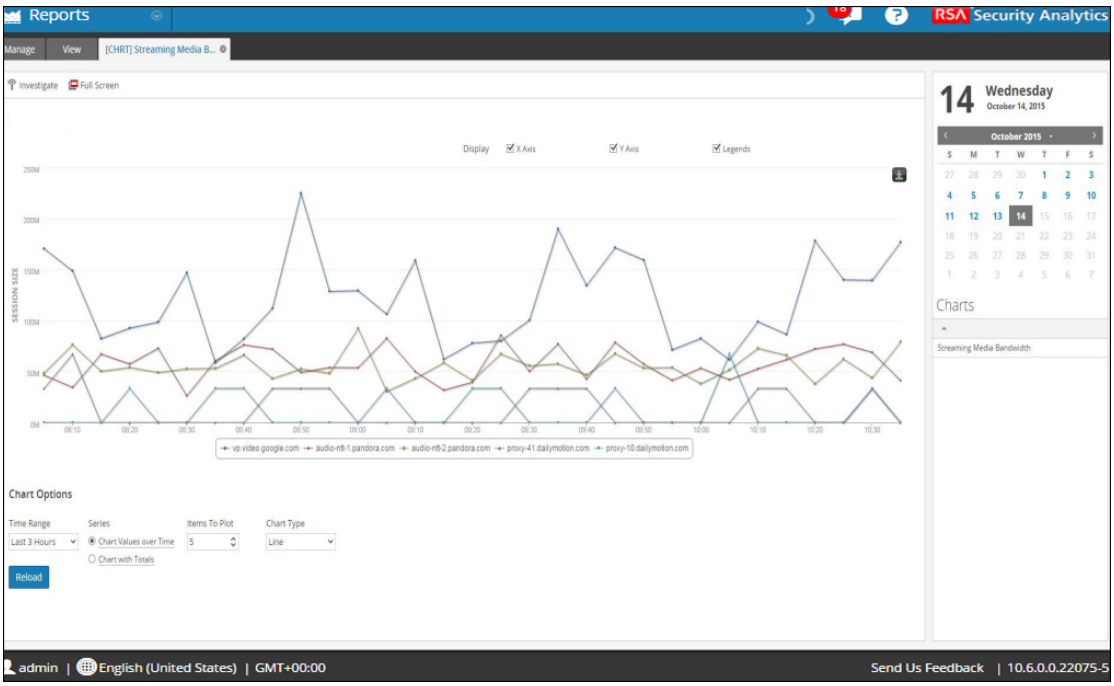
Requisitos previos

Asegúrese de tener actualmente un origen de datos activo.

Procedimiento

Realice los siguientes pasos para investigar un gráfico:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Gráficos**.
   Se muestra la vista Gráfico.
3. En la barra de herramientas **Gráfico**, haga clic en **Ver todos los gráficos**.
   Todos los gráficos ejecutados para la fecha seleccionada en el panel **Opciones de gráficos** se muestran en una nueva pestaña.
4. Haga clic en el nombre del gráfico para ver sus detalles.



5. Realice una de las siguientes acciones
   - Haga clic en un punto de datos del gráfico para investigar ese punto de datos.
   - En la barra de herramientas, haga clic en **Investigar** para investigar el rango de tiempo completo.

Trabajar con alertas en el módulo Reporting

El módulo Alertas se usa para definir y ver alertas.

Temas

- Descripción general de una alerta
- Definir alertas
- Definir plantillas de alertas
- Administrar el acceso para una alerta
- Configurar Security Analytics para que genere una alerta
- Investigar una alerta
- Configurar el motor de creación de informes para enviar mensajes de Sylog mediante TCP/TLS para las alertas

Descripción general de una alerta

En este tema se proporciona una descripción breve de una alerta. Una alerta es una regla que puede programar para que se ejecute de manera continua y registre sus conclusiones en distintas salidas de alerta, incluidos el módulo **Reporting > Administrar > Alertas**, registro, SMTP, SNMP y Syslog. Puede utilizar cualquier regla que exista en Security Analytics y crear una alerta a partir de ella si esa regla tiene una cláusula Where única. Después de crear una alerta, puede agregarla a la línea de espera de alertas. Después de agregaruna alerta a la línea de espera, se ejecuta a cada minuto (de manera predeterminada).

Propiedad	Descripción	Ejemplo
Nombre **Nota:** En el campo **Nombre**, el ícono para expandir el tamaño de la columna no se muestra al final del campo de la columna. Debe mover el mouse un poco hacia la izquierda para ver el ícono que permite ampliar la columna.	Se usa para identificar la alerta. Si hace clic en el nombre de una alerta, se muestra la regla en la cual se basa esta alerta en el panel Definir reglas.	Alerta1

Propiedad	Descripción	Ejemplo
Descripción	Se usa para describir la alerta.	Mensajes de plantilla

Una alerta se compone de lo siguiente:

Nota: En la interfaz del usuario de Reporting, dondequiera que se muestre la fecha y hora o un valor ingresado para este campo, siempre están de acuerdo con el perfil de zona horaria que seleccionó el usuario. De forma predeterminada, Reporting Engine muestra todos los valores repetidos para una clave de metadatos. Si no desea que los valores de metadatos se repitan en la salida de la alerta, habilite la opción "removeRepeatedMetaValue", para lo cual debe navegar a **Configuración** > **Configuración de alerta** disponible para Reporting Engine en la vista **Configuración de servicios** > **Explorar**. Por ejemplo, en una sesión de HTTP, el valor correspondiente a la acción se muestra como `get, get, put, put, post, get`. Cuando esta opción está habilitada, el valor se muestra como `get, put, post`.

Definir alertas

Este tema es un conjunto de tareas para configurar alertas. Puede definir, eliminar, editar, importar y exportar alertas en Security Analytics. Cada tema describe los procedimientos pertinentes.

Temas

- Agregar una alerta
- Eliminar una alerta
- Desactivar una alerta
- Editar una alerta
- Activar una alerta
- Exportar una alerta
- Importar una alerta
- Actualizar una lista de alertas

Agregar una alerta

En este tema se proporcionan instrucciones para agregar una alerta.

Requisitos previos

Asegúrese de:

- Tener reglas definidas con cláusulas where únicas antes de agregar una alerta.
- Tener Decoders conectados al Concentrator agregado a Reporting Engine para el origen de datos seleccionado, antes de agregar una regla de alerta.
- Haber comprendido los componentes de la vista Crear/modificar alerta. Para obtener más información, consulte Vista Crear o modificar alerta.

Procedimiento

Realice los siguientes pasos para agregar una alerta:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Alertas**.
   Se muestra la vista Alerta.
3. En la barra de herramientas **Alerta**, haga clic en +.
   Aparece la pestaña Crear/modificar alerta.

Nota: Si desea agregar una clave de metadatos en la regla, especifique lo mismo en el formato: ${meta.metakey}. Por ejemplo, ${meta.ip.dst}.

4. Haga clic en **Activar** para activar la alerta.
5. En el campo **Base de la regla**, realice lo siguiente:
   a. Haga clic en **Navegar**.
      Se muestra el cuadro de diálogo Consultar base de la regla.
   b. Navegue al árbol Regla y seleccione una regla.

c. Haga clic en **Aceptar**.

El nombre de la regla se muestra en el campo Base de la regla.

6. Seleccione un origen de datos en la lista desplegable **Orígenes de datos**.

Nota: Si el origen de datos no se muestra, asegúrese de tener permisos de **lectura** configurados para el origen de datos. Esto se aplica a los orígenes de datos NWDB y Warehouse. Para obtener más información, consulte el tema Configurar permisos de orígenes de datos en la *Guía de configuración de hosts y servicios*.

7. Seleccione la casilla de verificación **Migrar a decodificadores** para que Reporting Engine envíe la regla al Decoder.
8. (Opcional) Ingrese una descripción de alerta en el campo **Descripción**.
9. Seleccione el nivel de gravedad en la lista desplegable **Gravedad**.
10. En el campo **Notificación**, realice lo siguiente:
    a. Seleccione la notificación adecuada.

    Se muestra la pestaña de notificación seleccionada en el cuadro de diálogo Crear/modificar alerta.

    b. (Opcional) Deseleccione la notificación para desactivar la pestaña de notificación.
    c. Defina la acción en una de las pestañas **Notificación**:
        i. En la pestaña **Registro**, realice lo siguiente:
            a. En la lista desplegable **Ejecutar**, seleccione la frecuencia para registrar una alerta.
            b. Ingrese el mensaje REGISTRO. Puede crear el mensaje desde cero o puede seleccionar una plantilla en el campo **Plantilla de cuerpo** y modificarla aquí.
            c. (Opcional) Si se definieron plantillas, seleccione una para el mensaje de REGISTRO, la cual puede utilizar tal como está o modificar.
        ii. En la pestaña **SMTP**, realice lo siguiente:
            a. En la lista desplegable **Ejecutar**, seleccione un valor para identificar la cantidad de veces que desea enviar un mensaje de correo electrónico para la alerta.
            b. Ingrese una única dirección de correo electrónico o una lista de direcciones de correo electrónico separadas por comas a las cuales desea enviar esta alerta.
            c. Ingrese el asunto del mensaje de correo electrónico.

d. Ingrese el cuerpo del mensaje. Puede crear el mensaje desde cero o puede seleccionar una plantilla en el campo **Plantilla de cuerpo** y modificar la plantilla aquí.

e. (Opcional) Si se definieron plantillas, seleccione una para el mensaje de SMTP, la cual puede utilizar tal como está o modificar.

iii. En la pestaña **SNMP**, realice lo siguiente:

a. En la lista desplegable **Ejecutar**, seleccione un valor para identificar la cantidad de veces que desea enviar un mensaje de SNMP para la alerta.

b. Ingrese el mensaje de SNMP. Puede crear el mensaje desde cero o puede seleccionar una plantilla en el campo **Plantilla de cuerpo** y modificarla aquí.

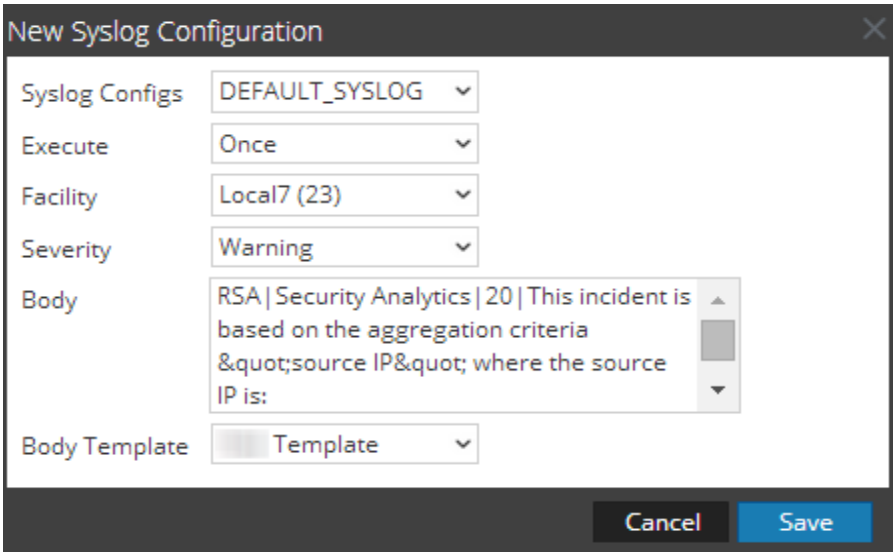
c. (Opcional) Si se definieron plantillas, seleccione una para el mensaje de SNMP, la cual puede utilizar tal como está o modificar.

iv. En el campo de la pestaña **Syslog**, realice lo siguiente:

Nota: Puede configurar varios servidores de Syslog en el panel Configuración de syslog. Para obtener más información, consulte el tema Acciones de salida de Reporting Engine de la *Guía de configuración de hosts y servicios*.

a. Haga clic en +.

Aparece el cuadro de diálogo Nueva configuración de syslog.



b. En la lista desplegable **Configuraciones de syslog**, seleccione un valor para la configuración de syslog.

c. En la lista desplegable **Ejecutar**, seleccione un valor para identificar la cantidad de veces que desea enviar un mensaje de Syslog para la alerta.

d. Seleccione la herramienta en la lista desplegable **Herramienta**.

e. Seleccione el nivel de gravedad en la lista desplegable **Gravedad**.

f. Ingrese el mensaje de Syslog. Puede crear el mensaje desde cero o puede seleccionar una plantilla en el campo **Plantilla de cuerpo** y modificarla aquí.

g. (Opcional) Si se definieron plantillas, seleccione una para el mensaje de syslog, la cual puede utilizar tal como está o modificar.

h. Haga clic en **Guardar**.
La configuración de Syslog se agrega a la alerta.

11. Haga clic en **Crear**.
Security Analytics crea la alerta con un mensaje de configuración que indica que la alerta se guardó correctamente. Security Analytics activa la alerta ye ejecuta las acciones de salida a cada minuto.

Eliminar una alerta

En este tema se proporcionan instrucciones para eliminar una alerta.

Requisitos previos

Asegúrese de haber comprendido los componentes de la vista Alerta. Para obtener más información, consulte Vista Alerta.

Procedimiento

Realice los siguientes pasos para eliminar una alerta:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
Se muestra la pestaña Administrar.
2. Haga clic en **Alertas**.
Se muestra la vista Alerta.
3. En el panel **Lista de alertas**, seleccione la alerta y haga clic en −.
Un cuadro de diálogo de advertencia solicita confirmación de que desea quitar las alertas seleccionadas.
4. Haga clic en **Sí** para eliminar la alerta.
Se muestra un mensaje que confirma la correcta eliminación de la alerta y la alerta seleccionada se elimina del panel Lista de alertas.

Desactivar una alerta

En este tema se proporcionan instrucciones sobre cómo desactivar las alertas seleccionadas y eliminar las alertas del Decoder y Log Decoder.

Requisitos previos

Asegúrese de haber comprendido los componentes de la vista Alerta. Para obtener más información, consulte Vista Alerta.

Procedimiento

Realice los siguientes pasos para inhabilitar una alerta:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.

   Se muestra la pestaña Administrar.

2. Haga clic en **Alertas**.

   Se muestra la vista Alerta.

3. En el panel **Lista de alertas**, seleccione la alerta que muestra en la columna **Activado**.

4. Haga clic en .

   Un mensaje de confirmación indica que el estado de la alerta cambió correctamente.

Editar una alerta

En este tema se proporcionan instrucciones para editar una alerta.

Requisitos previos

Asegúrese de:

- Haber comprendido los componentes de la vista Alerta. Para obtener más información, consulte Vista Alerta.
- Haber comprendido los componentes de la vista Crear o modificar alerta. Para obtener más información, consulte Vista Crear o modificar alerta.

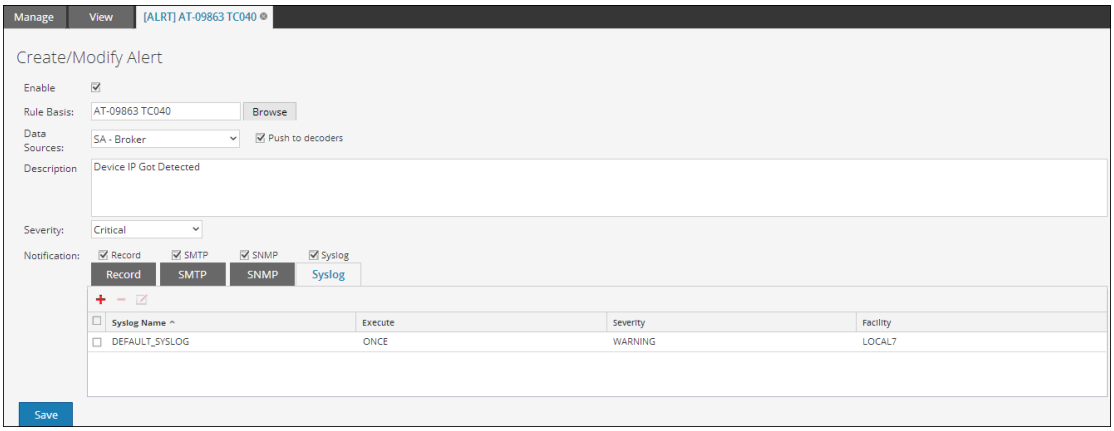
Procedimiento

Realice los siguientes pasos para editar una alerta:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Alertas**.
   Se muestra la vista Alerta.

3. En el panel **Lista de alertas**, seleccione una alerta y haga clic en .

   Aparece la pestaña Crear/modificar alerta.



4. En el campo **Base de la regla**, navegue por el árbol de reglas y seleccione otra regla.

   El nombre de la regla se muestra en el campo Base de la regla.

5. (Opcional) Seleccione un origen de datos de la lista desplegable **Orígenes de datos**.

   Nota: si el origen de datos no se muestra, asegúrese de tener permisos de **lectura** configurados para el origen de datos. Esto se aplica a los orígenes de datos NWDB y Warehouse. Para obtener más información, consulte el tema Configurar permisos de orígenes de datos en la *Guía de configuración de hosts y servicios*.

6. (Opcional) Modifique la descripción de la alerta en el campo **Descripción**.
7. Modifique las pestañas de **Notificación** adecuadas: **REGISTRO**, **SMTP**, **SNMP** y **Syslog**.
8. Haga clic en **Crear**.

   Se muestra un mensaje de confirmación que indica que la alerta se editó correctamente.

Activar una alerta

En este tema se proporcionan instrucciones sobre cómo activar una alerta para ejecutar y enviar acciones de salida a cada minuto cuando se cumplen las condiciones de la alerta.

Requisitos previos

Asegúrese de:

- Haber comprendido los componentes de la vista Alerta. Para obtener más información, consulte Vista Alerta.

- Haber comprendido los componentes de la vista Crear o modificar alerta. Para obtener más información, consulte Cuadro de diálogo Crear/modificar plantilla.

Procedimiento

Realice los siguientes pasos para habilitar una alerta:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Alertas**.
   Se muestra la vista Alerta.
3. En el panel **Lista de alertas**, seleccione la alerta que muestra ○ en la columna **Activado**.
4. Haga clic en ●.
   Un mensaje de confirmación indica que el cambio en el estado de las alertas se realizó correctamente.

Exportar una alerta

En este tema se proporcionan instrucciones para exportar alertas a un archivo externo que pueda importarse posteriormente a Security Analytics.

Requisitos previos

Asegúrese de haber comprendido los componentes de la vista Alerta. Para obtener más información, consulte Vista Alerta.

Procedimiento

Realice los siguientes pasos para exportar alertas a un archivo externo:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Alertas**.
   Se muestra la vista Alerta.
3. En el panel **Lista de alertas**, seleccione una alerta.
4. Haga clic en  > **Exportar**.
   El archivo binario exportado se guarda en la unidad local.

Importar una alerta

En este temase proporcionan instrucciones para importar alertas desde otras instancias de Security Analytics en el panel Lista de alertas. Las alertas importadas desde otra instancia de Security Analytics deben ser de un archivo binario válido.

Durante el proceso de importación, se selecciona el archivo binario y se especifica si las alertas existentes se deben sobrescribir con las alertas del mismo nombre que contengan el archivo binario de importación.

- Si elige sobrescribirlas, todas las reglas, listas e informes duplicados se sobrescribirán con los contenidos del archivo binario de importación.
- Si decide no sobrescribirlas y existe una regla, una lista o una alerta duplicada en la carpeta de destino, la importación se realizará y no se mostrará ningún mensaje acerca de las alertas duplicadas.

Requisitos previos

Asegúrese de:

- Tiene alertas exportadas desde otras instancias de Security Analytics.
- Haber comprendido los componentes de la vista Alerta. Para obtener más información, consulte Vista Alerta.
- Haber comprendido los componentes del cuadro de diálogo Importar una alerta. Para obtener más información, consulte Cuadro de diálogo Importar alerta.

Procedimiento

Realice los siguientes pasos para importar alertas desde otras instancias de Security Analytics al panel Lista de alertas:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Alertas**.
   Se muestra la vista Alerta.
3. En la barra de herramientas **Alerta**,  haga clic en> **Importar**.
   Se muestra el cuadro de diálogo Importar alerta.
4. Haga clic en **Navegar** para seleccionar el archivo binario.
   Security Analytics proporciona una vista del sistema de archivos de los archivos.
5. Busque el archivo binario y haga clic en **Abrir**.
   El archivo se agrega a la lista Importar gráfico.

6. (Opcional) Para sobrescribir cualquier alerta existente en la biblioteca con una alerta que tiene el mismo nombre en el archivo binario al realizar la importación, seleccione la casilla de verificación Alerta. Si no selecciona la opción Sobrescribir y se encuentra una alerta idéntica en el archivo binario, este archivo se importa y no se muestra ningún mensaje de error.
7. Haga clic en **Importar** para importar el archivo binario.

Actualizar una lista de alertas

En este tema se proporcionan instrucciones para actualizar la lista de alertas.

Requisitos previos

Asegúrese de haber comprendido los componentes de la vista Alerta. Para obtener más información, consulte Vista Alerta.

Procedimiento

Realice los siguientes pasos para actualizar la lista de alertas:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Alertas**.
   Se muestra la vista Alerta.
3. En la barra de herramientas **Alerta**, haga clic en para actualizar la lista de alertas.
   Se actualiza el panel Lista de alertas completo.

Definir plantillas de alertas

Este tema es un conjunto de tareas para configurar plantillas de alertas. Puede definir, eliminar, editar, importar y exportar plantillas de alertas en Security Analytics. Cada tema describe los procedimientos pertinentes.

Temas

- Agregar una plantilla
- Eliminar una plantilla
- Editar una plantilla
- Ver todas las plantillas

Agregar una plantilla

En este tema se proporcionan instrucciones para agregar una plantilla.

Requisitos previos

Asegúrese de:

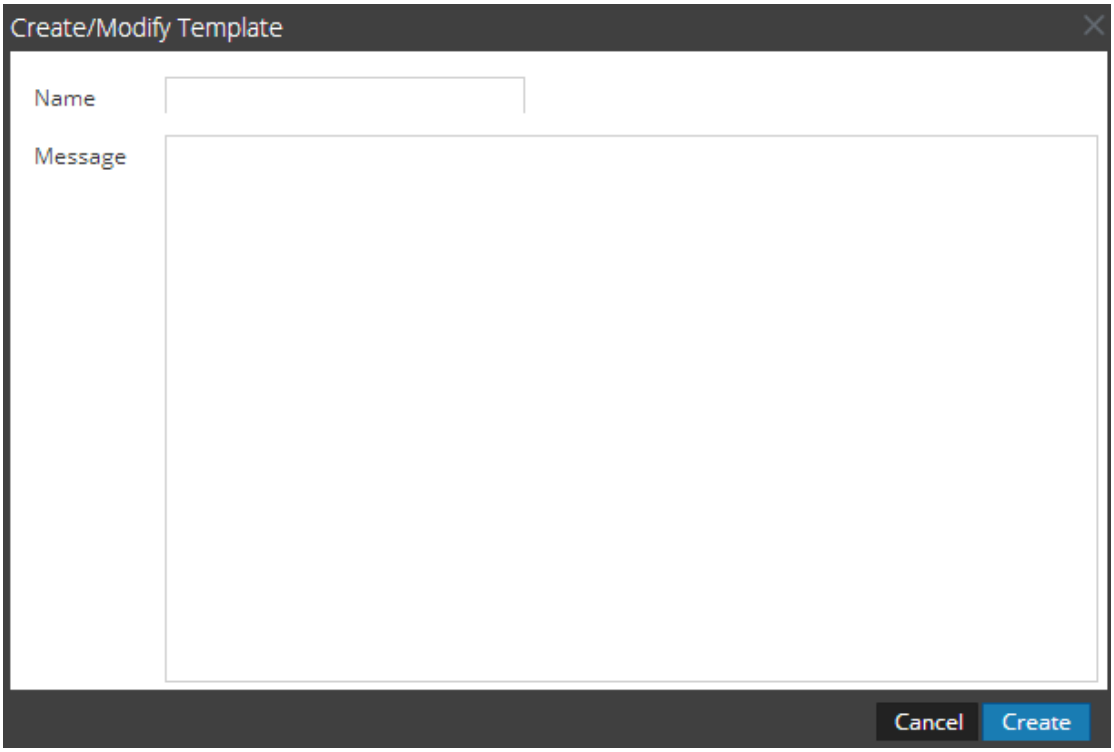
- Haber comprendido los componentes de la vista Alerta. Para obtener más información, consulte Vista Alerta.
- Haber comprendido los componentes de la vista Plantilla. Para obtener más información, consulte Barra de herramientas de Plantilla.

Procedimiento

Realice los siguientes pasos para agregar una plantilla:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Alertas**.
   Se muestra la vista Alerta.
3. Haga clic en Template.
   Se muestra la pestaña de la vista Plantilla.

4. En la barra de herramientas **Plantilla**, haga clic en +.
   Se muestra el cuadro de diálogo Crear/modificar plantilla.



5. Ingrese el nombre de la plantilla.
6. Ingrese un mensaje de alerta.
7. Haga clic en **Crear**.
   Se muestra un mensaje de confirmación que indica que la plantilla se creó correctamente.

Eliminar una plantilla

En este tema se proporcionan instrucciones para eliminar una plantilla.

Requisitos previos

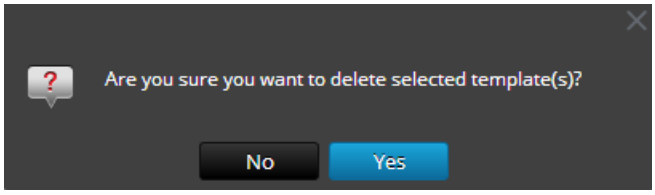
Asegúrese de:

- Haber comprendido los componentes de la vista Alerta. Para obtener más información, consulte . Vista Alerta.
- Haber comprendido los componentes de la vista Plantilla. Para obtener más información, consulte Barra de herramientas de Plantilla.

Procedimiento

Realice los siguientes pasos para eliminar una plantilla:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Alertas**.
   Se muestra la vista Alerta.
3. Haga clic en Template.
   Se muestra la pestaña de la vista Plantilla.
4. En el panel **Lista de plantillas**, seleccione la plantilla y haga clic en .
   Se muestra un cuadro de diálogo de confirmación.



5. Haga clic en **Sí** para eliminar la plantilla.
   Se muestra un mensaje de confirmación que indica que la plantilla se eliminó correctamente.

Editar una plantilla

En este tema, se proporcionan instrucciones para editar una plantilla.

Requisitos previos

Asegúrese de:

- Haber comprendido los componentes de la vista Alerta. Para obtener más información, consulte Vista Alerta.
- Haber comprendido los componentes de la vista Plantilla. Para obtener más información, consulte Barra de herramientas de Plantilla.
- Haber comprendido los componentes de la vista Crear o modificar plantilla. Para obtener más información, consulte Cuadro de diálogo Crear/modificar plantilla.

Procedimiento

Realice los siguientes pasos para editar una plantilla:

1. En el menú de Security Analytics, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Alertas**.
   Se muestra la vista Alerta.

3. Haga clic en Template.
   Se muestra la pestaña de la vista Plantilla.

4. En el panel **Lista de plantillas**, seleccione una plantilla y haga clic en .
   Se muestra el cuadro de diálogo Crear/modificar plantilla.
5. Modifique el nombre de la plantilla y el mensaje de alerta.
6. Haga clic en **Guardar**.
   Se muestra un mensaje de confirmación que indica que la plantilla se editó correctamente.

Ver todas las plantillas

En este tema se proporcionan instrucciones para ver todos los mensajes de plantilla.

Requisitos previos

Asegúrese de:

- Haber comprendido los componentes de la vista Alerta. Para obtener más información, consulte Vista Alerta.
- Haber comprendido los componentes de la vista Plantilla. Para obtener más información, consulte Barra de herramientas de Plantilla.

Procedimiento

Realice los siguientes pasos para ver todos los mensajes de plantilla:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Alertas**.
   Se muestra la vista Alerta.
3. En la barra de herramientas **Alerta**, haga clic en **Plantilla**.
   La pestaña de la vista Plantilla se muestra con una lista de plantillas.

Administrar el acceso para una alerta

En este tema se proporciona una descripción general de los permisos de acceso que puede tener el usuario de acuerdo con la función de usuario para administrar una alerta. El módulo Reporting proporciona el control de acceso en el nivel de alertas. Solo un usuario que posee el conjunto de permisos correcto puede ejecutar las tareas del módulo Reporting. El administrador administra el control de acceso en la pestaña **Administration > Seguridad > Funciones**.

Nota: Los permisos de alerta de Reporting Engine tienen el prefijo “RE” para distinguirlos de Event Streaming Analysis (ESA).

Cuando crea usuarios y funciones de usuario, el administrador debe asegurarse de que las funciones creadas para tareas específicas tengan acceso a todos los permisos más altos en la jerarquía de funciones.

Las alertas se pueden vincular a un conjunto específico de funciones de usuario de modo que, cuando un usuario inicie sesión en Security Analytics, las únicas alertas a las que pueda acceder sean alertas accesibles a la función a la cual pertenece. Los usuarios que pertenecen a una función de usuario con el permiso de acceso “Lectura y escritura” pueden definir alertas. Además, el acceso se puede restringir de modo que solo accedan a las alertas quienes tengan el acceso de “Solo lectura”.

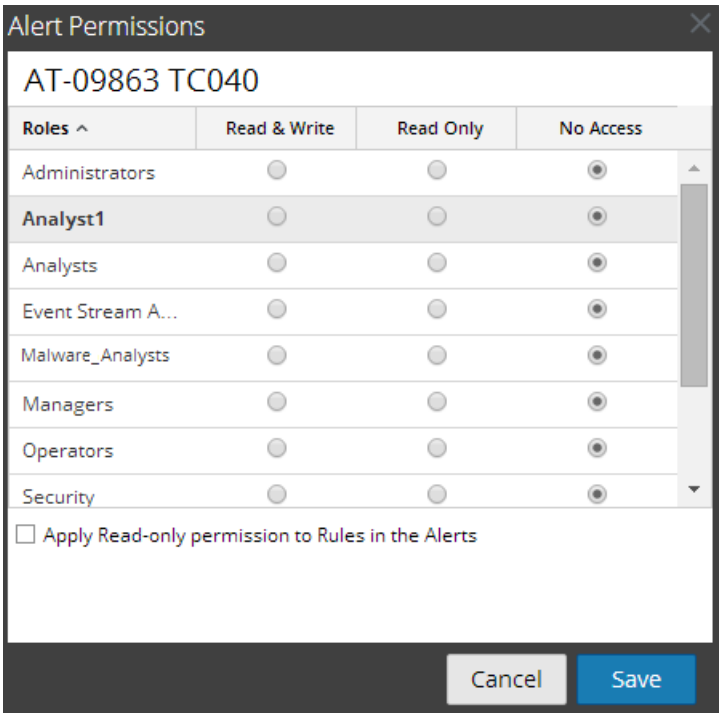
En el nivel de alerta, puede establecer los siguientes permisos de acceso para las funciones de usuario en Security Analytics:

- Lectura y escritura
- Solo lectura
- Sin acceso

Control de acceso para una alerta

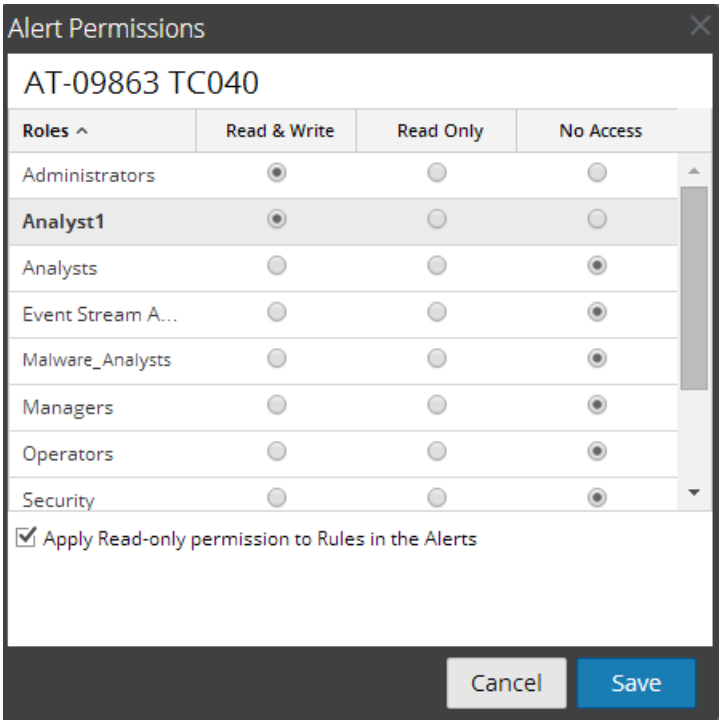
Cuando desea cambiar los permisos de alertas, debe seleccionar una alerta y configurar sus permisos de acceso en el panel Permisos de alerta.

Antes de aplicar permisos de alertas, el permiso predeterminado configurado para todas las funciones de usuario es el permiso “Sin acceso” y la casilla de verificación está deseleccionada, como se muestra en la figura.



Si desea cambiar el permiso de acceso para una función de usuario específica, debe configurarlo en el nivel de alerta, como se muestra en la figura. Suponga que desea que los **administradores** tengan acceso a una alerta específica. Para esto, puede configurar el permiso "**Lectura y escritura**" en el panel Permisos de alerta.

Además, puede aplicar permisos de solo lectura a las reglas en las alertas si selecciona la casilla de verificación.



Los dos escenarios se explican de forma resumida:

- Escenario 1: permisos aplicados a alertas/reglas de acuerdo con la función del usuario.
- Escenario 2: Permiso de solo lectura aplicado a reglas en la alerta.

	Función (analistas)	Permisos aplicados a alertas/reglas de acuerdo con la función del usuario	Permiso (de solo lectura) aplicado a las reglas de las alertas
Alerta	Lectura y escritura	**Lectura y escritura**	Lectura y escritura
Reglas	Lectura	**Lectura**	**Lectura**

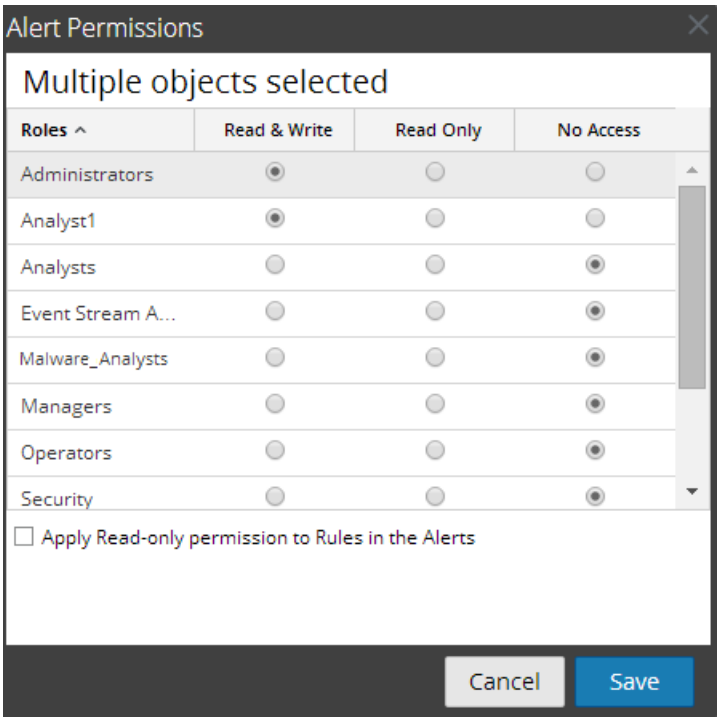
A la alerta se asigna la función de un **analista de seguridad** y los permisos se configuran en **Lectura y escritura** para las alertas.

En el escenario 1, cada uno de los niveles tiene un permiso configurado según la función del usuario. En el escenario 2 se configura el permiso de lectura para las reglas, salvo que el permiso para las reglas no debe ser mayor que el permiso para las alertas.

Nota: Si el permiso para las reglas es mayor que el permiso para las alertas, el permiso no se aplica. Por ejemplo, si configura los permisos para la alerta como **Sin acceso** y especifica la opción *Aplicar permisos de solo lectura a las reglas de las alertas*, el permiso de solo lectura no se configura para las reglas.

Control de acceso para una alerta cuando se seleccionan múltiples alertas

Cuando desea cambiar los permisos de varias alertas, debe seleccionarlas y configurar sus permisos de acceso en el panel Permisos de alerta. El permiso de acceso que elige se aplica a todas las alertas seleccionadas.

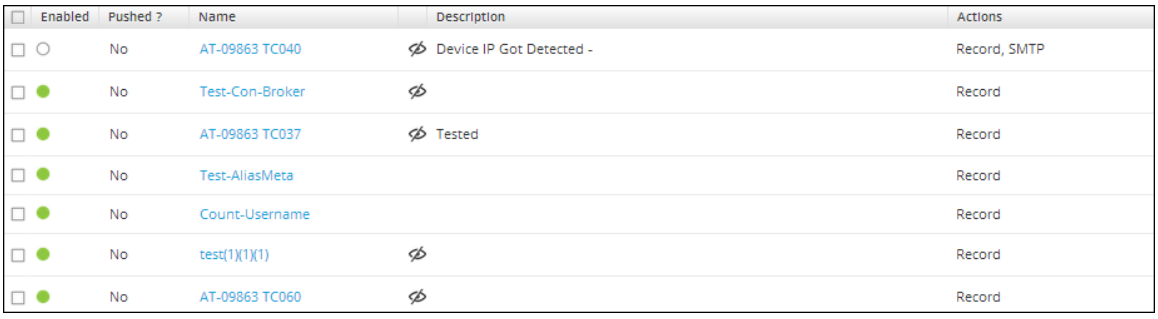


Inicie sesión como un usuario específico y vea los detalles de acceso

Cuando inicia sesión en la interfaz del usuario de Security Analytics como un usuario que tiene el permiso "Acceso de lectura", todas las alertas se marcan con el símbolo (📖), y cuando hace clic en el símbolo, se muestra la leyenda "Solo lectura" en el panel Lista de alertas.

Cuando inicia sesión en la interfaz del usuario de Security Analytics como un usuario que no tiene el permiso de acceso "Lectura y escritura" en una alerta, todas las alertas se marcan con el símbolo ( ) y aparecen en gris en el panel Lista de alertas.

En la siguiente figura se muestra el panel Lista de alertas cuando se inicia sesión con un permiso de acceso de "Lectura y escritura" mínimo.



Nota: Si un usuario (que no sea el superusuario) crea una alerta, no habrá acceso a la alerta para el superusuario.

En la siguiente tabla se indican las diversas columnas del panel Permisos de alerta:

Columna	Descripción
Funciones	La función del usuario que inició sesión en la interfaz del usuario de Security Analytics.
Lectura y escritura	El usuario puede acceder, ver, editar, importar, exportar y eliminar la alerta en la página Alertas. El usuario también puede cambiar el permiso en la alerta.
Solo lectura	El usuario solo puede acceder a la alerta y verla en la vista Alertas.
Sin acceso	El usuario no puede acceder a una alerta ni verla cuando tiene configurado este permiso.
 Aplicar permisos de solo lectura a las reglas de las alertas	Seleccione la casilla de verificación para aplicar permisos a las reglas de las alertas de forma automática.

Temas

- Establecer el control de acceso para una alerta

Establecer el control de acceso para una alerta

En este tema se proporcionan instrucciones para establecer el control de acceso para una alerta.

Requisitos previos

Asegúrese de:

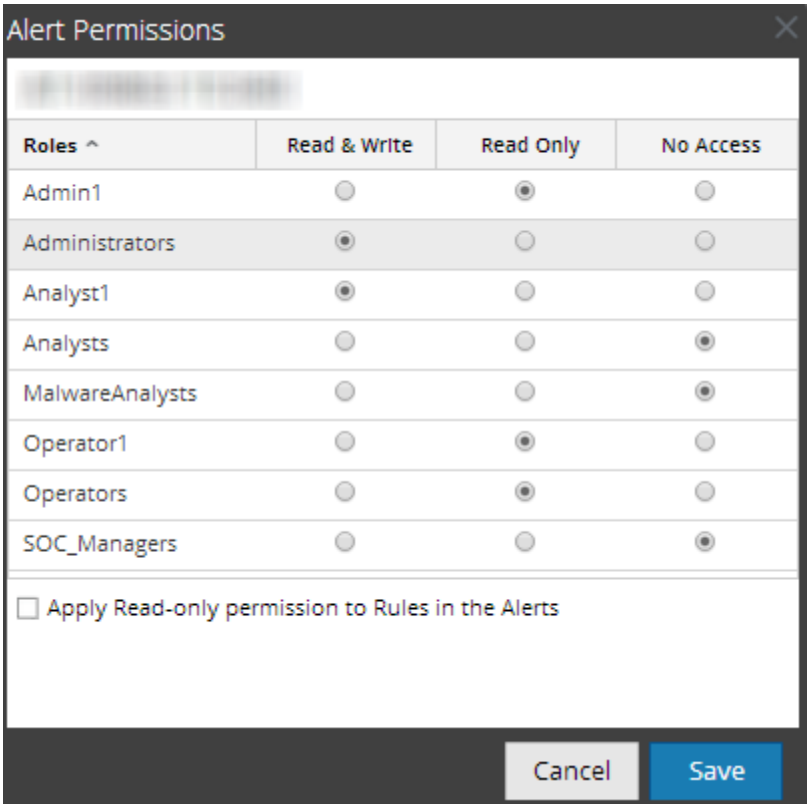
- Haber comprendido los componentes de la vista Alerta. Para obtener más información, consulte Vista Alerta.
- Haber comprendido los permisos de acceso que tendrá el usuario según la función de usuario. Para obtener más información, consulte Administrar el acceso para una alerta.

- Tener un permiso de acceso de “Lectura y escritura” mínimo para establecer permisos de acceso para una alerta.

Procedimiento

Realice los siguientes pasos para establecer permisos de acceso para una alerta:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Alertas**.
   Se muestra la vista Alerta.
3. En el panel **Lista de alertas**, seleccione una alerta.
4. Haga clic en > **Permisos**.
   Aparece el cuadro de diálogo Permisos de alerta.



5. Según la función de usuario, seleccione los botones que correspondan.
6. (Opcional) Seleccione la casilla de verificación si desea proporcionar automáticamente un permiso de acceso de lectura a las reglas dependientes.

Nota: cuando se selecciona la casilla de verificación, a todas las reglas dependientes con permiso Sin acceso se les otorga permiso de acceso de LECTURA.

6. Haga clic en **Guardar**.
   Se muestra un mensaje de confirmación que indica que el permiso se estableció correctamente para la alerta seleccionada.

Configurar Security Analytics para que genere una alerta

En este tema se proporcionan instrucciones para configurar Security Analytics a fin de que genere una alerta.

Procedimiento

Realice los siguientes pasos para configurar Security Analytics de modo que genere una alerta:

1. Configure un origen de datos de NWDB para Reporting Engine.
2. Cree alertas:
   a. Agregue o modifique una alerta en la Vista Crear o modificar alerta.
   b. (Opcional) Configure plantillas de mensajes de alerta en la Barra de herramientas de Plantilla.
3. Programe alertas en Ver calendario de alertas.
   Después de activar una alerta en la vista Ver calendario de alertas, Security Analytics la ejecuta una vez por minuto (de forma predeterminada).
4. Vea las alertas que se activaron en Ver una lista de alertas.

Temas

- Desactivar una alerta calendarizada
- Ver una lista de alertas
- Ver calendario de alertas

Desactivar una alerta calendarizada

En este tema se proporcionan instrucciones para deshabilitar las alertas calendarizadas y quitar las alertas.

Requisitos previos

Asegúrese de:

- Haber comprendido los componentes de la vista Alerta. Para obtener más información, consulte . Vista Alerta.
- Haber comprendido los componentes de Ver calendario de alertas. Para obtener más información, consulte Vista Ver calendario de alertas.

Procedimiento

Realice los siguientes pasos para inhabilitar una alerta calendarizada:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Alertas**.
   Se muestra la vista Alerta.
3. Haga clic en View Schedule.
   Se muestra la pestaña de la vista Ver calendario de alertas.
4. En el panel **Lista de calendario de alertas**, seleccione las alertas calendarizadas que desea deshabilitar.
5. Haga clic en ○.
   Un mensaje de confirmación indica que el estado de las alertas se cambió exitosamente y que las alertas ahora están disponibles en el panel Lista de alertas.

Ver una lista de alertas

En este tema se proporcionan instrucciones para ver alertas. Debe ver las alertas en función de la fecha seleccionada y la cantidad máxima de alertas.

Requisitos previos

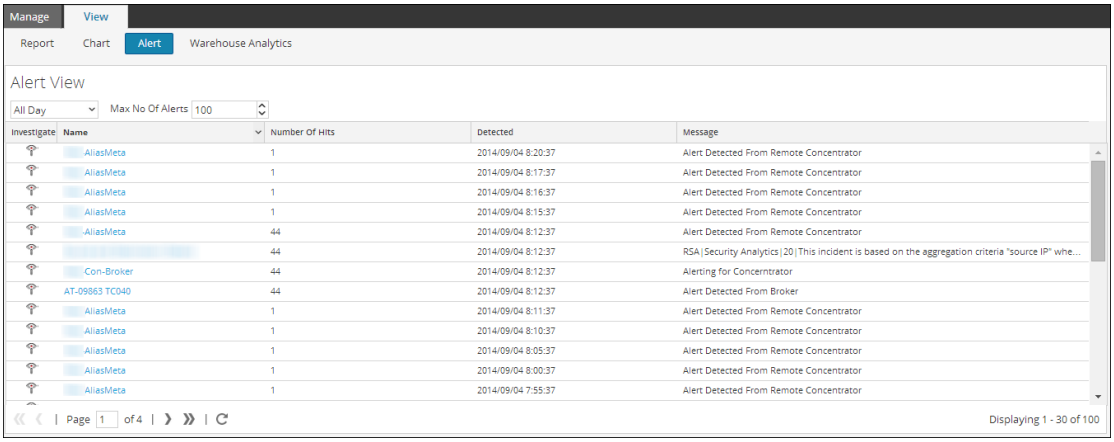
Asegúrese de:

- Haber comprendido los componentes de la vista Alerta. Para obtener más información, consulte Vista Alerta.
- Haber comprendido los componentes del panel Ver alertas. Para obtener más información, consulte Panel Ver alertas.

Procedimiento

Realice los siguientes pasos para ver alertas:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Alertas**.
   Se muestra la vista Alerta.
3. En la barra de herramientas **Alerta**, haga clic en **Ver alertas**.
   Se muestra la pestaña de la vista Ver alertas.



4. Seleccione la última cantidad de días en la lista desplegable.
5. Ingrese un valor en **Número máximo de alertas**.
   La lista de alertas se muestra en función del valor del filtro elegido.

Ver calendario de alertas

En este tema se proporcionan instrucciones para ver las alertas calendarizadas. Debe ver las alertas calendarizadas para conocer el estado de la alerta.

Requisitos previos

Asegúrese de:

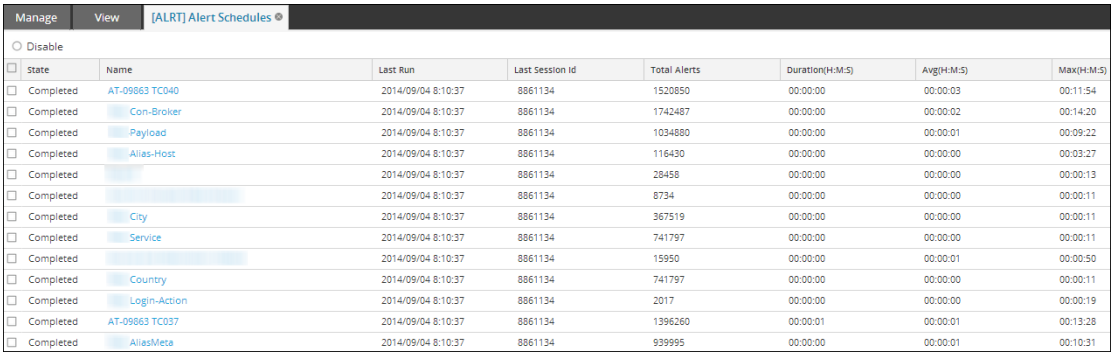
- Haber comprendido los componentes de la vista Alerta. Para obtener más información, consulte Vista Alerta.
- Haber comprendido los componentes de Ver calendario de alertas. Para obtener más información, consulte Vista Ver calendario de alertas.

Procedimiento

Realice los siguientes pasos para ver las alertas calendarizadas:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.

2. Haga clic en **Alertas**.
   Se muestra la vista Alerta.
3. En la barra de herramientas **Alerta**, haga clic en **Ver calendario**.
   La pestaña Ver calendario de alertas se muestra con una lista de alertas calendarizadas.



State	Name	Last Run	Last Session Id	Total Alerts	Duration(H:M:S)	Avg(H:M:S)	Max(H:M:S)
Completed	AT-09863 TC040	2014/09/04 8:10:37	8861134	1520850	00:00:00	00:00:03	00:11:54
Completed	Con-Broker	2014/09/04 8:10:37	8861134	1742487	00:00:00	00:00:02	00:14:20
Completed	Payload	2014/09/04 8:10:37	8861134	1034880	00:00:00	00:00:01	00:09:22
Completed	Alias-Host	2014/09/04 8:10:37	8861134	116430	00:00:00	00:00:00	00:03:27
Completed		2014/09/04 8:10:37	8861134	28458	00:00:00	00:00:00	00:00:13
Completed		2014/09/04 8:10:37	8861134	8734	00:00:00	00:00:00	00:00:11
Completed	City	2014/09/04 8:10:37	8861134	367519	00:00:00	00:00:00	00:00:11
Completed	Service	2014/09/04 8:10:37	8861134	741797	00:00:00	00:00:00	00:00:11
Completed		2014/09/04 8:10:37	8861134	15950	00:00:00	00:00:01	00:00:50
Completed	Country	2014/09/04 8:10:37	8861134	741797	00:00:00	00:00:00	00:00:11
Completed	Login-Action	2014/09/04 8:10:37	8861134	2017	00:00:00	00:00:00	00:00:19
Completed	AT-09863 TC037	2014/09/04 8:10:37	8861134	1396260	00:00:01	00:00:01	00:13:28
Completed	AliasMeta	2014/09/04 8:10:37	8861134	939995	00:00:00	00:00:01	00:10:31

Investigar una alerta

En este tema se proporcionan instrucciones para investigar una alerta. Puede investigar cada alerta que se active y los detalles de investigación de una alerta específica se muestran en el módulo Investigation.

Requisitos previos

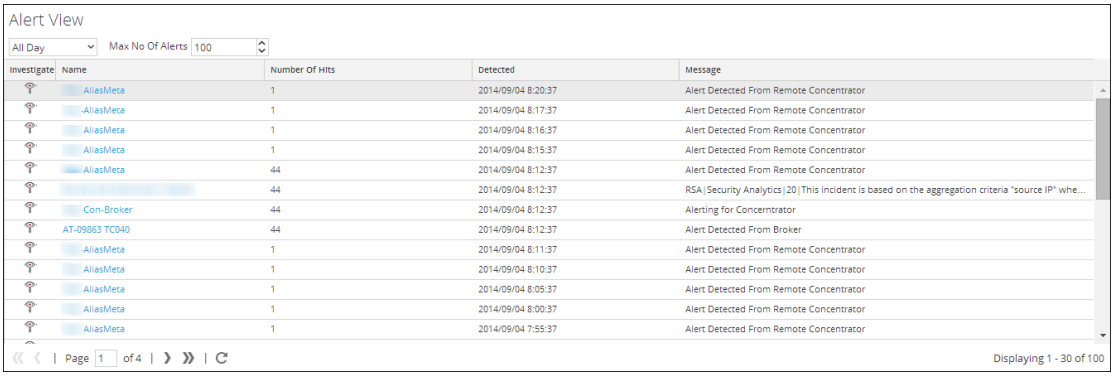
Asegúrese de haber comprendido los componentes del panel Ver alertas. Para obtener más información, consulte Panel Ver alertas.

Procedimiento

Procedimiento

Realice los siguientes pasos para investigar una alerta:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Alertas**.
   Se muestra la vista Alerta.
3. En la barra de herramientas **Alerta**, haga clic en **Ver alertas**.
   Se muestra la pestaña de la vista Ver alertas.



4. Realice una de las siguientes acciones

   - Haga clic en el botón en la alerta que desea investigar.

     El módulo Investigation muestra los detalles de la primera sesión que registró la coincidencia de la alerta especificadapara realizar un análisis inmediato.

   - Haga clic en el nombre de la alerta que desea investigar.

     El módulo Investigation muestra todas las coincidencias de una alerta en especial durante la hora aproximada en la que se registró la alerta.

Configurar el motor de creación de informes para enviar mensajes de Sylog mediante TCP/TLS para las alertas

En este tema se proporcionan instrucciones para configurar Reporting Engine de modo que envíe mensajes de syslog mediante TCP con Transport Layer Security (TLS) cuando se activa una alerta.

Requisitos previos

Asegúrese de haber instalado y configurado un servidor de syslog que sea compatible con TCP/TLS en el ambiente. Por ejemplo, WinSyslog.

Procedimiento

Realice los siguientes pasos para configurar Reporting Engine de modo que envíe una alerta de syslog mediante TCP con Transport Layer Security (TLS):

1. Obtenga los certificados necesarios.
2. (Opcional) Convierta el formato del certificado de PEM a JKS.

3. Copie los pares de claves generados para el servidor de Reporting Engine y el servidor de Syslog.
4. Configure la distribución de los mensajes de alerta en Security Analytics.

Tarea 1: Obtenga los certificados necesarios

Realice lo siguiente a fin de generar certificados para configurar Reporting Engine para que envíe mensajes de syslog mediante TCP con TLS:

1. Genere un certificado de autoridad de certificación (CA). Para obtener más información, consulte http://www.rsyslog.com/doc/tls_cert_ca.html.

Nota: Puede omitir este paso si ya tienen un CA ejecutándose en su ambiente.

2. Genere el par de claves (clave pública y clave privada) para el servidor de Reporting Engine. Para obtener más información, consulte http://www.rsyslog.com/doc/tls_cert_machine.html.
3. Genere el par de claves para el servidor de Syslog. Para obtener más información, consulte http://www.rsyslog.com/doc/tls_cert_machine.html.

Nota: Puede omitir este paso, si ya configuró la seguridad del servidor de syslog con la clave y los certificados generados por la misma CA.

Tarea 2: (Opcional) Convierta el formato del certificado de PEM a JKS

Si ha generado los certificados en formato PEM (Privacy Enhanced Mail), debe convertir el formato del certificado a formato Java KeyStore (JKS). Realice lo siguiente en la máquina donde instaló el servidor de Reporting Engine.
Para convertir los certificados con formato PEM a JKS:

1. Convierta los certificados en formato PEM existentes a archivos PKCS. En la línea de comandos, escriba el siguiente comando y presione INTRO:

```
openssl pkcs12 -export -in <certificate.pem> -inkey <private_
key.pem> -out <sample>.p12 -name re
 -CAfile ca.pem -caname root
```

Donde:

- `certificate.pem`: es el certificado en formato PEM.
- `private_key.pem`: es la clave privada en formato PEM.
- `sample`: es el archivo PKCS12 creado durante la conversión.
- `ca.pem`: es el certificado de CA.

2. Convierta el archivo PKCS12 existente en un certificado con formato JKS para crear el almacenamiento de claves. En el símbolo del sistema, escriba el siguiente comando y presione INTRO:

   ```
   keytool -importkeystore -destkeystore<re-keystore.jks> -srckeystore <sample>.p12 -srcstoretype PKCS12 -alias re
   ```

   Donde:

   - `re-keystore.jks`: es el certificado en formato JKS.
   - `sample`: es el archivo PKCS12 creado durante la conversión.
   - `ca.pem`: es el certificado de CA.

3. Agregar el certificado de CA (ca.pem) a Truststore. En la línea de comandos, escriba el siguiente comando y presione INTRO:

   ```
   keytool -importcert -alias myca -file <ca.pem> -keystore <re-truststore.jks>
   ```

   Donde:

   - `ca.pem`: es el certificado de CA.
   - `re-truststore.jks`: es el certificado de CA en formato JKS.

Nota: Asegúrese de anotar las contraseñas que proporciona para Keystore y Truststore durante la conversión. Debe proporcionar estas contraseñas cuando habilite SECURE_TCP en Security Analytics.

Tarea 3: Copie los pares de claves generados

Copie manualmente los pares de claves (Keystore y Truststore) desde la ubicación donde los generó a **/home/rsasoc/rsa/soc>/reporting-engine/keystores/**, ubicación del servidor de Reporting Engine.

Tarea 4: Configure la distribución de los mensajes de alerta en Security Analytics

Configure Reporting Engine para que envíe mensajes de syslog a través de TCP con Transport Layer Security (TLS) cuando se active una alerta, mediante la habilitación de **SECURE_TCP** en la pestaña **Acciones de salida** para el servicio Reporting Engine en la vista Configuración de servicios de Reporting Engine. Para obtener más información, consulte el tema Acciones de salida de Reporting Engine de la *Guía de configuración de hosts y servicios*.

Trabajar con listas en el módulo Reporting

El módulo Listas permite definir y ver listas que se pueden usar en informes.

Temas:

- Descripción general de listas
- Definir listas y grupos de listas
- Administrar el acceso para una lista o un grupo de listas

Descripción general de listas

En este tema se proporciona una descripción breve de una lista. Una lista es una variable que hace referencia a una serie de valores separados por comas (CSV). Puede insertar una lista en una regla o usarla como argumento para una acción de regla. Las listas pueden actuar como marcadores de posición para otros valores, los que puede completar y actualizar según sea necesario.

Nota: En la interfaz del usuario, la fecha o la hora mostradas dependen del perfil de zona horaria que seleccionó el usuario

Las listas no pueden estar vacías ni tener valores duplicados o en blanco. Por ejemplo, incluso si la lista tiene un valor, no puede estar en blanco.

Nota: Si va a definir un informe con una regla que tiene lookup_and_add en la cláusula Then y dirigir la salida de informe a una lista, a lista no se completa con el resultado.
Por ejemplo, si crea una regla con ip.src en la cláusula Select y lookup_and_add ('ip.dst','ip.src', 10) en la cláusula Then, el informe muestra el resultado, pero si redirigió la salida a una lista, la lista estará vacía.

Definir listas y grupos de listas

Este tema es un conjunto de tareas para configurar grupos de listas y listas. Puede definir, eliminar, editar, importar y exportar grupos de listas y listas en Security Analytics. Cada tema describe los procedimientos pertinentes.

Temas

- Agregar una lista
- Agregar un grupo de listas
- Eliminar una lista

- Eliminar un grupo de listas
- Duplicar una lista
- Editar una lista
- Exportar una lista
- Exportar un grupo de listas
- Importar listas y grupos de listas

Agregar una lista

En este tema se proporcionan instrucciones para crear una lista. Las listas se pueden agregar dentro de un grupo o en la carpeta raíz.

Requisitos previos

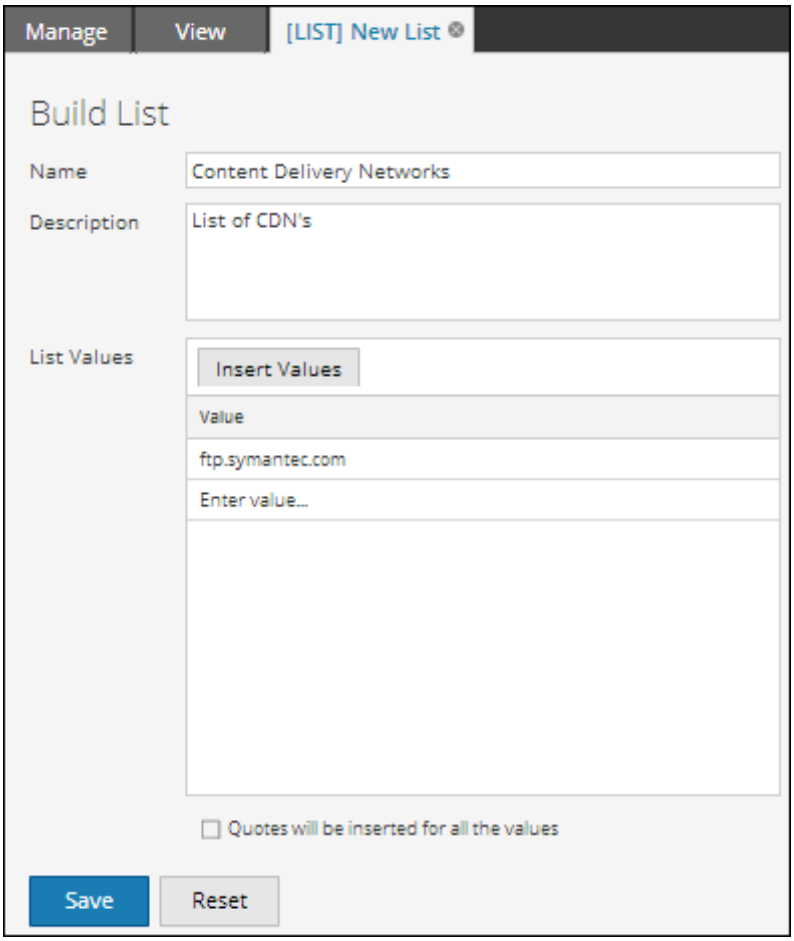
Asegúrese de:

- Comprende los componentes de la vista Lista. Para obtener más información, consulte Vista de lista.
- Comprender los componentes de la vista Crear lista. Para obtener más información, consulte Vista Crear lista.

Procedimiento

Realice los siguientes pasos para crear una lista:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Listas**.
   Se muestra la vista Lista.
3. En la barra de herramientas **Lista**, haga clic en .
   Se muestra la pestaña de la vista Crear lista.



4. En el campo **Nombre**, ingrese un nombre único para la lista.
5. En el campo **Descripción**, ingrese una descripción de la lista.
6. En el campo **Valores de lista**, realice una de las siguientes acciones:
   - Haga clic en **Insertar** e ingrese los valores separados por comas. Puede pegar una lista de valores de un archivo o de otras listas definidas.
   - En la columna **Valor**, ingrese los valores.
7. Si desea que se inserten comillas directamente para los valores en el tiempo de ejecución, seleccione la opción **Se insertarán comillas para todos los valores**.
8. Haga clic en **Guardar**.

Agregar un grupo de listas

En este tema se proporcionan instrucciones para agregar grupos de listas y subgrupos de listas.

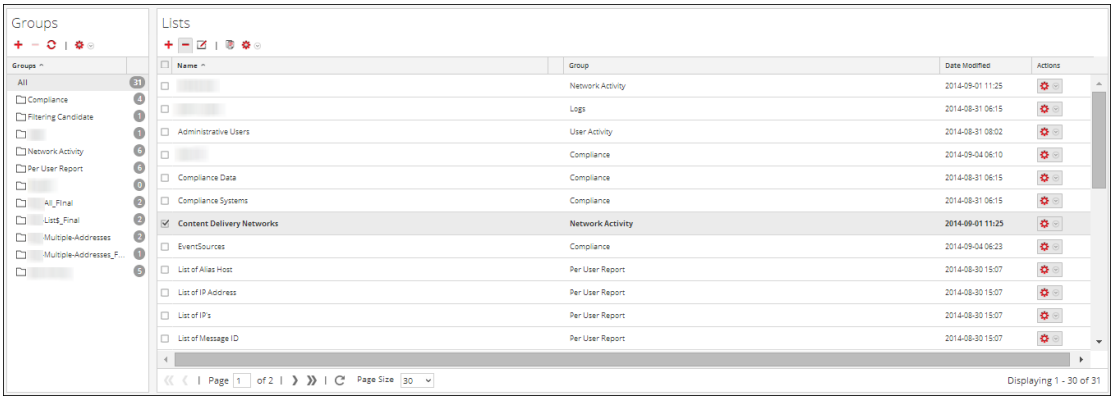
Requisitos previos

Asegúrese de comprender los componentes de la vista de lista. Para obtener más información, consulte Vista de lista.

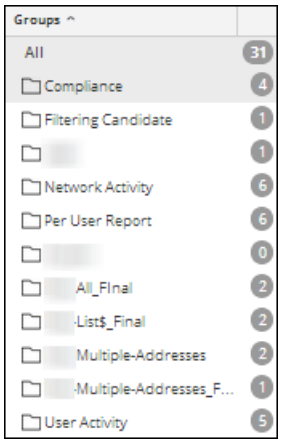
Procedimiento

Realice los siguientes pasos para agregar grupos de listas y subgrupos de listas:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Listas**.
   Se muestra la vista Lista.



3. Realice una de las siguientes acciones:
   - Para crear un grupo de listas:
     1. En el panel Grupos de listas, haga clic en +.
        En la siguiente figura se muestra el nuevo grupo de listas agregado al panel Grupos de listas.



2. Escriba el nombre del grupo de listas y presione INTRO.
   - Para agregar un subgrupo de listas:
     1. En el panel Grupos de listas, seleccione el grupo de listas para el que desea agregar un subgrupo.
     2. Haga clic en +.
        Se agrega un nuevo subgrupo de listas al grupo de listas.
     3. Escriba el nombre del subgrupo de listas y presione INTRO.

Eliminar una lista

En este tema se proporcionan instrucciones para eliminar una o varias listas.

Requisitos previos

Asegúrese de comprender los componentes de la vista de lista. Para obtener más información, consulte Vista de lista.

Procedimiento

Realice los siguientes pasos para eliminar una lista:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Listas**.
   Se muestra la vista Lista.
3. En el panel **Vista de lista**, realice una de las siguientes acciones:
   - Seleccione una o varias listas que desee eliminar y haga clic en − en la barra de herramientas Listas.

- Haga clic en  **>Eliminar**.

  Un cuadro de diálogo solicita confirmar que desea eliminar las listas seleccionadas.

  Nota: Antes de eliminar una lista, asegúrese de que la lista no esté asociada a ninguna regla.

4. Haga clic en **Sí** para eliminar la lista.

   Se muestra un mensaje que confirma la correcta eliminación de la lista y la lista seleccionada se elimina del panel Vista de lista.

Eliminar un grupo de listas

En este tema se proporcionan instrucciones para eliminar un grupo de listas.

Requisitos previos

Asegúrese de comprender los componentes de la vista de lista. Para obtener más información, consulte Vista de lista.

Procedimiento

Realice los siguientes pasos para eliminar un grupo de listas:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.

   Se muestra la pestaña Administrar.

2. Haga clic en **Listas**.

   Se muestra la vista Lista.

3. En el panel **Grupos de listas**, seleccione el grupo y haga clic en .

   Un cuadro de diálogo solicita confirmar que desea eliminar el grupo seleccionado.

   Precaución: Si elimina un grupo, se eliminan todos los subgrupos y las listas de ese grupo.

4. Haga clic en **Sí** para eliminar el grupo seleccionado.

   Se muestra un mensaje que confirma la correcta eliminación del grupo y el grupo seleccionado se elimina del panel Grupos de listas.

Nota: Si intenta eliminar un grupo de listas cuyas listas se usan como referencia en una regla o alerta, se muestra un mensaje de advertencia que informa que una regla hace referencia a las listas.

Duplicar una lista

En este tema se proporcionan instrucciones para duplicar una lista.

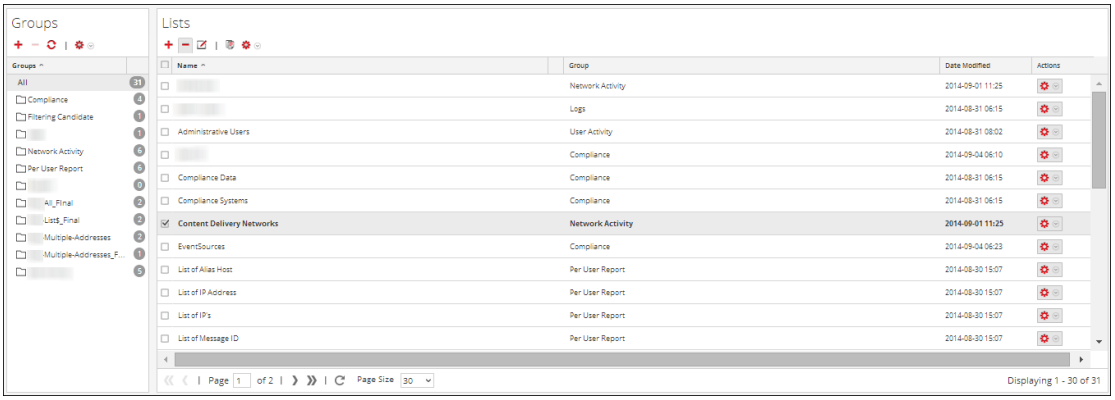
Requisitos previos

Asegúrese de comprender los componentes de la vista de lista. Para obtener más información, consulte Vista de lista.

Procedimiento

Realice los siguientes pasos para duplicar una lista:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Listas**.
   Se muestra la vista Lista.



3. En el panel **Vista de lista**, seleccione una lista que desee duplicar.

   Nota: Solo puede duplicar una lista por vez.

4. En la barra de herramientas **Lista**, haga clic en .

Editar una lista

En este tema se proporcionan instrucciones para editar una lista.

Requisitos previos

Asegúrese de:

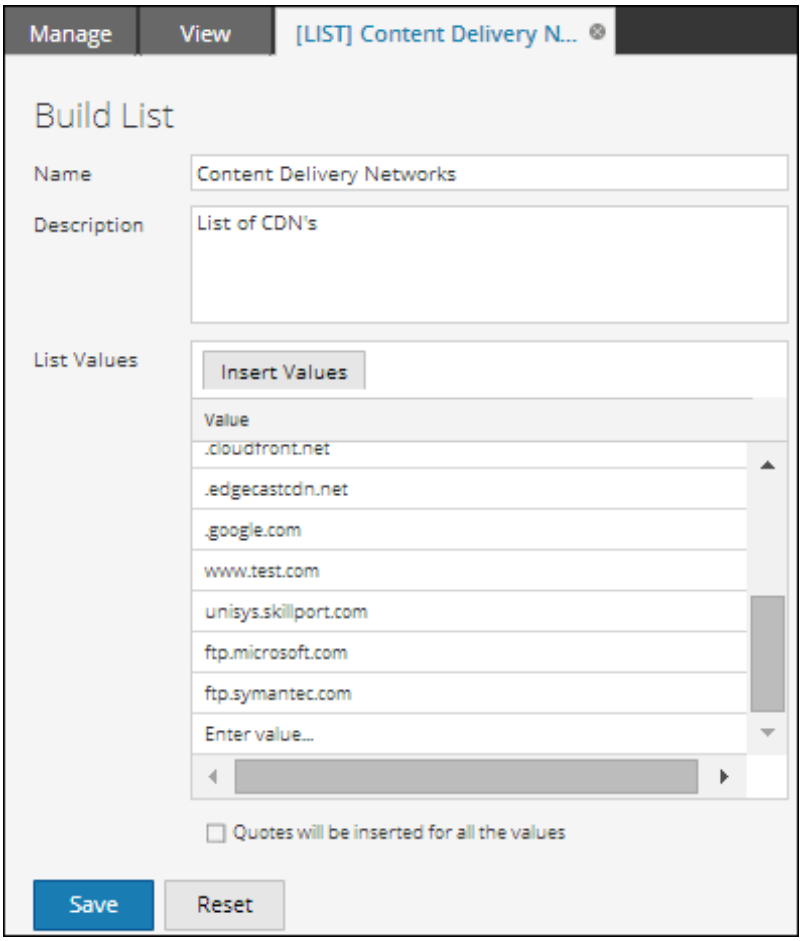
- Comprende los componentes de la vista Lista. Para obtener más información, consulte Vista de lista.
- Comprender los componentes de la vista Crear lista. Para obtener más información, consulte Vista Crear lista.

Procedimiento

Realice los siguientes pasos para editar una lista**:**

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Listas**.
   Se muestra la vista Lista.
3. En el panel **Vista de lista**, seleccione una lista que desee editar.
4. Realice una de las siguientes acciones:
   - Haga clic en  en la barra de herramientas Lista.
   - En el panel Vista de lista, haga clic en  > **Editar**.

   Se muestra la pestaña de la vista Crear lista.



Nota: Solo puede editar una lista por vez.

5. Modifique los campos requeridos y agregue nuevos valores a la lista.
6. Haga clic en **Guardar**.
   Se muestra un mensaje de confirmación que indica que la lista se guardó correctamente.

Exportar una lista

En este tema se proporcionan instrucciones para exportar una lista del panel Vista de lista.

Requisitos previos

Asegúrese de comprender los componentes de la vista de lista. Para obtener más información, consulte Vista de lista.

Procedimiento

Realice los siguientes pasos para exportar una lista:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Listas**.
   Se muestra la vista Lista.
3. En el panel **Vista de lista**, realice una de las siguientes acciones.
   - Seleccione una lista y haga clic en  **> Exportar** en la barra de herramientas Lista.
   - Haga clic en  > **Exportar**.

   Puede aparecer un cuadro de diálogo de exportación específico del navegador que permite abrir o guardar el archivo.

Nota: Solo puede exportar una lista por vez.

Exportar un grupo de listas

En este tema se proporcionan instrucciones para exportar un grupo de listas. Puede exportar grupos de listas seleccionados a un archivo externo que posteriormente se puede importar en Security Analytics. Si no se selecciona nada en el panel Biblioteca de listas, entonces se exporta el árbol de lista completo. Cuando se exporta, el resultado es un único archivo de exportación en formato binario.

Requisitos previos

Asegúrese de comprender los componentes de la vista de lista. Para obtener más información, consulte Vista de lista.

Procedimiento

Realice los siguientes pasos para exportar un grupo de listas:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Listas**.
   Se muestra la vista Lista.
3. En el panel **Grupos de listas**, seleccione el grupo de listas que contiene las listas que desea exportar.
4. Haga clic en  > **Exportar**.
   El archivo exportado se guarda en la unidad local.

Importar listas y grupos de listas

En este tema se proporciona información para importar listas y grupos de listas. Puede importar listas y grupos de listas desde instancias de Security Analytics en el árbol de listas del panel Grupos de listas. Las listas deben estar en un archivo binario válido que se haya exportado desde una instancia de Security Analytics.

Requisitos previos

Asegúrese de:

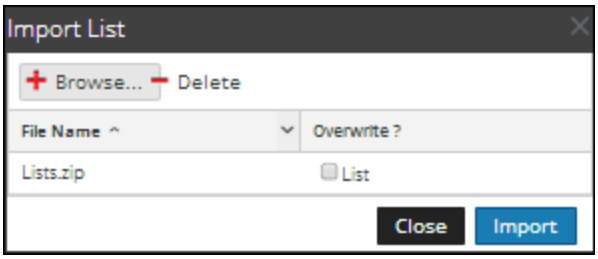
- Las listas o los grupos de listas se exportan desde una instancia de Security Analytics.
- Haber comprendido los componentes de la vista Lista. Para obtener más información, consulte Vista de lista.

Procedimiento

Realice los siguientes pasos para importar listas o grupos de listas:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Listas**.
   Se muestra la vista Lista.
3. Realice una de las siguientes acciones:
   - En el panel **Grupos de listas**, haga clic en > **Importar**.
   - En la barra de herramientas **Lista**, haga clic en > **Importar**.

   Se muestra el cuadro de diálogo Importar lista.



4. Haga clic en **Navegar** para navegar y seleccionar el archivo que contiene las listas.
5. Haga clic en **Importar**.

Nota: Durante el proceso de importación, si hay una lista duplicada y no selecciona la opción para sobrescribir, se importan la lista y no se muestra un mensaje acerca de la duplicación de listas.

Administrar el acceso para una lista o un grupo de listas

En este tema se describen los permisos de acceso que tiene el usuario según la función del usuario para administrar una lista o un grupo de listas. El módulo Reporting proporciona un control de acceso en el nivel de lista y grupo de listas. Solo un usuario con el conjunto de permisos correcto puede ejecutar las tareas del módulo Reporting. El administrador administra el control de acceso desde la pestaña **Administration > Seguridad > Funciones**.

Cuando el administrador crea usuarios y funciones de usuario, debe asegurarse de que las funciones creadas para tareas específicas tengan acceso a todos los permisos más altos en la jerarquía de funciones.

Las listas o los grupos de listas se pueden vincular a un conjunto específico de funciones de usuario de modo que, cuando un usuario inicie sesión en Security Analytics, las únicas listas a las que pueda acceder sean listas accesibles al grupo al cual pertenece. Los usuarios que pertenecen a una función de usuario con el permiso de acceso “Lectura y escritura” tienen derechos de acceso completos para la lista. Además, el acceso se puede restringir de modo que solo accedan a las listas quienes tengan el acceso de “Solo lectura”.

Nota: debe tener permiso de “Solo lectura” en un grupo para ver las listas dentro de ese grupo.

En el nivel de la lista, puede establecer los siguientes permisos de acceso para las funciones de usuario en Security Analytics:

- Lectura y escritura
- Solo lectura
- Sin acceso

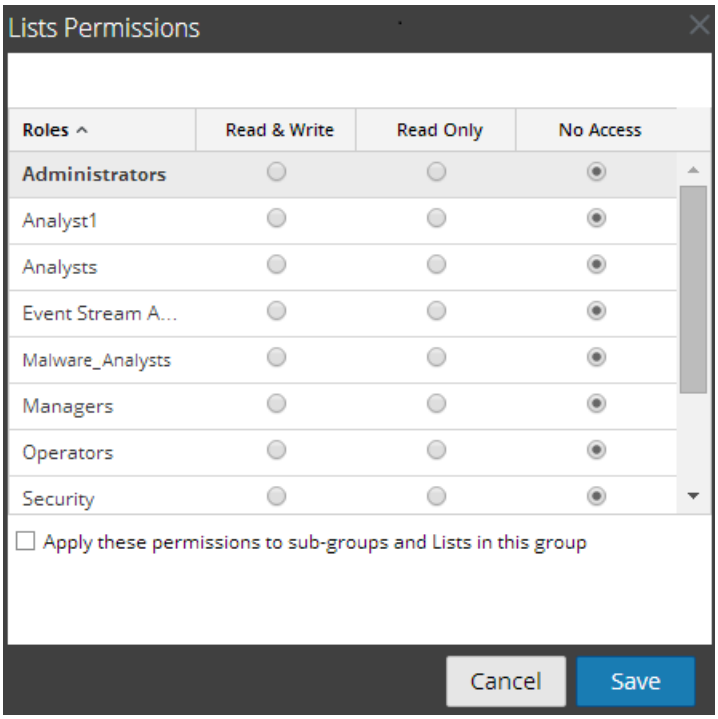
Suponga que desea que los **analistas de seguridad** tengan acceso a todas las listas de un grupo de listas. Para esto, puede configurar el permiso “**Lectura y escritura**” en el nivel del grupo de listas. Y si no desea que la función **Operador** tenga acceso a un conjunto específico de listas en un grupo de listas, puede configurar el permiso “**Sin acceso**” en el nivel del grupo de listas.

El permiso se configura solo para el grupo de listas, pero no para las listas ni los subgrupos del grupo de listas.

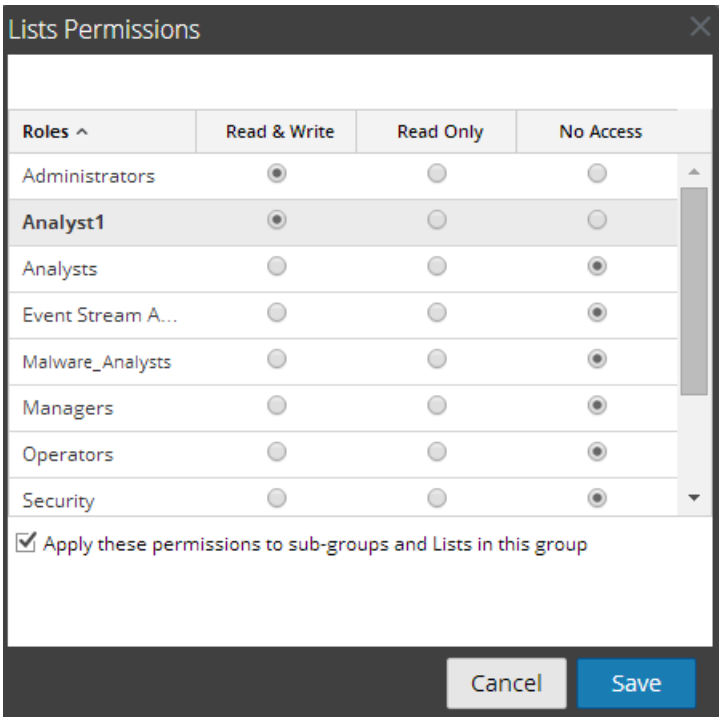
Control de acceso para un grupo de listas

Cuando desee cambiar los permisos del grupo de listas, debe seleccionar un grupo de listas y configurar sus permisos de acceso en el panel Permisos de listas.

Antes de aplicar permisos del grupo de listas, el permiso predeterminado configurado para todas las funciones de usuario es el permiso “Sin acceso” y las casillas de verificación están deseleccionadas, como se muestra en la figura.



Si desea cambiar el permiso de acceso para una función de usuario específica, debe configurarlo en el nivel del grupo de listas, como se muestra en la figura. Suponga que desea que los **administradores** tengan acceso a todas las listas de un grupo de listas. Para esto, puede configurar el permiso "**Lectura y escritura**" en el panel Permisos de grupo de listas.



También puede aplicar permisos a los subgrupos y a las listas del grupo si selecciona la casilla de verificación, como se muestra en la figura.

Los dos escenarios se explican de forma resumida:

- Escenario 1: Permisos aplicados a grupo de listas/subgrupo según la función de usuario.
- Escenario 2: Permisos aplicados a subgrupo y listas del grupo.

Función (analistas)	Permisos aplicados a grupo de listas/subgrupo según la función de usuario	Permisos aplicados a subgrupo y listas del grupo
Grupo	**Lectura y escritura**	**Lectura y escritura**
Subgrupo	**Lectura**	**Lectura y escritura: heredados**
Listas	**Lectura**	**Lectura y escritura: heredados**

Los permisos de acceso que configura se pueden aplicar a subgrupos y objetos secundarios de este grupo.

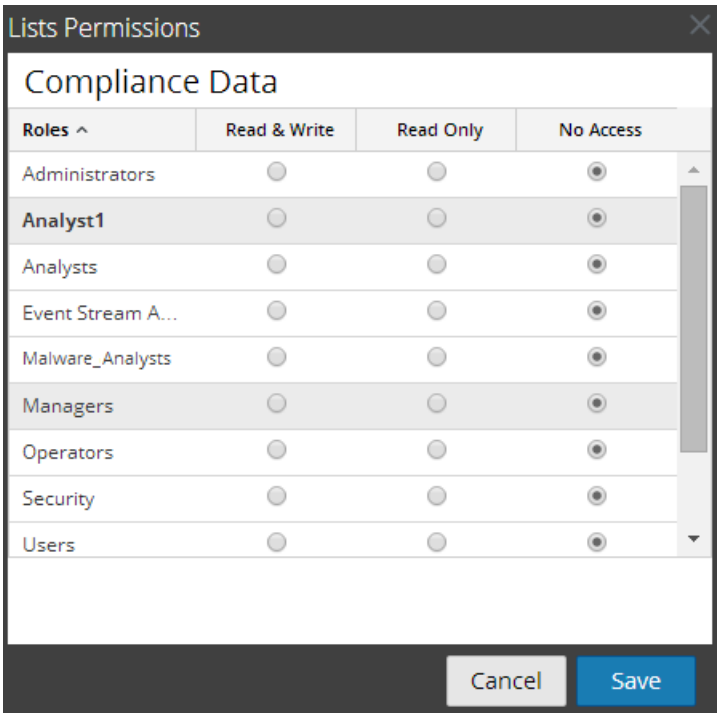
Al grupo de listas se asignará la función de un **analista de seguridad** y los permisos se configuran en **Lectura y escritura** para el grupo de listas.

En el escenario 1, cada uno de los niveles tendrá un permiso configurado de acuerdo con la función del usuario. En el escenario 2, el subgrupo y las listas del grupo heredarán el permiso en el nivel del grupo de listas.

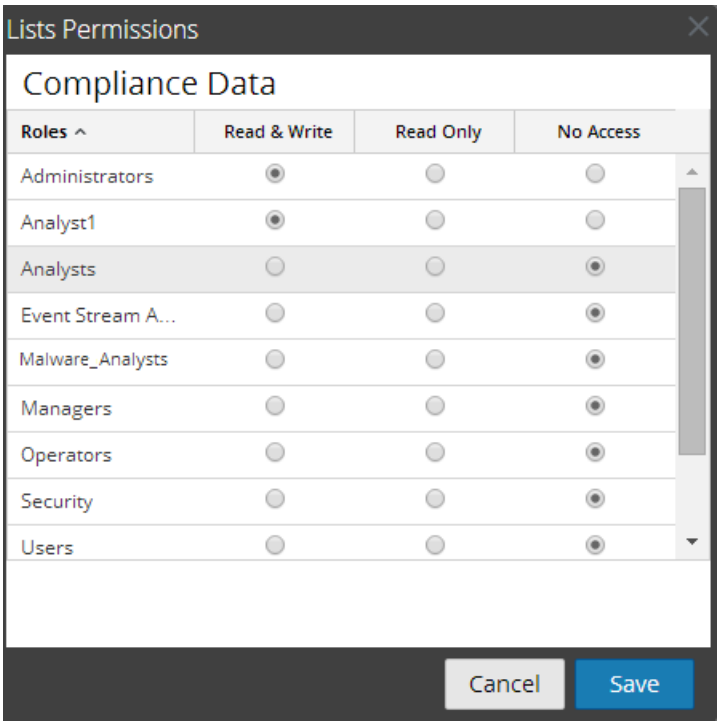
Control de acceso para una lista

Cuando desea cambiar los permisos de listas, debe seleccionar una lista y configurar sus permisos de acceso en el panel Permisos de listas.

Antes de aplicar permisos de listas, el permiso predeterminado configurado para todas las funciones de usuario es el permiso “Sin acceso” y la casilla de verificación está deseleccionada, como se muestra en la figura.



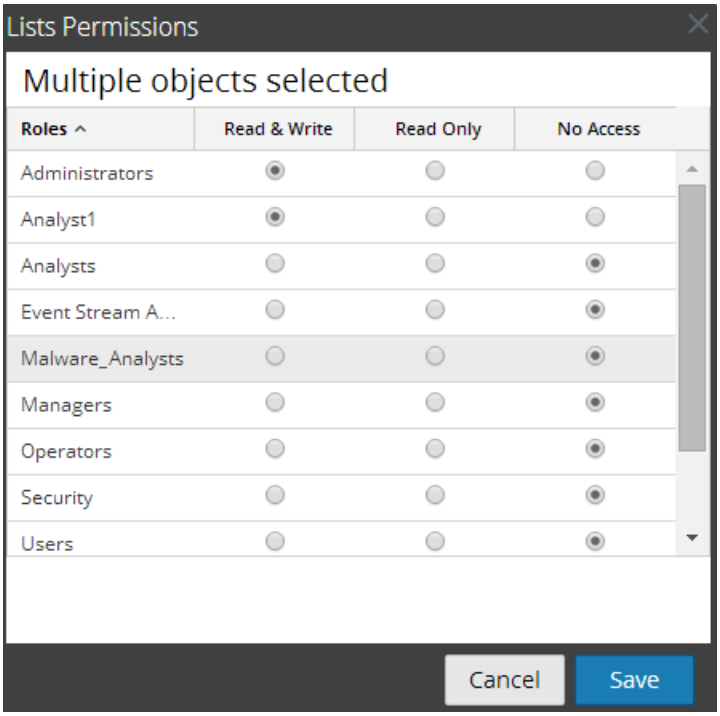
Si desea cambiar el permiso de acceso para una función de usuario específica, debe configurarlo en el nivel de lista, como se muestra en la figura. Suponga que desea que los **administradores** tengan acceso a una lista específica. Para esto, puede configurar el permiso "**Lectura y escritura**" en el panel Permisos de listas.



Control de acceso para una lista cuando se seleccionan múltiples listas

Cuando desea cambiar los permisos de múltiples listas, puede seleccionar simultáneamente varias listas y configurar sus permisos de acceso en el panel Permisos de listas. El permiso de acceso que elige se aplica a todas las listas seleccionadas.

Nota: El carácter "*" junto al nombre de función indica que hay otros permisos disponibles en la función de usuario. Si desea cambiar el permiso de acceso para la función de usuario requerida, seleccione la función de usuario y cambie el permiso de acceso.



Nota: Si un usuario (distinto del administrador) crea una lista, el administrador no puede acceder a ella.

Lista tabular

En la siguiente tabla se indican las diversas columnas del panel Permisos de listas:

Columna	Descripción
Funciones	La función del usuario que inició sesión en la interfaz del usuario de Security Analytics.
Lectura y escritura	El usuario puede acceder, ver, editar, eliminar, importar y exportar listas en la vista Listas. El usuario también puede cambiar el permiso en la regla.

Columna	Descripción
Solo lectura	El usuario solo puede acceder a la lista y verla en la vista Listas
Sin acceso	El usuario no puede acceder a una lista ni verla cuando tiene configurado este permiso.

Temas

- Establecer el control de acceso para una lista
- Establecer el control de acceso para grupos de listas

Establecer el control de acceso para una lista

En este tema se proporcionan instrucciones para establecer permisos para una lista. Puede establecer permisos de lista desde el panel Lista. En el nivel de la lista, puede establecer los siguientes permisos de acceso para las funciones de usuario en Security Analytics:

- Lectura y escritura: Ver o editar la lista.
- Solo lectura: ver la lista.
- Sin acceso: la lista no se puede ver ni editar.

Requisitos previos

Asegúrese de:

- Haber comprendido los componentes de la vista Lista. Para obtener más información, consulte Vista de lista.
- Tener un permiso de acceso de “Lectura y escritura” mínimo para establecer permisos de acceso para una lista.

Procedimiento

Realice los siguientes pasos para establecer el control de acceso para una lista:

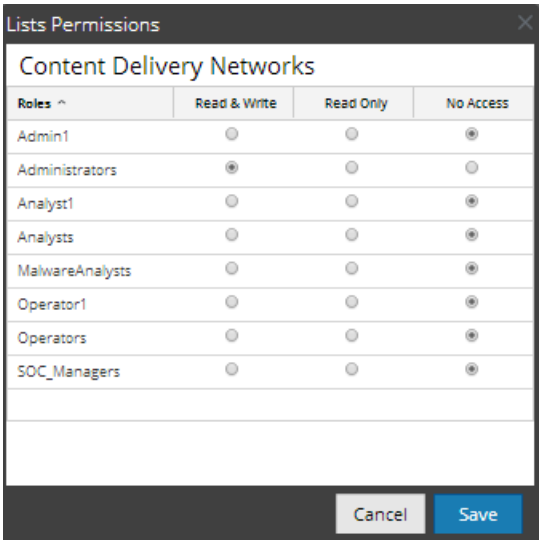
1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.

   Se muestra la pestaña Administrar.
2. Haga clic en **Listas**.

   Se muestra la vista Lista.
3. En la **Vista de lista**, seleccione una lista.

4. Haga clic en  > **Permisos** en la barra de herramientas Lista.

   Aparece el cuadro de diálogo Permisos de listas.



5. Seleccione el permiso de acceso apropiado para cada una de las funciones de usuario y haga clic en **Guardar**.

   Se muestra un mensaje de confirmación que indica que el permiso se estableció correctamente para la lista seleccionada.

Establecer el control de acceso para grupos de listas

En este tema se proporcionan instrucciones para establecer permisos para grupos de listas. Puede establecer permisos de grupos de listas desde el panel Grupos de listas. En el nivel de grupo de listas, puede establecer los siguientes permisos de acceso para las funciones de usuario en Security Analytics:

- Lectura y escritura: Ver o editar el grupo de listas.
- Solo lectura: ver el grupo de listas.
- Sin acceso: el grupo de listas no se puede ver ni editar.

Requisitos previos

Asegúrese de:

- Haber comprendido los componentes de la vista Lista. Para obtener más información, consulte Vista de lista.
- Tener un permiso de acceso de “Lectura y escritura” mínimo para establecer permisos de acceso para un grupo de listas.

Procedimiento

Realice los siguientes pasos para establecer el control de acceso para un grupo de listas:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.

   Se muestra la pestaña Administrar.

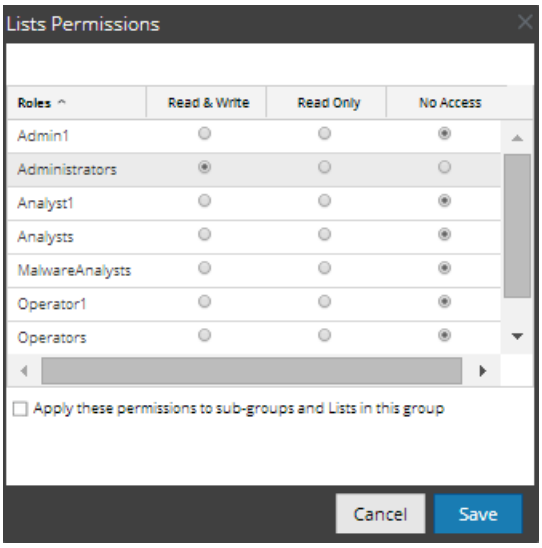
2. Haga clic en **Listas**.

   Se muestra la vista Lista.

3. En el panel **Grupos de listas**, seleccione un grupo de listas.

4. Haga clic en  > **Permisos**.

   Aparece el cuadro de diálogo Permisos de listas.



5. (Opcional) Seleccione la casilla de verificación correspondiente para aplicar estos permisos a subgrupos y objetos secundarios de este grupo.

6. Haga clic en **Guardar**.

   Se muestra un mensaje de confirmación que indica que el permiso se estableció correctamente para el grupo de listas seleccionado.

Referencias del módulo Reporting

En este tema se describen las características y las funciones de la interfaz del usuario de Reporting en Security Analytics. Las referencias se agrupan por la ubicación en la interfaz de usuario: Alerta, gráfico, lista, informe y regla.

Temas

- Referencias de alertas
  - Cuadro de diálogo Permisos de alerta
  - Vista Alerta
  - Vista Crear o modificar alerta
  - Cuadro de diálogo Importar alerta
  - Referencias de plantillas
    - Cuadro de diálogo Crear/modificar plantilla
    - Barra de herramientas de Plantilla
  - Panel Ver alertas
  - Vista Ver calendario de alertas
- Referencias de gráficos
  - Vista Crear gráfico
  - Cuadro de diálogo Permisos de gráficos
  - Vista Gráfico
  - Cuadro de diálogo Importar gráfico
  - Vista Probar un gráfico
  - Panel Ver un gráfico
- Referencias de listas
  - Vista Crear lista
  - Cuadro de diálogo Permisos de listas
  - Vista de lista
- Referencias de informes

- Vista Crear informe
- Cuadro de diálogo Importar informe
- Cuadro de diálogo Permisos de informes
- Vista Informe
- Referencias de calendarios
  - Características
  - Características
  - Características
  - Características
  - Características
- Cuadro de diálogo Seleccionar un logotipo
- Panel Ver todos los informes
- Panel Ver un informe

- Referencias de reglas
  - Vista Crear regla
  - Agregados de consulta
  - Cuadro de diálogo Permisos de regla
  - Vista Regla
  - Especificación de orígenes de eventos de IPDB
  - Modos de definición de reglas de la base de datos de Warehouse
    - Sintaxis general de una regla avanzada
    - Informe Todas las categorías de eventos

Referencias de alertas

La interfaz del usuario del módulo Reporting proporciona acceso a alertas de Security Analytics. Este tema contiene descripciones de la interfaz del usuario, así como otra información de referencia para ayudar a los usuarios a administrar las alertas.

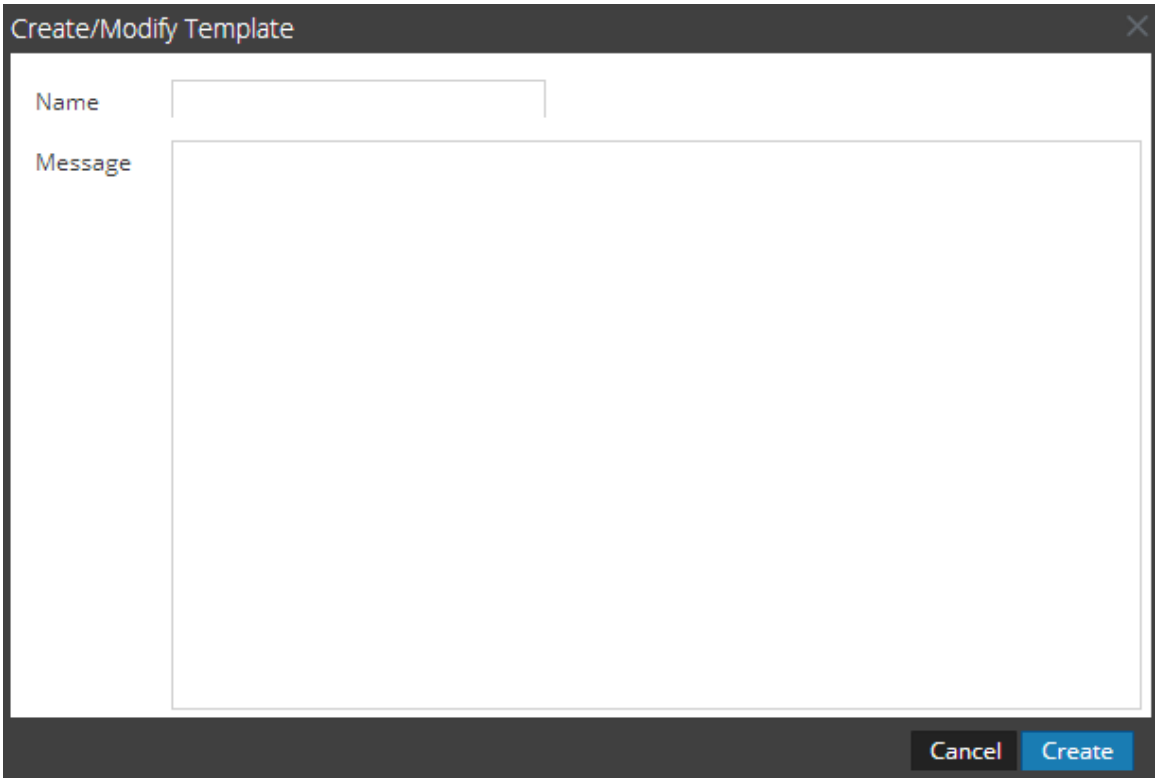
Temas

- Cuadro de diálogo Permisos de alerta
- Vista Alerta
- Vista Crear o modificar alerta
- Cuadro de diálogo Importar alerta
- Referencias de plantillas
  - Cuadro de diálogo Crear/modificar plantilla
  - Barra de herramientas de Plantilla
- Panel Ver alertas
- Vista Ver calendario de alertas

Cuadro de diálogo Crear/modificar plantilla

En este tema se describen las funciones del cuadro de diálogo Crear/modificar plantilla. El cuadro de diálogo Crear/modificar plantilla permite personalizar plantillas de alerta para su uso en la creación de alertas. Los procedimientos asociados con este cuadro de diálogo se describen en Definir plantillas de alertas.

La siguiente figura es un ejemplo del cuadro de diálogo Crear/modificar plantilla.



En la siguiente tabla se describen los campos del cuadro de diálogo Crear/modificar plantilla.

Característica	Descripción
Nombre	Indica el nombre de la plantilla para las alertas de Reporting. Por ejemplo, IP de origen.
Mensaje	Especifica el mensaje que se enviará cuando se activa una alerta.
Crear	Crea la plantilla con un mensaje de confirmación y queda disponible para su uso en Reporting de inmediato.
Guardar	Guarda la plantilla con los detalles editados o cuando se crea una nueva plantilla. Este botón es visible solo en el modo de edición.
Cancelar	Cuando hace clic en Cancelar se cierra el cuadro de diálogo sin guardar la plantilla ni los cambios realizados en ella.

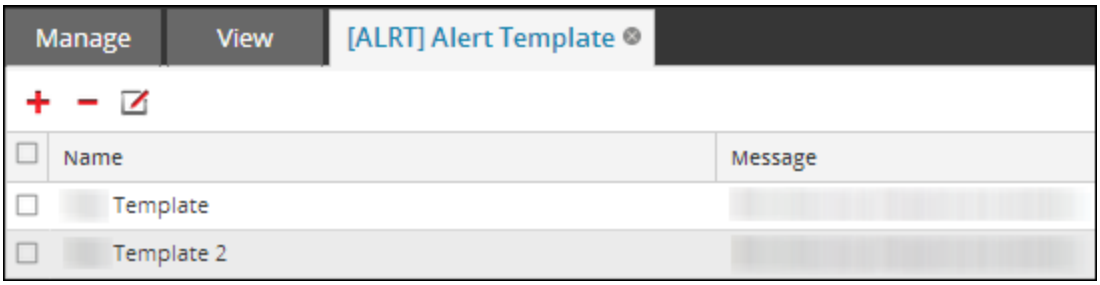
Vista Plantilla

En este tema se describen las funciones de la vista Plantilla. La vista Plantilla permite agregar, ver y eliminar plantillas de alertas. Los procedimientos asociados se proporcionan en Definir plantillas de alertas.

Para acceder a la vista Plantilla:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes.**
   Se muestra la pestaña Administrar.
2. Haga clic en **Alertas**.
   Se muestra la vista Alerta.
3. Haga clic en Template.

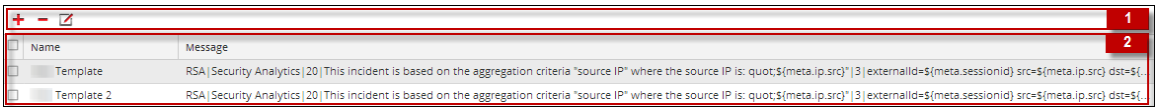
La siguiente figura es un ejemplo de la vista Plantilla.



La vista Plantilla incluye los siguientes paneles:

- Barra de herramientas de Plantilla
- Panel de lista de plantillas

En la siguiente figura se muestran los diferentes paneles de la vista Plantilla de alertas.



Barra de herramientas de Plantilla

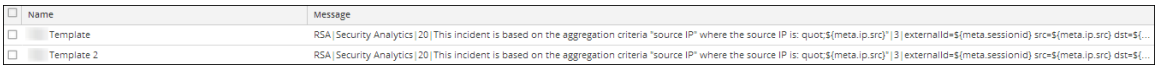
La barra de herramientas de Plantilla permite agregar, modificar y eliminar plantillas de alertas. Una vez que se definen las plantillas, puede seleccionar una plantilla para simplificar la definición y la modificación de los mensajes de alerta.

En la siguiente tabla se indican las diversas acciones de la vista Plantilla y su descripción.

Acciones	Descripción
+	Esta opción le permite crear una nueva plantilla de alerta.
−	Esta opción elimina la plantilla de alerta seleccionada.
	Esta opción le permite editar una plantilla de alerta existente.

Lista de plantillas

La Lista de plantillas presenta todas las plantillas en formato tabular.



En la siguiente tabla se describen las columnas del panel Lista de plantillas.

Columna	Descripción
Nombre	Este es el nombre de la plantilla.
Mensaje	Este es el mensaje de alerta definido para la plantilla.

Cuadro de diálogo Permisos de alerta

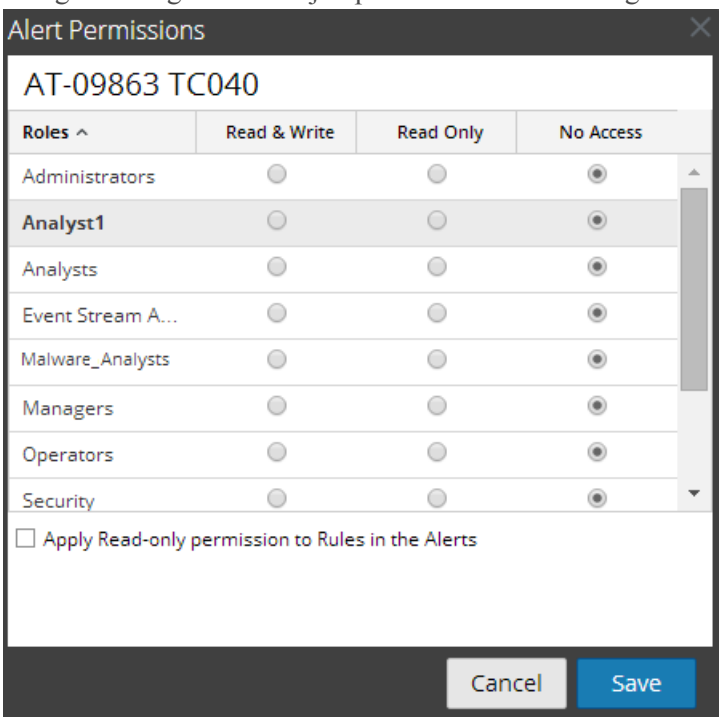
En este tema se describen las funciones del cuadro de diálogo Permisos de alerta y los permisos de acceso que puede tener el usuario de acuerdo con la función de usuario para administrar una alerta. Los usuarios que tienen permiso de acceso de “Lectura y escritura” para configurar permisos de acceso para una alerta pueden configurar los permisos en el cuadro de diálogo Permisos de alerta.

Los procedimientos relacionados con este cuadro de diálogo se describen en Administrar el acceso para una alerta.

Para acceder al cuadro de diálogo:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Alertas**.
   Se muestra la vista Alertas.
3. En el panel **Lista de alertas**, seleccione un informe.
4. Haga clic en > **Permisos**.
   Se muestra el cuadro de diálogo Permisos de alerta.

La siguiente figura es un ejemplo del cuadro de diálogo Permisos de alerta.



En la siguiente tabla se describen las funciones del cuadro de diálogo Permisos de alerta.

Característica	Descripción
Funciones	La función del usuario que inició sesión en la interfaz del usuario de Security Analytics.

Característica	Descripción
Lectura y escritura	El usuario puede acceder, ver, editar, importar, exportar y eliminar la alerta en la página Alertas. El usuario también puede cambiar el permiso en la alerta.
De solo lectura	El usuario solo puede acceder a la alerta y verla en la vista Alertas.
Sin acceso	El usuario no puede acceder a una alerta ni verla cuando tiene configurado este permiso.
Aplicar permisos de solo lectura a las reglas de las alertas	Seleccione la casilla de verificación para aplicar permisos a las reglas de las alertas de forma automática.
Cancelar	Esta opción cancela todos los cambios realizados a los permisos.
Guardar	Esta opción guarda las selecciones y proporciona acceso a las funciones de acuerdo con las selecciones.

Vista Alerta

La vista Alerta permite importar, exportar, administrar y agregar alertas. Los procedimientos relacionados con esta vista se proporcionan en Trabajar con alertas en el módulo Reporting

En esta barra de herramientas puede realizar las siguientes acciones:

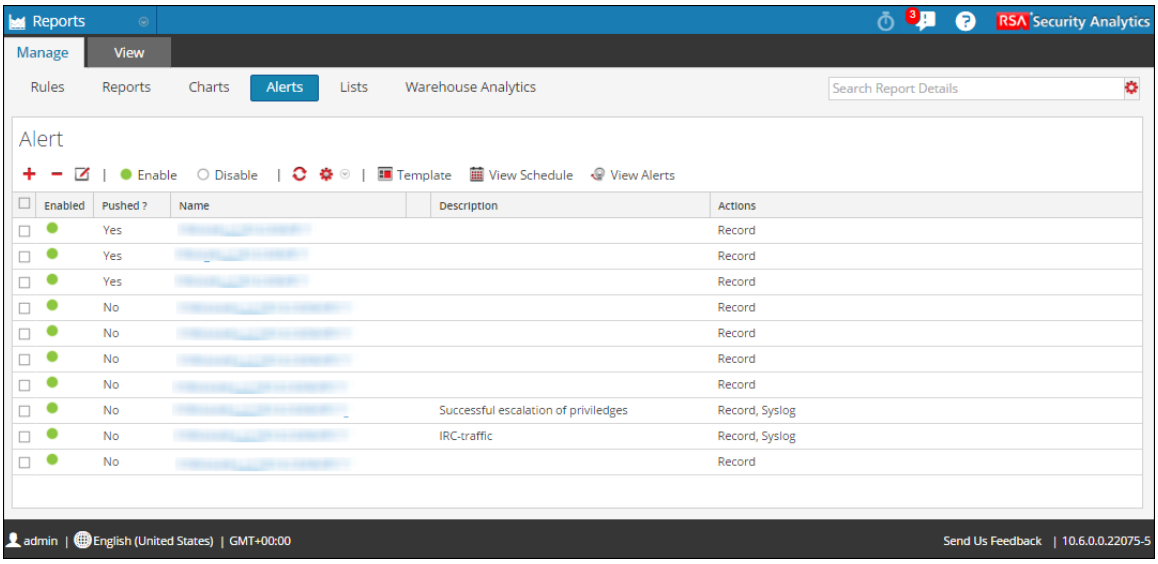
- Agregar una alerta.
- Editar una alerta.
- Eliminar una alerta.
- Activar una alerta.
- Desactivar una alerta.
- Actualizar una lista de alertas.
- Importar una alerta.
- Exportar una alerta.
- Establecer permisos de acceso para la alerta.

- Ver todas las plantillas.
- Ver calendario de alertas.
- Ver una lista de alertas.

Para acceder a la vista Alerta:

1. En el menú de **Security Analytics**, haga clic en **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Alertas**.
   Se muestra la vista Alerta.

En la siguiente figura se muestran los diferentes paneles de la vista Alerta.



La vista Alerta incluye las siguientes funciones:

- Barra de herramientas Alerta
- Panel de lista de alertas

Barra de herramientas Alerta

La barra de herramientas Alerta permite agregar, modificar, eliminar, habilitar, inhabilitar, actualizar, importar y exportar una alerta. Con esta barra de herramientas, también puede establecer permisos de acceso para la alerta seleccionada.

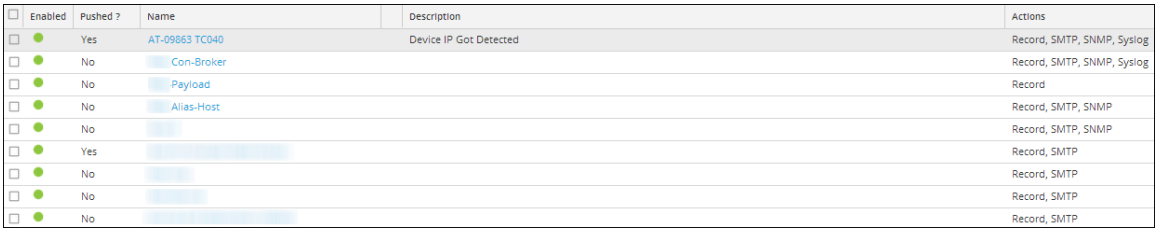
En la siguiente tabla se describen las funciones de la barra de herramientas Alerta.

Característica	Descripción
	Esta opción le permite agregar una nueva alerta al módulo Reporting.
	Esta opción le permite eliminar uno o más alertas seleccionadas.
	Esta opción le permite editar una alerta.
Activar	Esta opción habilita las alertas seleccionadas.
Desactivar	Esta opción deshabilita las alertas seleccionadas.
	Esta opción actualiza la vista.
	El menú Acciones tiene las siguientes opciones: Importar, exportar y permisos.

Panel de lista de alertas

El panel de lista de alertas enumera todas las alertas en formato tabular. En la siguiente tabla se indican las diversas columnas del panel de lista de alertas y su descripción.

Este es un ejemplo del panel de lista de alertas.



Enabled	Pushed ?	Name	Description	Actions
	Yes	AT-09863 TC040	Device IP Got Detected	Record, SMTP, SNMP, Syslog
	No	Con-Broker		Record, SMTP, SNMP, Syslog
	No	Payload		Record
	No	Alias-Host		Record, SMTP, SNMP
	No			Record, SMTP, SNMP
	Yes			Record, SMTP
	No			Record, SMTP
	No			Record, SMTP
	No			Record, SMTP

En la siguiente tabla se describen las funciones del panel Listas de alertas.

Característica	Descripción
Activado	Muestra el estado de la alerta: • Activada: la alerta está activa y se inicia según las reglas que se le asignaron. • Desactivada: la alerta no está activa.

Característica	Descripción
¿Migrado?	Indica si la alerta se envía a Decoders o Log Decoders: • Sí: la alerta se envía a Decoders o Log Decoders. • No: la alerta no se envía a Decoders o Log Decoders.
Nombre	Identifica el nombre de la alerta. Si hace clic en el nombre de una alerta, se muestra la regla en la cual se basa esta alerta en el panel Definir reglas.
Descripción	Indica la descripción de la alerta.
Acciones	Indica la acción que implementa el sistema cuando se activa la alerta. Los diversos tipos de acciones disponibles son: • Registro • SMTP • SNMP • Syslog

Vista Crear o modificar alerta

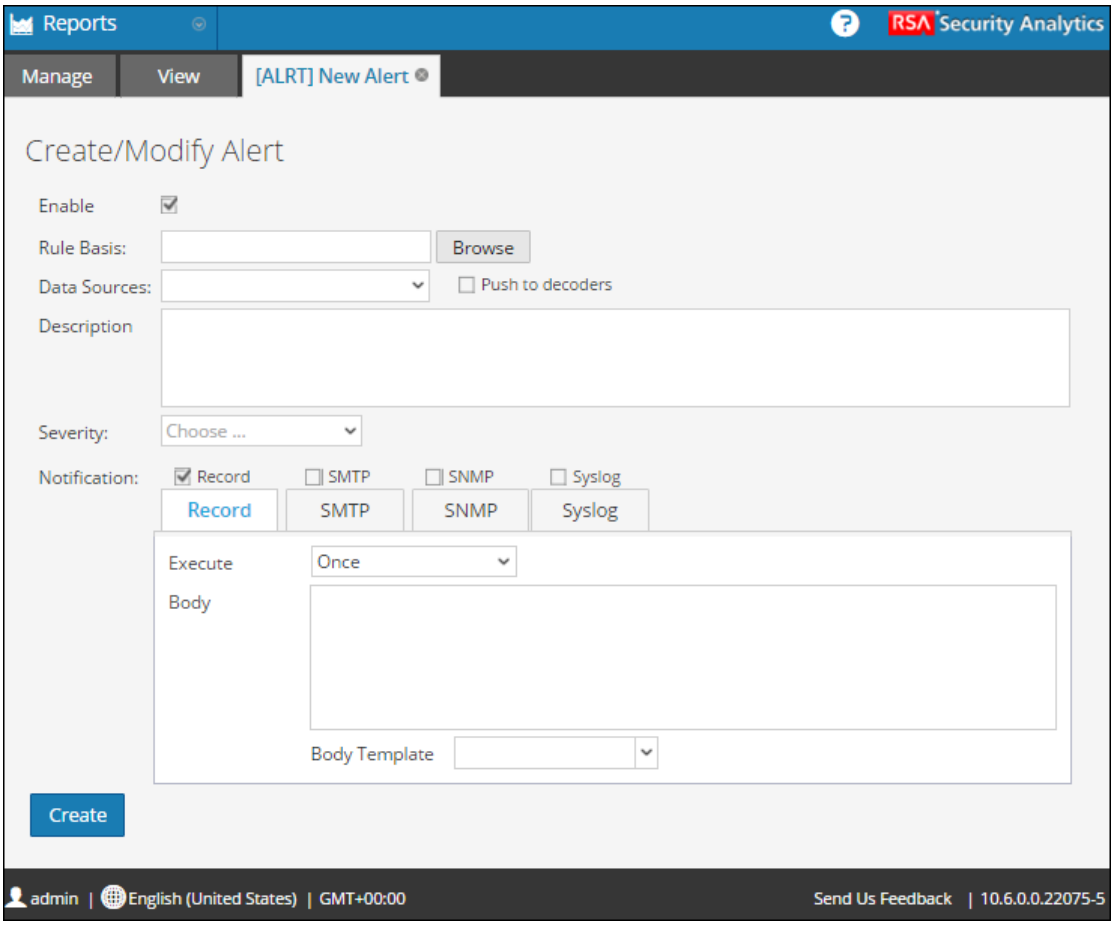
La vista Crear/modificar alerta permite agregar, administrar y editar alertas. En Trabajar con alertas en el módulo Reporting se proporcionan procedimientos relacionados.

Para acceder a la vista Crear/modificar alerta:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Alertas**.
   Se muestra la vista Alerta.

3. En la barra de herramientas **Alerta**, haga clic en +.

   La siguiente figura es un ejemplo de la vista Crear/modificar alerta.

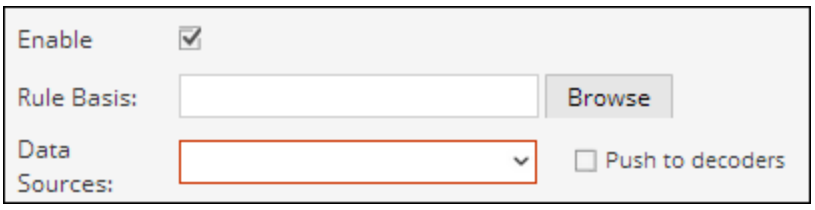


En la vista Crear/modificar alerta se incluyen las siguientes secciones:

- Sección Definición de alerta
- Sección Descripción de alerta
- Sección Notificación de alerta

Sección Definición de alerta

La sección Definición de alerta permite seleccionar una regla y orígenes de datos de alerta, enviar el evento al Decoder o al Log Decoder y habilitar o deshabilitar la alerta.



En la tabla siguiente se describen los campos de la sección Definición de alerta:

Campo	Descripción
Habilitar	• **Activar** activa la alerta. La alerta ejecuta y envía acciones de salida a cada minuto (de forma predeterminada) cuando se cumplen las condiciones de la alerta. • **Desactivar** desactiva la alerta. La alerta no se ejecuta y no envía acciones de salida.
Base de la regla	Si hace clic en el botón Navegar, se muestra el panel Biblioteca de reglas en el cual se selecciona la regla que es la base de esta alerta. Debe seleccionar una regla que tenga una cláusula where única para una alerta.
Orígenes de datos	Especifica el origen de datos de una alerta.
Migrar a deco-dificadores	Seleccione esta opción para enviar la cláusula “where” de la regla de alerta a los Decoders conectados al origen de datos de NWDB seleccionado. Esta es la opción recomendada para crear una alerta RE, ya que las condiciones de alerta se comprueban en el Decoder y las consultas de alerta serán comparativamente más rápidas en NWDB. Si deselecciona esta opción, la cláusula “where” de la regla de alerta se consultará contra el origen de datos de NWDB seleccionado. Sobre la base de la complejidad y los metadatos en la cláusula “where” de la regla, podría ser más lento procesar las consultas en NWDB. **Nota:** Security Analytics no envía reglas al Decoder de forma automática.

Sección Notificación de alerta

La sección Notificación de alerta permite definir la acción de notificación que realiza Security Analytics cuando se activa la alerta, es decir, la alerta se registra o se envía mediante una de las acciones de salida definidas. Las acciones de salida son Protocolo simple de transferencia de correo (SMTP), Protocolo simple de administración de redes (SNMP) o mensaje de syslog.

Cuando crea una alerta, la sección Notificación incluye la pestaña Registro de manera predeterminada. El ícono junto a la pestaña Registro permite seleccionar el tipo de notificación de la lista desplegable para la salida que se desea especificar para esta alerta: SMTP, SNMP o syslog.

Según el tipo de notificación seleccionado, la sección Notificación se completa con texto predefinido que tiene ciertas variables que agregarán metadatos apropiados a la alerta. En Reporting Engine, estas variables se reemplazan por valores reales. La siguiente tabla enumera las variables y su descripción.

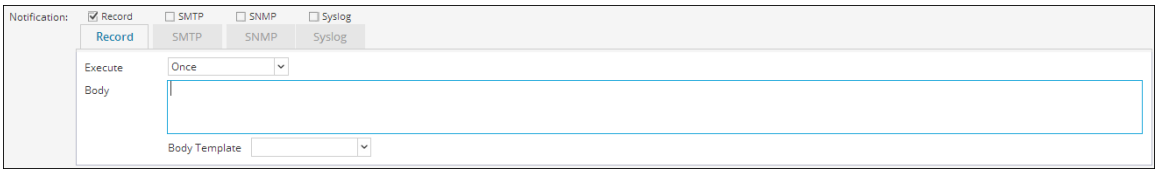
Variable	Descripción
`${me-ta.<metakey>}`	El valor de clave de metadatos. **Nota:** Si <metakey> no recuperó ningún valor, se imprime una cadena vacía (“”).
`${meta.time}` / `${me-ta.time:<time_format>}`	`${meta.time}`: La hora de la sesión se imprime en formato “aaaa-MMM-dd HH:mm:ss”. `${meta.time:<time_format>}` : La hora de la sesión se imprime en el formato de hora personalizado que proporcionó el usuario. Por ejemplo, `${meta.time:dd-MM-yyyy HH:-mm:ss}`. Para obtener más información sobre los formatos de hora compatibles, consulte http://-docs.o-racle.com/javase/7/docs/api/java/text/SimpleDateFormat.html **Nota:** Si el formato de hora proporcionado por el usuario no es válido, se utilizará el formato de hora predeterminado. El formato de hora predeterminado es “aaaa-MMM-dd HH:mm:ss”.
`${name}`	El nombre de alerta definido en Reporting Engine.
`${count}`	La cantidad de veces que se detecta una alerta en un marco de tiempo determinado. (De manera predeterminada, es un minuto)
`${sa.host}`	El nombre de host de Security Analytics como está configurado en Reporting Engine.
`${device.id}`	El ID de dispositivo de Security Analytics del origen de datos.

La sección Notificación de alerta tiene cuatro pestañas:

- **Registro**
- **SMTP**
- **SNMP**
- **Syslog**

Pestaña Registro

La pestaña Registro permite definir la frecuencia de registro de una alerta y el mensaje que se desea generar cuando se activa la alerta.

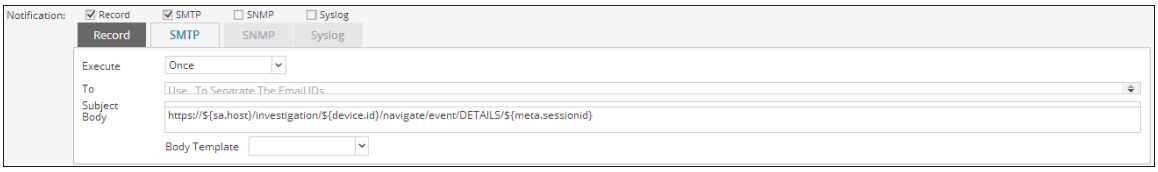


En la siguiente tabla se indican los diversos campos de la pestaña Registro y su descripción.

Campo	Descripción
Ejecutar	Indica la frecuencia para registrar una alerta. • **Una vez**: Registra la alerta solo una vez en función del intervalo de la alerta sin importar la frecuencia con que se active la alerta. Security Analytics registra la cantidad de veces que la alerta se activó realmente durante ese intervalo en el archivo de registro, de forma que los analistas sepan cuántas veces la alerta registró una coincidencia en un día determinado. • **Cada evento:** registra la alerta cada vez que se activa. Si una alerta se activa un número ilimitado de veces durante un día, se trata a menudo como ruido y se puede omitir, salvo en caso de alertas que requieren un monitoreo continuo, como los cambios de configuración de red y los ataques DDoS. **Nota:** Seleccione la configuración **Cada evento** en la lista desplegable Ejecutar para las acciones de salida de SNMP y syslog.
Cuerpo	Indica el cuerpo del mensaje.
Plantilla de cuerpo	(Opcional) Si se han definido plantillas, puede seleccionar una plantilla para el mensaje de la alerta.

Pestaña SMTP

La pestaña SMTP le permite definir la salida SMTP (correo electrónico) de esta alerta.



En la siguiente tabla se indican los diversos campos de la pestaña SMTP y su descripción.

Campo	Descripción
Ejecutar	Indica la cantidad de veces que desea enviar un correo electrónico de la alerta. • **Una vez** : se envía solo un correo electrónico por intervalo, si la alerta se activa en ese intervalo, independientemente de cuántas alertas se activan. • **Cada evento**: se envía un correo electrónico con la alerta por cada evento en el cual se cumplen los criterios de la regla.
Para	Identifica la dirección de correo electrónico o una lista de direcciones de correo electrónico separadas por comas a las cuales desea enviar esta alerta.
Asunto	Indica el asunto del mensaje de correo electrónico.
Cuerpo	Indica el cuerpo del mensaje.
Plantilla de cuerpo	(Opcional) Si se definieron plantillas, seleccione una para el mensaje de SMTP, la cual puede utilizar tal como está o modificar.

Pestaña SNMP

La pestaña SNMP le permite definir la salida SNMP de la alerta.

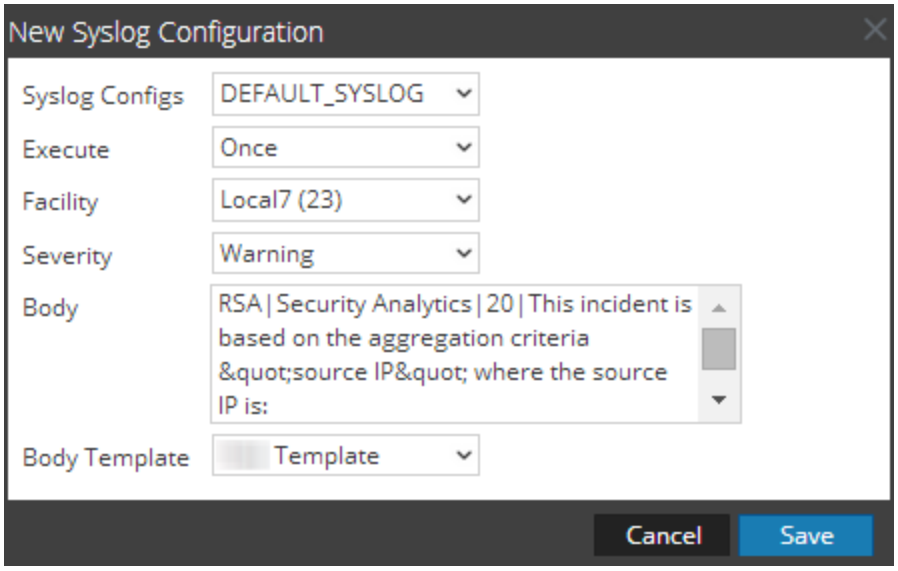
En la siguiente tabla se indican los diversos campos de la pestaña SNMP y su descripción.

Campo	Descripción
Ejecutar	Indica la cantidad de veces que desea enviar una salida SNMP de la alerta. • **Una vez**: se envía un mensaje SNMP junto con un correo electrónico por intervalo, si la alerta se activa en ese intervalo, independientemente de cuántas alertas se activan. • **Cada evento**: se envía un mensaje SNMP con la alerta por cada evento en el cual se cumplen los criterios de la regla.
Cuerpo	Indica el cuerpo del mensaje.
Plantilla de cuerpo	(Opcional) Si se definieron plantillas, seleccione una para el mensaje de SNMP, la cual puede utilizar tal como está o modificar.

Pestaña Syslog

La pestaña Syslog le permite definir la salida de mensaje syslog de esta alerta.

Haga clic en + para agregar la configuración de syslog a una alerta. Aparece el cuadro de diálogo Nueva configuración de syslog:



En la siguiente tabla se describen los campos del cuadro de diálogo Nueva configuración de syslog:

Campo	Descripción
Configuraciones de syslog	Indica la configuración de syslog definida en el panel Configuración de syslog de la vista Configuración de dispositivo.
Ejecutar	Indica la cantidad de veces que desea enviar una salida de syslog de la alerta. • **Una vez**: se envía una salida de syslog junto con un correo electrónico por intervalo, si la alerta se activa en ese intervalo, independientemente de cuántas alertas se activan. • **Cada evento**: se envía una salida de syslog con la alerta por cada evento en el cual se cumplen los criterios de la regla.
Funcionalidad	Indica el tipo de programa que registra el mensaje. Varios ejemplos del tipo de programa: syslog, demonio, correo, kernel.

Campo	Descripción
Gravedad	Indica el nivel de gravedad de la alerta activada. • Emergencia • Alerta • Critical • Error • Advertencia • Aviso • Creación de informes • Depurar
Cuerpo	Indica el cuerpo del mensaje.
Plantilla de cuerpo	(Opcional) Si se definieron plantillas, seleccione una para el mensaje de syslog, la cual puede utilizar tal como está o modificar.

Sección Descripción de alerta

La sección Descripción de alerta permite proporcionar una descripción de la alerta.

E la tabla siguiente se describen los campos de la sección Descripción de alerta.

Campo	Descripción
Descripción	Identifica la descripción de la alerta.
Crear	Crea una alerta. (Se muestra esta opción cuando se crea una alerta.)
Guardar	Guarda los cambios realizados a la alerta. (Se muestra esta opción cuando se modifica una alerta.)

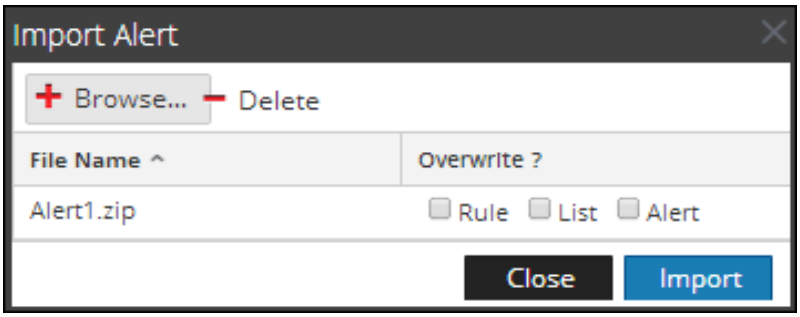
Cuadro de diálogo Importar alerta

En el cuadro de diálogo Importar alerta, puede importar un archivo de alertas y especificar si las reglas, las listas y las alertas existentes se sobrescribirán. Los procedimientos asociados se proporcionan en Definir alertas

Para acceder al cuadro de diálogo:

1. En el menú de **Security Analytics**, haga clic en **Administration** > Informes.
   Se muestra la pestaña Administrar.
2. Haga clic en Alertas.
   Se muestra la vista Alerta.
3. En el panel **Alerta**, seleccione una carpeta para importar el archivo.
4. En la barra de herramientas **Alerta**, haga clic en > Importar para importar una alerta.

La siguiente figura es un ejemplo del cuadro de diálogo Importar informe.



En la siguiente tabla se indican las diversas acciones del cuadro de diálogo Importar alerta y su descripción.

Acciones	Descripción
Browse...	Esta opción muestra una vista del sistema de archivos zip local para que pueda seleccionar la alerta que desea importar.
−	Elimina la alerta seleccionada del cuadro de diálogo Importar alerta.
Nombre de archivo	Indica el nombre del archivo binario importado.

Acciones	Descripción
¿Sobrescribir?	Le permite seleccionar la opción para sobrescribir una versión existente de la alerta que se va a importar. Si no selecciona la opción de sobrescritura, se importa un archivo duplicado y no se muestra ningún mensaje de error.
Cerrar	Cierra el cuadro de diálogo Importar alerta.
Importar	Importa la alerta con un mensaje de confirmación.

Referencias de plantillas

La interfaz del usuario del módulo Reporting proporciona acceso a las plantillas de alerta de Security Analytics. Este tema contiene descripciones de la interfaz del usuario, además de otra información de referencia, para ayudar a los usuarios a administrar las Plantillas de alerta.

Temas

- Cuadro de diálogo Crear/modificar plantilla
- Barra de herramientas de Plantilla

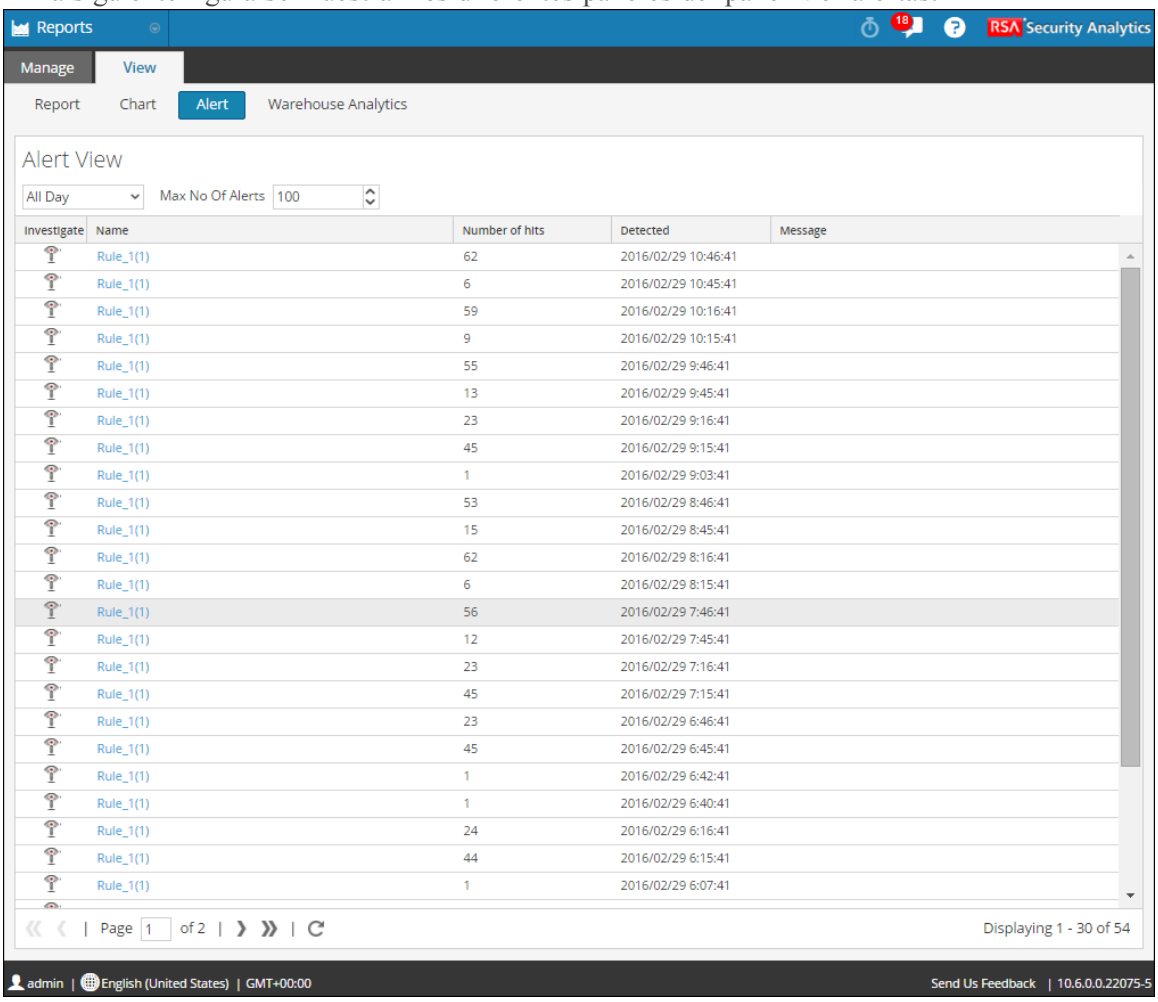
Panel Ver alertas

En este tema se describen las funciones del panel Ver alertas. El panel Ver alertas permite ver las alertas activadas por el módulo Reporting e investigar cualquier alerta del módulo Investigation. Solo sus alertas (es decir, las alertas que tiene permitido ver) se enumeran en una tabla. Puede personalizar la vista para mostrar las alertas de un período de tiempo específico y configurar la cantidad máxima de alertas que se muestran en una sola página. Los procedimientos asociados con este panel se proporcionan en Ver una lista de alertas

Para acceder al cuadro de diálogo:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Alerta**.
   Se muestra la vista Alerta.
3. Haga clic en View Alerts.

En la siguiente figura se muestran los diferentes paneles del panel Ver alertas.



Características

El panel Ver alertas incluye las siguientes funciones:

- Barra de herramientas de Ver alertas
- Lista Ver alertas

Barra de herramientas de Ver alertas

La barra de herramientas de Ver alertas permite filtrar alertas de acuerdo con un conteo o con la fecha de inicio y finalización de las alertas.
En la siguiente tabla se indican las operaciones de la barra de herramientas de Ver alertas.

Opción	Descripción
Datos de las últimas horas	Los datos obtenidos en la ejecución anterior.
Número máximo de alertas	La cantidad máxima de alertas que desea mostrar en una página.

Lista Ver alertas

En la lista Ver alertas se muestran todas las alertas filtradas en formato tabular. En la siguiente tabla se indican las columnas del panel de lista Ver alertas.

Columna	Descripción
	Investiga la alerta. Si hace clic en el botón, se abre el módulo Investigation, donde se muestran los detalles de la primera sesión que registró la coincidencia de la alerta específica para análisis inmediato. **Nota:** No se le redirige al módulo Investigation cuando: -Vuelve a configurar un origen de datos para una alerta existente y ejecuta una alerta en el nuevo origen de datos. -Ingresa un nombre de host en lugar de una dirección IP en el campo de origen de datos.
Nombre	Indica el nombre de la alerta que registró la coincidencia. El hipervínculo en el nombre abre el módulo Investigation para ver todas las coincidencias de esa alerta específica correspondientes a la hora aproximada de la alerta registrada.
Número de coincidencias	Indica la cantidad de veces que se activa la alerta.
Detected	Indica la fecha y la hora en las cuales se activó la alerta.
Mensaje	Indica el mensaje de alerta.

Vista Ver calendario de alertas

En la vista Ver calendario de alertas, puede ver la siguiente información acerca de cada una de las alertas calendarizadas.

- Estado de finalización, nombre, hora de la última ejecución, ID de la última sesión, total de alertas activadas.
- Estadística del tiempo necesario para ejecutar la alerta calendarizada: duración, promedio de duración, duración máxima.

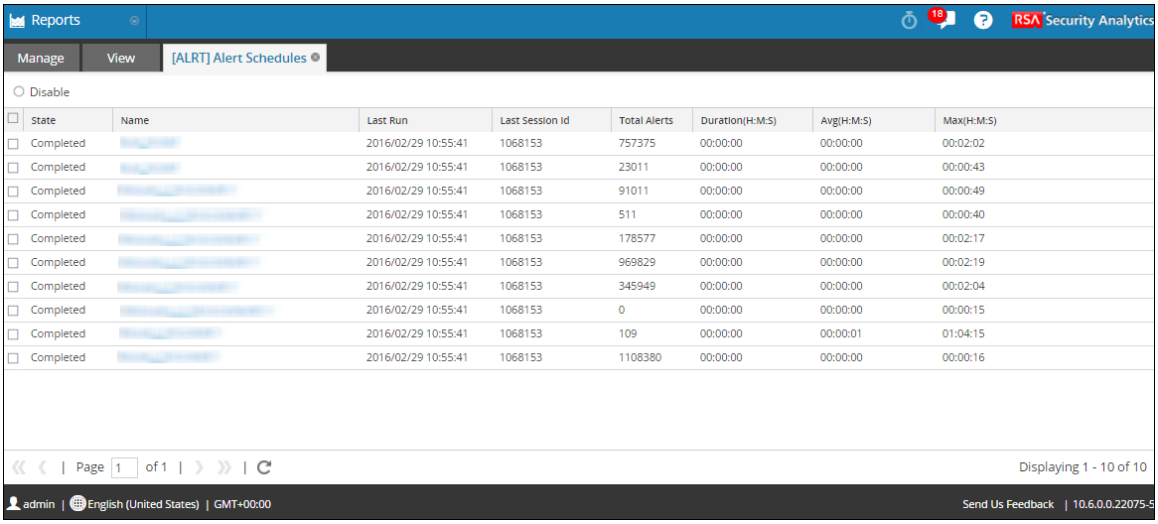
También puede deshabilitar las alertas calendarizadas.

Los procedimientos relacionados se proporcionan en Activar una alerta

Para acceder al cuadro de diálogo:

1. En el menú de **Security Analytics**, haga clic en Administration > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en Alerta.
   Se muestra la vista Alerta.
3. Haga clic en View Schedule.

En la siguiente figura se muestra la vista Ver calendario de alertas.



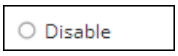
Características

La vista Ver calendario de alertas incluye los siguientes paneles:

1. Barra de herramientas Calendario de alertas
2. Lista de calendario de alertas

Panel de barra de herramientas Calendario de alertas

El panel Barra de herramientas Calendario de alertas permite modificar el estado de la alerta calendarizada.



Cuando se hace clic en Desactivar, se desactiva la alerta seleccionada. Cuando las alertas del programa ya no son necesarias o se determina que son ineficaces, puede deshabilitarlas para que ya no se ejecuten. Puede seleccionar una o más alertas para deshabilitar. Cuando se deshabilita una alerta, se quita de la lista de alertas calendarizadas, de modo que no puede verla aquí; no se ejecutará de nuevo a menos que la ejecute manualmente o que configure un nuevo calendario para ella.

Panel Lista de calendario de alertas

El panel Lista de calendario de alertas muestra solo las alertas habilitadas en formato tabular. En la siguiente tabla se indican las columnas del panel Lista de calendario de alertas y su descripción.

Columna	Descripción
State	El estado de la alerta calendarizada: • Finalizado • Fallido
Nombre	El nombre de la alerta calendarizada.
Última ejecución {#time}	La última vez que se ejecutó la alerta calendarizada.
Último identificador de sesión	El ID de sesión de la última alerta calendarizada.
Alertas totales	La cantidad total de apariciones de eventos.
Duración	El tiempo que tomó ejecutar la alerta calendarizada.
Promedios	El tiempo promedio que tomó ejecutar la alerta calendarizada.
Valores máximos (s)	El tiempo máximo que tomó ejecutar la alerta calendarizada.

Referencias de gráficos

La interfaz del usuario del módulo Reporting proporciona acceso a gráficos de Security Analytics. Este tema contiene descripciones de la interfaz del usuario, así como otra información de referencia para ayudar a los usuarios a administrar los gráficos.

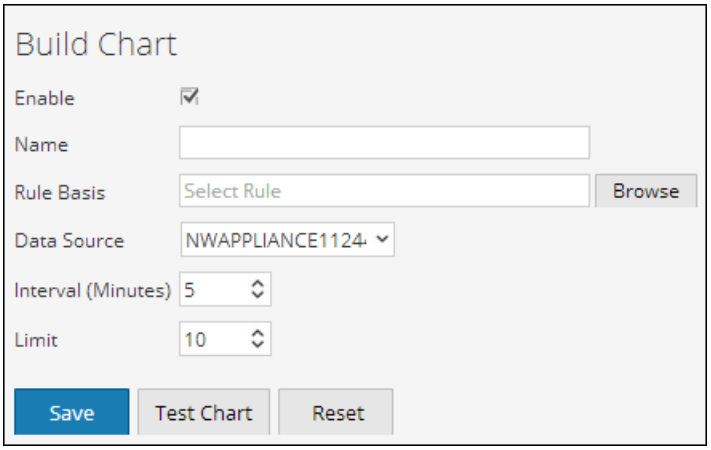
Temas

- Vista Crear gráfico
- Cuadro de diálogo Permisos de gráficos
- Vista Gráfico
- Cuadro de diálogo Importar gráfico
- Vista Probar un gráfico
- Panel Ver un gráfico

Vista Crear gráfico

La vista Crear gráfico permite definir y probar un gráfico. Puede crear un gráfico mediante la asignación de un nombre y la selección de reglas en el cuadro de diálogo Agregar regla. Las únicas reglas que puede usar en los gráficos son las reglas de la base de datos de NetWitness. Los procedimientos asociados con esta vista se proporcionan en Definir grupos de gráficos y gráficos y Probar un gráfico

En la siguiente figura se muestra la vista Crear gráfico.



Características

En la siguiente tabla se muestran las funciones de la vista Crear gráfico.

Campo	Descripción
Habilitar	Especifica si Reporting Engine debe recopilar los datos y generar los

Campo	Descripción
	resultados del gráfico. Si la casilla de verificación **Habilitar** no está seleccionada, no se generan resultados.
Nombre del gráfico	Identifica el nombre del gráfico.
Base de la regla	Haga clic en **Navegar** para mostrar el cuadro de diálogo Agregar reglas, el cual permite seleccionar una regla que es la base de este gráfico. Debe seleccionar una regla que no esté clasificada por ninguno.
Origen de datos	Permite que el usuario seleccione un origen de datos en la lista desplegable. El módulo Reporting funciona con los siguientes orígenes de datos: • Broker • Concentrator • Decoder • Log Decoder • Log Collector
Intervalo (minutos)	El intervalo de actualización de los datos del gráfico en minutos.
Límite	La cantidad de registros para los cuales se generó el gráfico.
Guardar	Guarda el gráfico en la base de datos.
Probar gráfico	Traza un gráfico de prueba según la definición del gráfico.

Cuadro de diálogo Permisos de gráficos

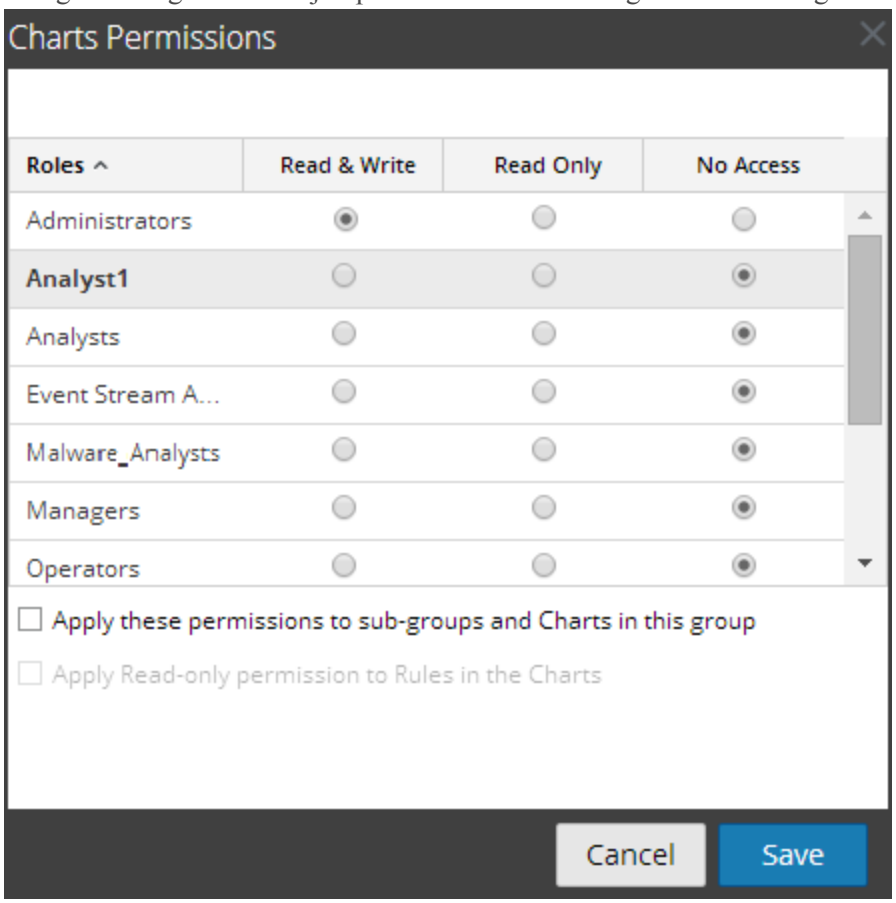
En este tema se describen las funciones del cuadro de diálogo Permisos de gráficos y los permisos de acceso que puede tener el usuario de acuerdo con la función de usuario para administrar un gráfico y un grupo de gráficos. Los usuarios que tienen permiso de acceso de "Lectura y escritura" para configurar permisos de acceso para un gráfico pueden configurar los permisos en el cuadro de diálogo Permisos de gráficos.

Los procedimientos relacionados con este cuadro de diálogo se describen en Administrar el acceso para un gráfico o un grupo de gráficos.

Para acceder al cuadro de diálogo:

1. En el menú de Security Analytics, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Gráficos**.
   Se muestra la vista Gráficos.
3. En el panel **Lista de gráficos**, seleccione un informe.
4. Haga clic en > **Permisos**.
   Se muestra el cuadro de diálogo Permisos de gráficos.

La siguiente figura es un ejemplo del cuadro de diálogo Permisos de gráficos.



En la siguiente tabla se describen las funciones del cuadro de diálogo Permisos de gráficos.

Característica	Descripción
Funciones	La función del usuario que inició sesión en la interfaz del usuario de Security Analytics.
Lectura y escritura	El usuario puede acceder, ver, editar, importar, exportar y eliminar el gráfico en la página Gráficos. El usuario también puede cambiar el permiso en el gráfico.
De solo lectura	El usuario solo puede acceder al gráfico y verlo en la vista Gráficos.
Sin acceso	El usuario no puede acceder a un gráfico ni verlo cuando tiene configurado este permiso.
Aplicar estos permisos a subgrupos y gráficos en este grupo	Seleccione la casilla de verificación para aplicar los permisos seleccionados al grupo de gráficos, subgrupos en el grupo y gráficos en el grupo. **Nota:** Esta casilla de verificación solo se completa cuando se establece permisos de acceso para un grupo de gráficos.
Aplicar permisos de solo lectura a las reglas de los gráficos	Seleccione la casilla de verificación para aplicar permisos a las reglas de los gráficos de forma automática.
Cancelar	Esta opción cancela todos los cambios realizados a los permisos.
Guardar	Esta opción guarda las selecciones y proporciona acceso a las funciones de acuerdo con las selecciones.

Vista Gráfico

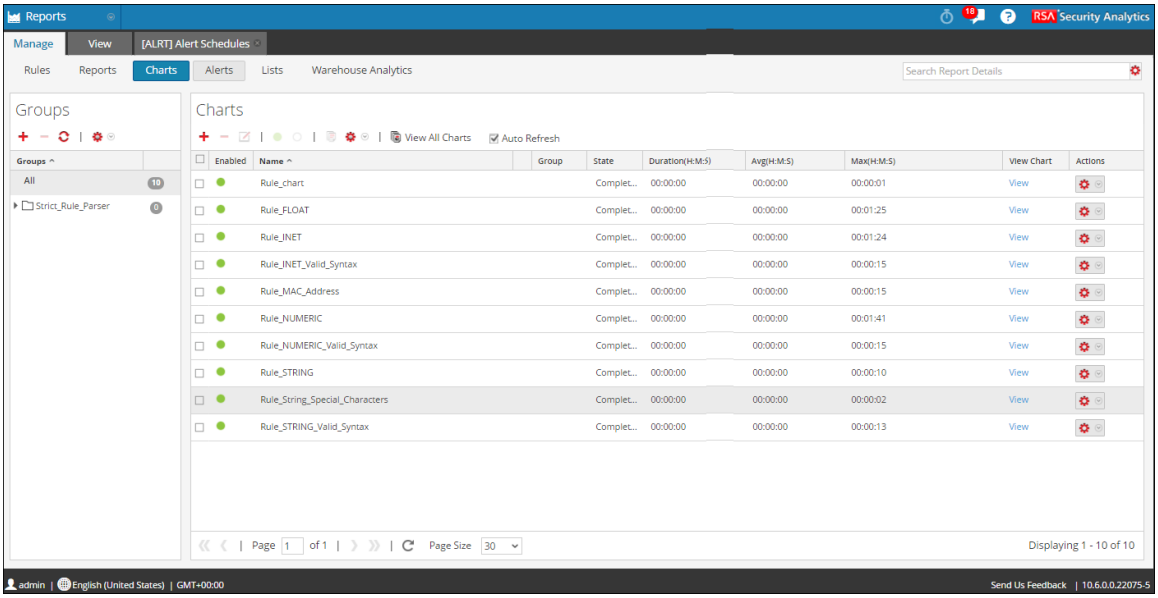
La vista Gráfico permite organizar, ver y administrar gráficos y grupos de gráficos. Los procedimientos asociados con esta vista se describen en Definir grupos de gráficos y gráficos, Administrar el acceso para un gráfico o un grupo de gráficosy Probar un gráfico.

1. En el menú de **Security Analytics**, haga clic en Administration > Informes.
   Se muestra la pestaña Administrar.

2. Haga clic en Gráficos.
   Se muestra la vista Gráfico.

Para acceder a la vista Gráfico:

En la siguiente figura se muestra la vista Gráfico.



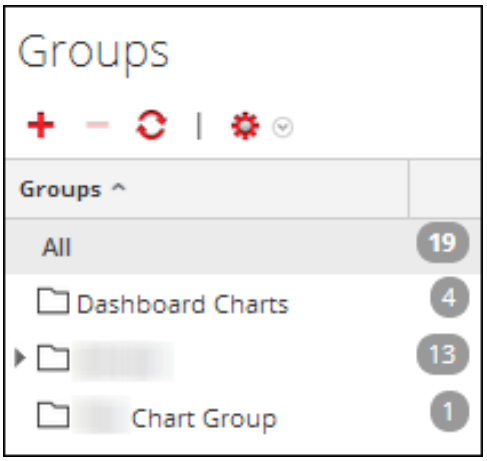
Características

La vista Gráfico incluye los siguientes paneles:

- Grupos de gráficos
- Barra de herramientas Gráfico
- Lista de gráficos

Panel Grupos de gráficos

El panel Grupos de gráficos permite organizar los gráficos en un grupo. Puede crear un grupo, agregar gráficos al grupo y transferirlos entre grupos. En la siguiente figura se muestra el panel Grupos de gráficos.



En el panel Grupos de gráficos se incluyen las siguientes opciones:

Característica	Descripción
+	Esta opción le permite agregar un nuevo gráfico al módulo Reporting.
−	Esta opción le permite eliminar uno o más gráficos seleccionados.
	Esta opción le permite editar un gráfico.
	Esta opción actualiza la vista.
	El menú Acciones tiene las siguientes opciones: Importar, exportar y permisos.

Barra de herramientas Gráficos

La barra de herramientas Gráfico permite agregar, modificar, eliminar, duplicar, habilitar, inhabilitar, importar y exportar un gráfico. También puede establecer permisos de acceso para gráficos en un grupo.

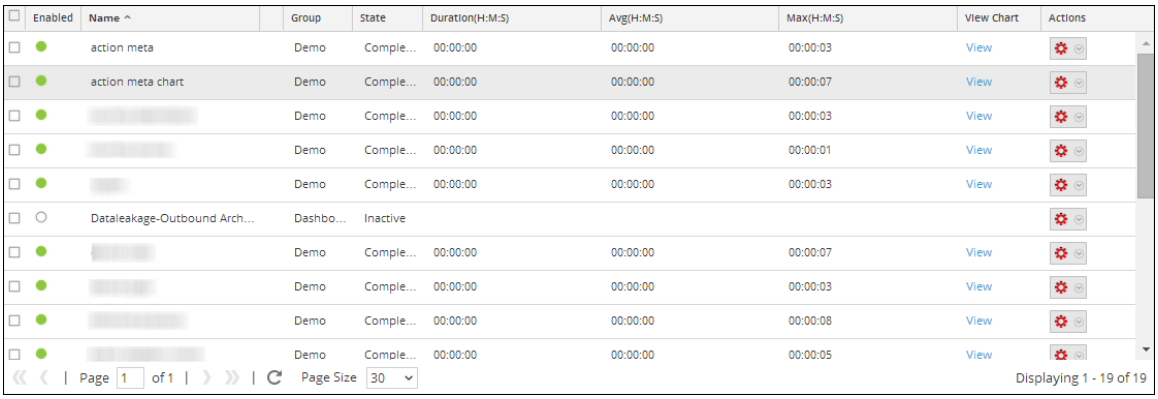
La barra de herramientasGráfico incluye las siguientes opciones:

Característica	Descripción
+	Esta opción le permite agregar un nuevo gráfico al módulo Reporting.

Característica	Descripción
	Esta opción le permite eliminar uno o más gráficos seleccionados.
	Esta opción le permite editar un gráfico.
Habilitar	Esta opción habilita los gráficos seleccionados.
Desactivar	Esta opción deshabilita los gráficos seleccionados.
	Esta opción crea una copia duplicada del gráfico seleccionado.
	El menú Acciones tiene las siguientes opciones: Importar, exportar y permisos.

Lista de gráficos

La Lista de gráficos presenta todos los gráficos en formato tabular o de cuadrícula.



En la siguiente tabla se indican las columnas del panel Lista de gráficos y su descripción.

Característica	Descripción
Nombre	El nombre del gráfico.
Grupo	El grupo de gráficos al cual pertenece el gráfico.
Activado	Sí: el gráfico está activado. No: el gráfico está desactivado.

Característica	Descripción
State	El estado del gráfico: • En línea de espera • Finalizado • Fallido
Duración	El tiempo que tomó ejecutar el último gráfico.
Promedios (en segundos)	El tiempo promedio que tardó la ejecución del gráfico.
Valores máximos (en segundos)	El tiempo mínimo que tardó la ejecución del gráfico.
Ver gráfico	Este es un hipervínculo que redirige al panel Ver un gráfico.
Acciones	El menú Acciones tiene las siguientes opciones: Activar, desactivar, ver, eliminar, editar y exportar.

Cuadro de diálogo Importar gráfico

En este tema se describen las funciones del panel Grupos de gráficos. En este cuadro de diálogo, puede importar gráficos que contienen subgrupos y gráficos de otras instancias de Security Analytics en el panel Grupos de gráficos. Los gráficos deben estar en un archivo binario válido que se haya exportado desde otra instancia de Security Analytics.

Los procedimientos relacionados con este cuadro de diálogo se describen en Importar gráficos y grupos de gráficos

El cuadro de diálogo tiene un aspecto distinto para importar grupos que contienen subgrupos y gráficos de otras instancias de Security Analytics en el panel Grupos de gráficos. Para acceder al cuadro de diálogo:

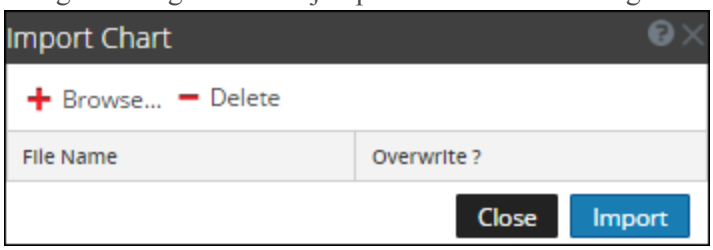
Realice los siguientes pasos para importar gráficos desde otras instancias de Security Analytics:

1. En el menú de Security Analytics, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en Gráficos.
   Se muestra la vista Gráfico.

3. En el panel **Grupos de gráficos**, seleccione una carpeta para importar el archivo.
4. Realice una de las siguientes acciones

    1. En el panel Grupos de gráficos, haga clic en  > **Importar**.
    2. En la barra de herramientas Gráfico, haga clic en  > **Importar**.

La siguiente figura es un ejemplo del cuadro de diálogo.



En la siguiente tabla se describen las funciones del cuadro de diálogo Importar gráfico.

Característica	Descripción
Examinar	Esta opción muestra una vista del sistema de archivos local para que pueda seleccionar el gráfico que desea importar.
Delete	Esta opción elimina un informe importado de la lista de gráficos importados.
Nombre de archivo	Muestra una lista de archivos de gráfico que se importarán al módulo Gráficos cuando hace clic en Importar.
¿Sobrescribir?	Le permite seleccionar la opción para sobrescribir una versión existente del gráfico que se va a importar. Si no selecciona la opción de sobrescritura, se importa un archivo duplicado y no se muestra ningún mensaje de error.
Cerrar	Esta opción cierra el cuadro de diálogo. Si tiene gráficos para seleccionar para importación, pero no ha hecho clic en Importar. Los gráficos no se importan y no se guardan en este cuadro de diálogo.
Importar	Esta opción importa los gráficos seleccionados a su módulo Gráficos.

Panel Ver un gráfico

Puede ver y administrar gráficos en el panel Ver un gráfico. Existen opciones para filtrar y ordenar la información en el gráfico, así como opciones para el tipo de gráfico, el número de elementos en el gráfico y la representación de valores o totales. Al visualizar un gráfico, puede abrir las sesiones representadas en el módulo Investigation y guardar el gráfico como un archivo PDF.

Los procedimientos asociados se describen en Trabajar con gráficos en el módulo Reporting

Para acceder a esta vista:

1. En el menú de Security Analytics, haga clic en Administration > **Informes**.

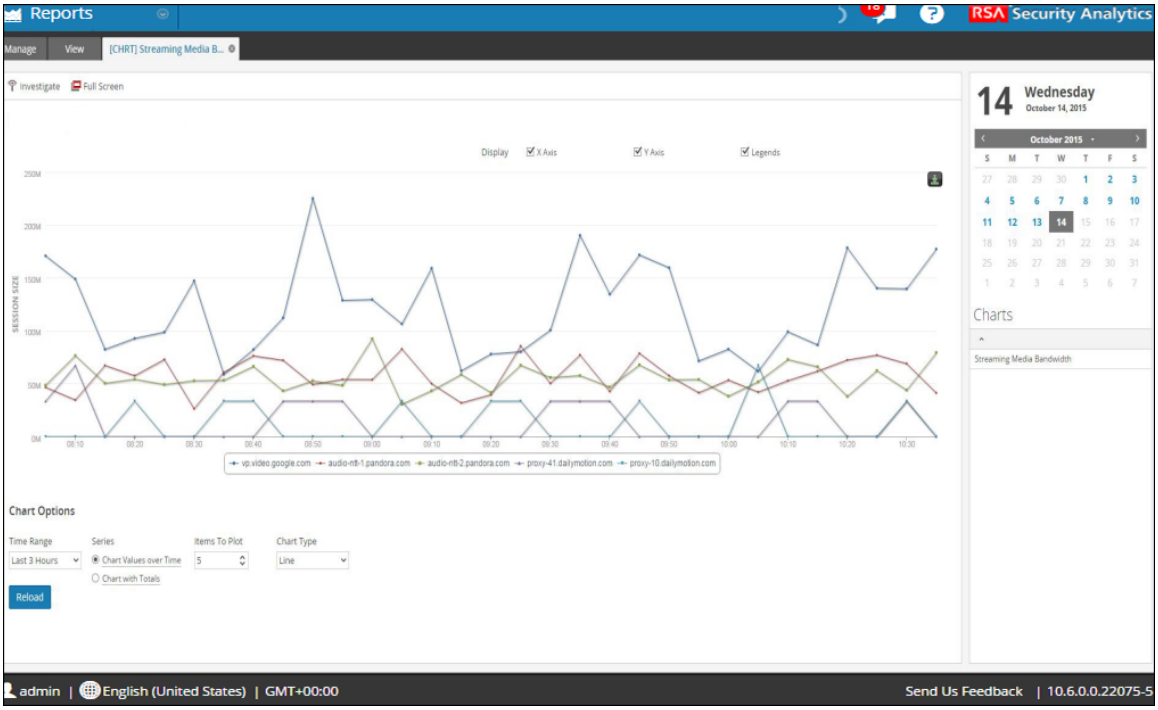
   Se muestra la pestaña Administrar.

2. Haga clic en Gráficos.

   Se muestra la vista Gráfico.

3. Haga clic en  > **Ver.**

La siguiente figura es un ejemplo.



El panel Ver un gráfico tiene los siguientes paneles:

- Barra de herramientas Gráficos
- Salida de gráficos
- Calendario de gráficos

- Opciones de gráficos
- Lista de gráficos ejecutados

Barra de herramientas Gráficos

La barra de herramientas Gráficos tiene opciones que permiten investigar y ver el gráfico en otra pantalla.

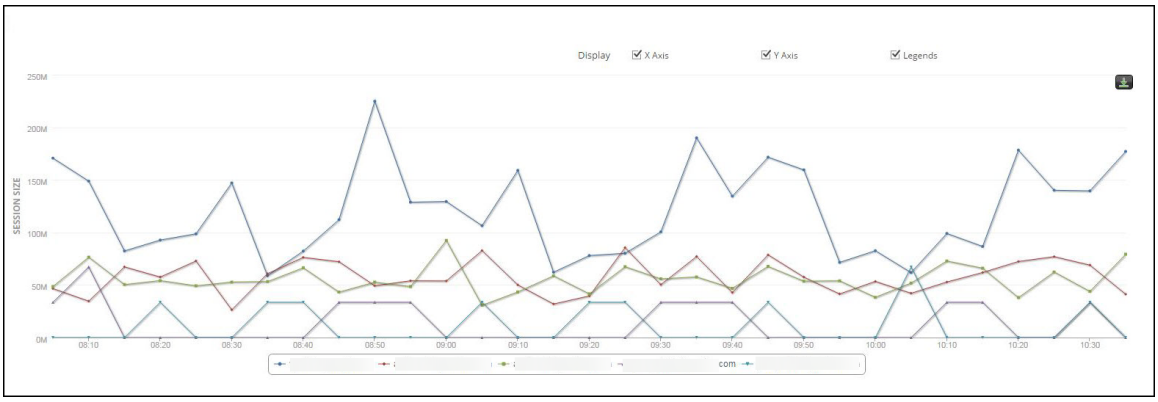
En la siguiente tabla se indican las opciones de la barra de herramientas Gráficos.

Operation	Descripción
Investigar	Investiga los detalles del gráfico.
Pantalla completa	Muestra el gráfico en pantalla completa.

Panel de salida de Gráficos

El panel Salida de gráficos muestra el gráfico con sortBy en el eje Y, la hora en el eje X y leyendas.

Nota: Puede guardar el gráfico como PDF con el ícono .



Panel de calendario de Gráficos

El panel de calendario de Gráficos filtra la lista de gráficos en función de la fecha que se selecciona en el Calendario, como se muestra en la siguiente figura.

El panel Opciones de gráficos

El panel Opciones de gráficos muestra los campos de rango de tiempo, serie y tipo de gráfico para configurar la visualización del gráfico.

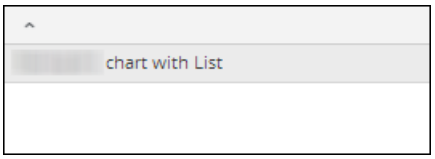
En la siguiente tabla se indican los campos del panel Opciones de gráficos.

Campo	Descripción
Rango de tiempo	El rango de tiempo predeterminado es Últimas 3 horas. Sin embargo, puede seleccionar un valor diferente en la lista desplegable, por ejemplo, Última hora o Últimas 6 horas, los cuales son los valores predefinidos. O puede personalizar seleccionando la opción Últimos n días o Personalizado. **Nota:** Se guardará el rango de tiempo que seleccionó para un gráfico. La próxima vez que se abre el mismo gráfico, se muestra el rango de tiempo que se guardó. Este comportamiento no se aplica a la opción personalizada.
De	La fecha y la hora de inicio (solo para la opción personalizada).
Hasta	La fecha y la hora de finalización (solo para la opción personalizada).

Campo	Descripción
Serie	El campo de serie proporciona dos opciones al usuario: • Valores del gráfico en el tiempo: Genera el gráfico para todo el rango de tiempo seleccionado. • Gráfico con totales: Genera el resumen de datos para el rango de fechas seleccionado.
Elementos para tra-zar	La cantidad máxima de eventos que el usuario desea ver en el gráfico.
Tipo de gráfico	El tipo de gráfico que se generará, ya sea de áreas, barras, columnas, líneas, línea escalonada, área escalonada, área de spline o spline.

Panel Lista de gráficos ejecutados

El panel Lista de gráficos ejecutados muestra todas las ejecuciones de un gráfico específico para la fecha seleccionada. Si hace doble clic en cualquier ejecución del gráfico, se carga el gráfico en el panel Salida de gráficos. De forma predeterminada, el último gráfico ejecutado se muestra en el panel Salida de gráficos.



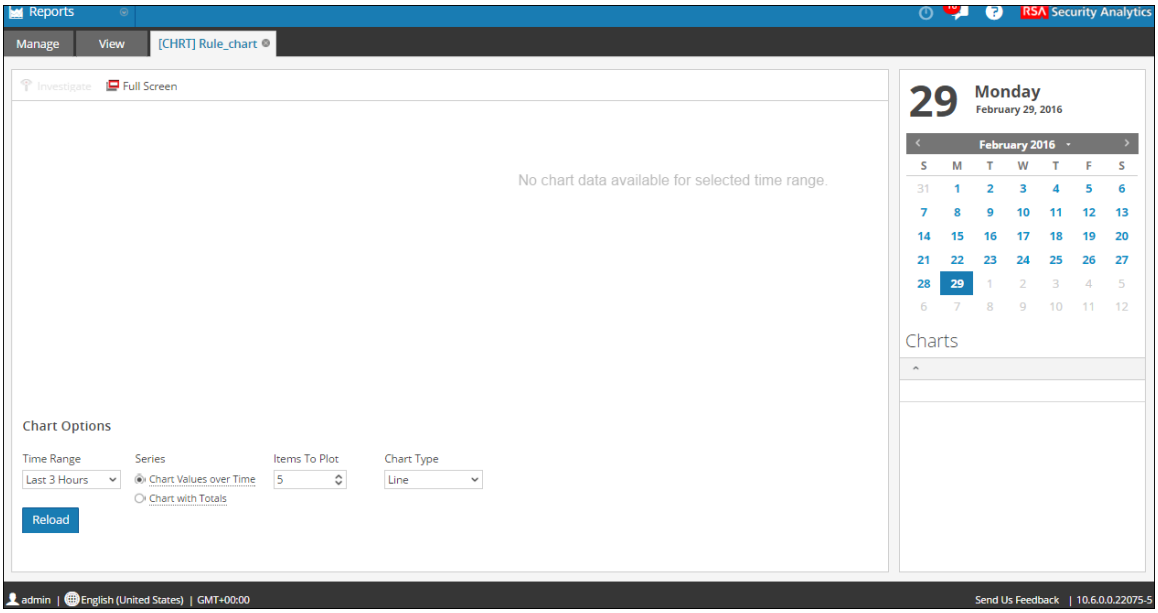
Vista Probar un gráfico

La vista Probar un gráfico permite que el usuario vea y pruebe los gráficos. Asociado. Los procedimientos asociados se proporcionan en Panel Ver un gráfico.

Para acceder a la vista Probar un gráfico:

1. En el menú de Security Analytics, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en Gráficos.
   Se muestra la vista Gráfico.
3. En el panel **Lista de gráficos**, seleccione un informe.
4. Haga clic en **View**.

En la siguiente figura se muestra la vista Probar un gráfico.



Características

La vista Probar un gráfico se compone de los siguientes paneles:

- Barra de herramientas Gráficos
- Salida de gráficos
- Opciones de gráficos

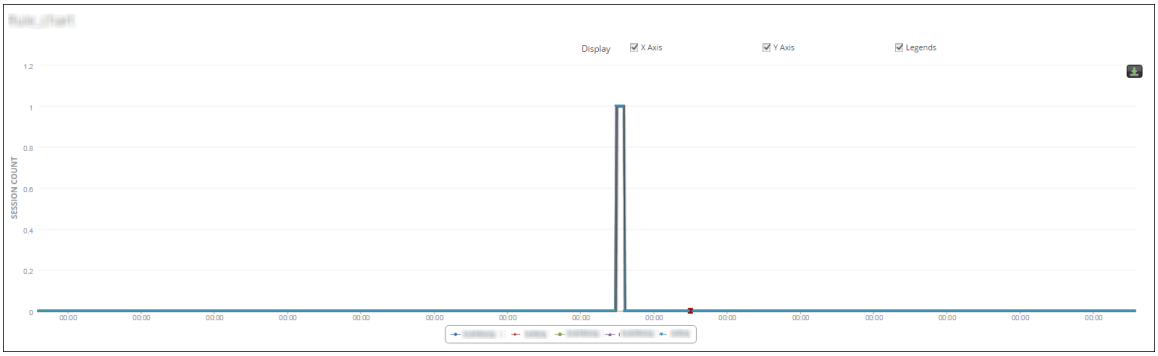
Barra de herramientas Gráficos

La barra de herramientas Gráficos permite investigar un gráfico específico y cambiar a pantalla completa.

Característica	Descripción
Investigar	Esta opción le permite investigar aún más el gráfico seleccionado.
Pantalla completa	Esta opción permite ver el gráfico en pantalla completa.

Salida del gráfico

La salida del gráfico muestra la información en un formato gráfico para las opciones del gráfico de tiempo seleccionado.

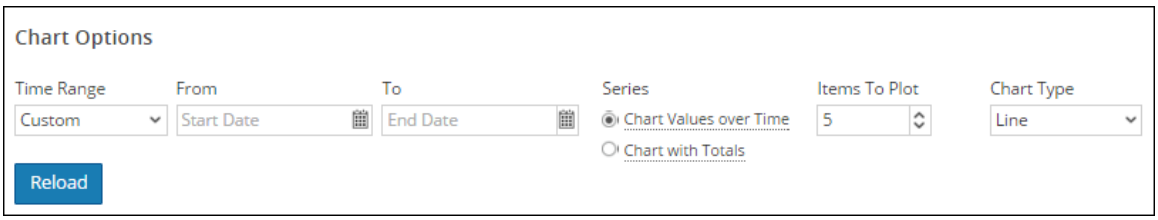


En la siguiente tabla se indican las funciones de la vista Probar un gráfico y su descripción.

Característica	Descripción
Display	Esta opción permite seleccionar los valores que se mostrarán y tiene las siguientes opciones: Eje X, Eje Y y Leyendas.
Eje X	Este campo muestra el conteo de la sesión.
Eje Y	Este campo muestra la salida real.
Leyendas	Este campo muestra la lista de variables que aparecen en el gráfico.

Opciones de gráficos

En la siguiente figura, el panel Opciones de gráficos muestra los campos de rango de tiempo, serie y tipo de gráfico para configurar la visualización del gráfico.



En la siguiente tabla se indican los campos y del panel Opciones de gráficos y sus descripciones.

Característica	Descripción
Rango de tiempo	El rango de tiempo predeterminado es Últimas 3 horas. Sin embargo, puede seleccionar un valor diferente en la lista desplegable, por ejemplo, Última hora o Últimas 6 horas, los cuales son los valores predefinidos. O puede personalizar seleccionando la opción Últimos n días o Personalizado.
De	La fecha y la hora de inicio (solo para la opción personalizada).
Hasta	La fecha y la hora de finalización (solo para la opción personalizada).
Serie	El campo de serie proporciona dos opciones al usuario: • Valores del gráfico en el tiempo: Genera el gráfico para todo el rango de tiempo seleccionado. • Gráfico con totales: genera el resumen de datos para el rango de fechas seleccionado.
Elementos para trazar	La cantidad máxima de eventos que el usuario desea ver en el gráfico.
Tipo de gráfico	El tipo de gráfico que se generará, ya sea de áreas, barras, columnas, líneas, línea escalonada, área escalonada, área de spline o spline.

Referencias de listas

Los siguientes son temas de referencias de listas:

- Vista Crear lista
- Cuadro de diálogo Permisos de listas
- Vista de lista

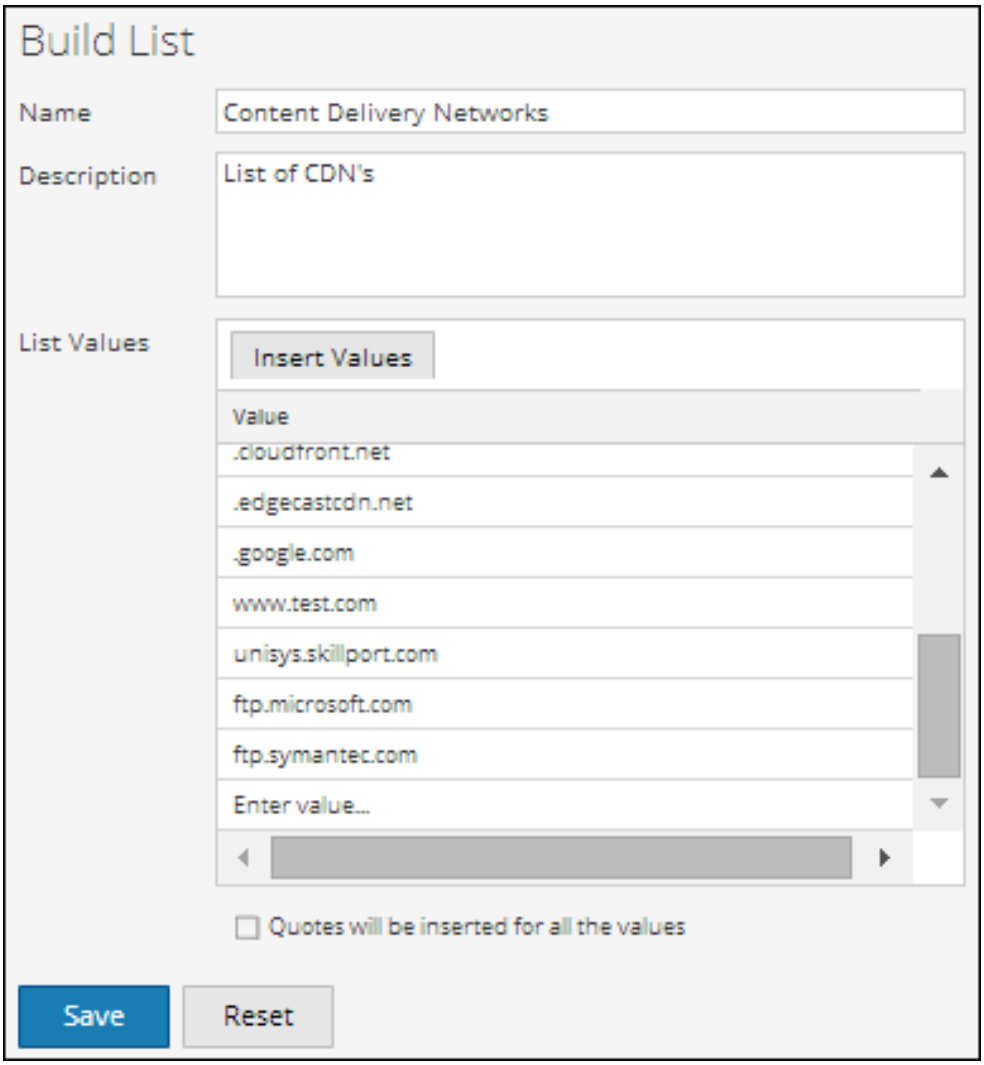
Vista Crear lista

La vista Crear lista permite ingresar valores para una lista y guardarlos o restablecerlos. Cuando escribe reglas de Reporting, puede usar listas para simplificar el proceso de especificación de valores en la regla. Los procedimientos asociados se proporcionan en Trabajar con listas en el módulo Reporting.

Para acceder a esta vista:

1. En el menú de **Security Analytics**, haga clic en Administration > Informes.
   Se muestra la pestaña Administrar.
2. Haga clic en Listas.
   Se muestra la vista Lista.
3. En la barra de herramientas Lista, haga clic en  .
   Se muestra la pestaña de la vista Crear lista.

En la siguiente figura se muestra la vista Crear lista.



En la siguiente tabla se describen las funciones de la vista Crear lista.

Característica	Descripción
Nombre	Identifica y etiqueta la lista.
Descripción	Una descripción breve de la lista.
Valores de lista	La cuadrícula de valores asociados a la lista seleccionada en el panel Biblioteca de listas.

Característica	Descripción
Se insertarán comillas para todos los valores	Si desea que las comillas se incluyan automáticamente para los valores en tiempo de ejecución, seleccione esta casilla de verificación. Si la casilla de verificación no está seleccionada y un valor en la lista contiene una coma, ese valor tiene que estar encerrado entre comillas simples. Cada valor de la lista de una regla IPDB debe encerrarse entre comillas simples. Esta sintaxis no se aplica a los valores de lista de una regla NWDB.
Guardar	Esta opción guarda la regla que se puede utilizar para crear un informe, un gráfico o una lista.
Restablecer	Esta opción elimina toda la información de los campos.

Cuadro de diálogo Permisos de listas

En el cuadro de diálogo Permisos de listas, puede administrar los permisos de acceso que pertenecen a una lista o un grupo de listas. Los usuarios que tienen permiso de "Lectura y escritura" para configurar permisos de acceso para una lista pueden configurar los permisos aquí. Los procedimientos asociados se proporcionan en Administrar el acceso para una lista o un grupo de listas.

Para mostrar el cuadro de diálogo Permisos de informes:

1. En el menú de Security Analytics, haga clic en **Administration > Informes**.

   Se muestra la pestaña Administrar.

2. Haga clic en **Listas**.

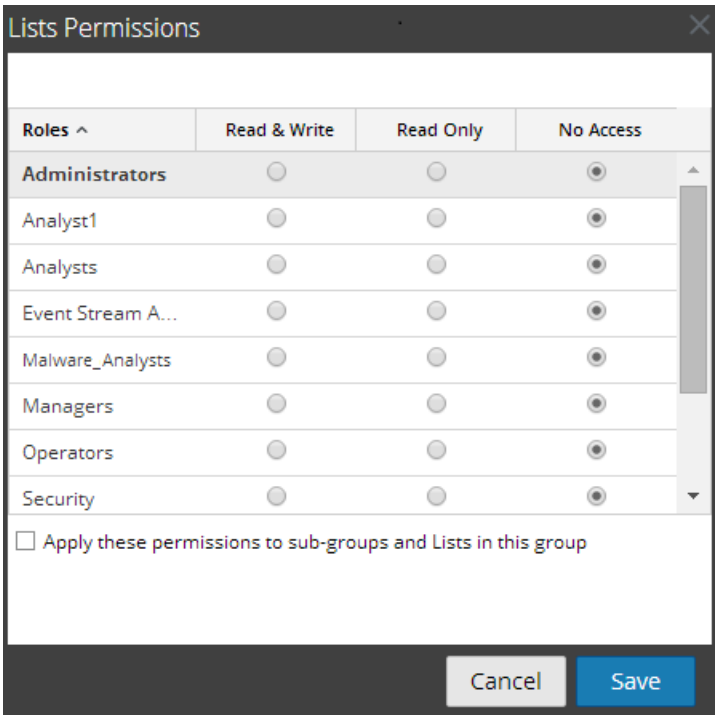
   Se muestra la vista de listas.

3. En el panel **Lista**, seleccione un informe.

4. Haga clic en  > Permisos.

   Aparece el cuadro de diálogo Permisos de listas.

La siguiente figura es un ejemplo del cuadro de diálogo Permisos de listas.



En la siguiente tabla se describen las funciones del cuadro de diálogo Permisos de listas.

Característica	Descripción
Funciones	La función del usuario que inició sesión en la interfaz del usuario de Security Analytics.
Lectura y escritura	El usuario puede acceder, ver, editar, eliminar, importar y exportar listas en la vista Listas. El usuario también puede cambiar el permiso en la regla.
De solo lectura	El usuario solo puede acceder a la lista y verla en la vista Listas.
Sin acceso	El usuario no puede acceder a una lista ni verla cuando tiene configurado este permiso.
Aplicar estos permisos a subgrupos y listas en estos grupos	Seleccione la casilla de verificación para aplicar permisos a los subgrupos y las listas en los grupos de forma automática.
Cancelar	Esta opción cancela todos los cambios realizados a los permisos.

Característica	Descripción
Guardar	Esta opción guarda las selecciones y proporciona acceso a las funciones de acuerdo con las selecciones.

Vista de lista

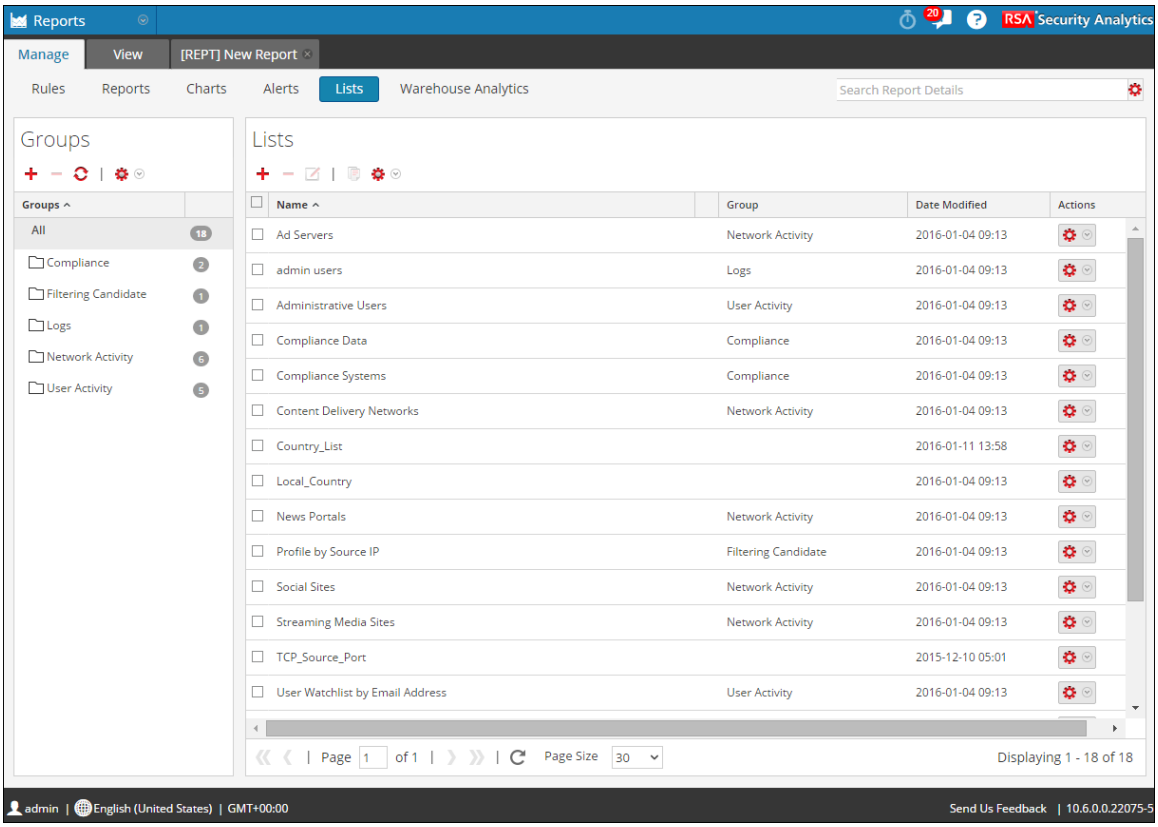
En la Vista de lista, las listas disponibles se presentan en una cuadrícula. Los procedimientos asociados con esta vista se proporcionan en: Definir listas y grupos de listas. Es posible realizar las siguientes acciones:

- Definir listas y grupos de listas.
- Eliminar listas y grupos de listas.
- Establecer permisos de acceso para listas y grupos de listas.
- Importar listas y grupos de listas.
- Exportar listas y grupos de listas.
- Editar una lista.
- Duplicar una lista.

Para acceder a esta vista:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Listas**.
   Se muestra la vista Lista.

En la siguiente figura se muestra la vista Lista.



Características

La vista Lista incluye los siguientes paneles:

- Panel Grupos de listas
- Barra de herramientas Lista
- Panel de la vista Lista

Panel Grupos de listas

El panel Grupos proporciona una lista de grupos que se utilizan para organizar listas y tiene una barra de herramientas que le permite realizar operaciones en los grupos. En la siguiente tabla se describen las funciones del panel Grupos.

Característica	Descripción
+	Esta opción le permite agregar un nuevo gráfico al módulo Reporting.
−	Esta opción le permite eliminar uno o más gráficos seleccionados.

Característica	Descripción
	Esta opción le permite editar un gráfico.
	Esta opción actualiza la vista.
	El menú Acciones tiene las siguientes opciones: Importar, exportar y permisos.

Puede realizar las siguientes acciones con el panel Grupos de listas:

- Actualizar las listas de un grupo.
- Mover listas entre diversos grupos. Puede mover una lista de un grupo a otro arrastrando y soltando la lista en el grupo requerido.
- Agregar un grupo de listas.
- Eliminar un grupo de listas.
- Importar listas y grupos de listas.
- Exportar grupos de listas.
- Establecer el control de acceso para grupos de listas.

Barra de herramientas Lista

Característica	Descripción
	Esta opción le permite agregar una nueva lista al módulo Reporting.
	Esta opción le permite eliminar una o más listas seleccionadas.
	Esta opción le permite editar una lista.
	Esta opción crea una copia duplicada de la lista seleccionada.
	El menú Acciones tiene las siguientes opciones: Importar, exportar y permisos.

Panel de la vista Lista

El panel de la vista Lista muestra las listas definidas en formato tabular. En la siguiente tabla se indican lascolumnas y su descripción.

Columna	Descripción
Nombre	El nombre de la lista. **Nota:** En el campo **Nombre**, el ícono para expandir el tamaño de la columna no se muestra al final del campo de la columna. Debe mover el mouse un poco hacia la izquierda para ver el ícono que permite ampliar la columna.
Grupo	El grupo de listas al cual pertenece la lista.
Fecha de modificación	La fecha y hora en que se modificó la lista.

Referencias de informes

La interfaz del usuario del módulo Reporting proporciona acceso a informes de Security Analytics. Este tema contiene descripciones de la interfaz del usuario, así como otra información de referencia para ayudar a los usuarios a administrar los informes.

Temas

- Vista Crear informe
- Cuadro de diálogo Importar informe
- Cuadro de diálogo Permisos de informes
- Vista Informe
- Referencias de calendarios
  - Características
  - Características
  - Características
  - Características
  - Características
- Cuadro de diálogo Seleccionar un logotipo

- Panel Ver todos los informes
- Panel Ver un informe

Panel Historial de ejecución

El panel Historial de ejecución permite buscar y mostrar detalles del historial.

Para acceder a esta vista:

1. En el panel Lista de informes, realice una de las siguientes acciones:

   - Mantenga el mouse sobre un informe y haga clic en > **Ver informes calendarizados**.
   - Haga clic en la columna **N.º de calendarios**.
   - En el panel Lista de informes, realice una de las siguientes acciones:

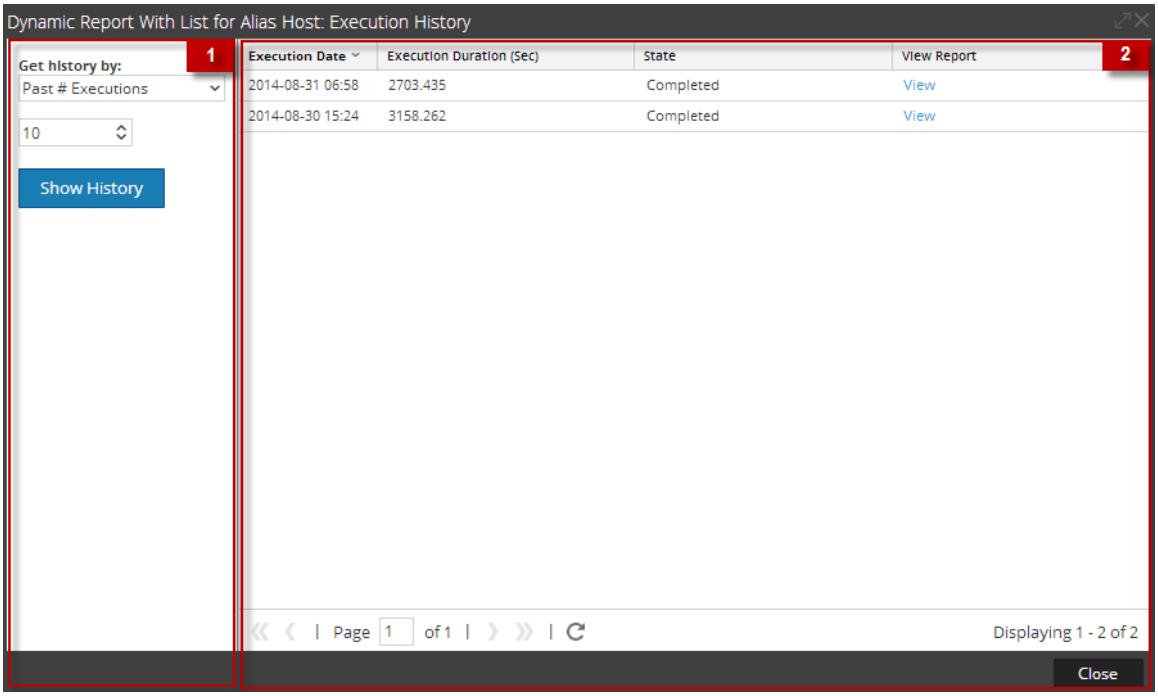
     - Mantenga el mouse sobre un informe y haga clic en > **Ver informes calendarizados**.
     - Haga clic en la columna **N.º de calendarios**.

     La vista Calendarizar informes se muestra con el estado de cada uno de los informes calendarizados.

   - Seleccione un informe programado y realice una de las siguientes acciones:

     - Haga clic en > **Historial de ejecución**.
     - Haga clic en en el panel de la barra de herramientas Informes calendarizados.

La siguiente figura es un ejemplo de la vista Historial de ejecución.



Características

Ver historial de ejecución incluye los siguientes paneles:

- Panel Opciones del historial de ejecución
- Panel Salida del historial de ejecución

Panel de opciones

El panel Opciones del historial de ejecución permite buscar los detalles del historial de acuerdo con una determinada cantidad de informes calendarizados pasados o un rango de fechas específico.

En la siguiente tabla se indican las operaciones del panel Opciones del historial de ejecución:

Operation	Descripción
Obtener historial por:	Corresponde a los criterios para ver el historial de ejecución: • **Últimas N ejecuciones**: una determinada cantidad de informes calendarizados pasados. • **Rango (específico)**: fecha inicial y fecha de finalización del rango de fechas. **Nota:** Los campos **De** y **Hasta** se completan en la interfaz del usuario de Security Analytics solo cuando se selecciona "Rango (específico)" en la lista **Obtener historial por**.
De	Fecha inicial del rango de fechas.
Hasta	Fecha de finalización del rango de fechas.
Count	Cantidad del historial de ejecución del informe programado que se mostrará.
Show History	Muestra los detalles del historial de acuerdo con los criterios seleccionados.

Panel Salida

El panel Salida del historial de ejecución muestra los detalles del historial con la fecha de ejecución, la duración de la ejecución (segundos), el estado del informe calendarizado y un vínculo para ver el informe.

En la siguiente tabla se indican las diversas columnas del panel Salida del historial de ejecución:

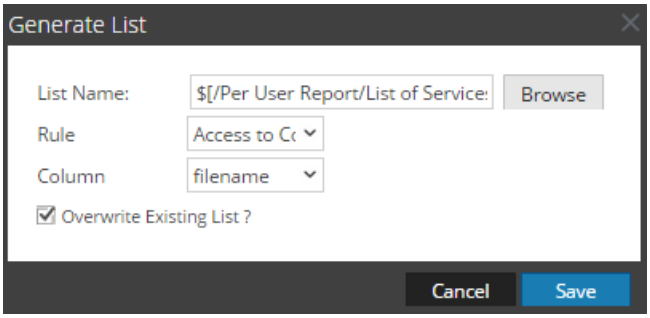
Columna	Descripción
Fecha de ejecución	Fecha en que se ejecutó el informe calendarizado. De forma predeterminada, la fecha de ejecución aparece en orden descendente.
Duración de la ejecución (segundos)	Tiempo que tardó la ejecución del informe calendarizado.

Columna	Descripción
State	Estado del informe calendarizado: • Programado: si un informe está calendarizado para ejecutarse cada una hora, de forma diaria, semanal o mensual o más adelante, su estado se muestra como calendarizado para la primera ejecución. • En línea de espera: si un informe aún espera su ejecución, su estado se muestra como en línea de espera. • En ejecución: Si el programa del informe está en curso, su estado se muestra como en ejecución. • Parcial: si en un informe con varias reglas se produce una falla en una única ejecución de regla, en una acción de salida o en la creación de PDF/CSV, el estado del informe se muestra como parcial. Por ejemplo, considere un informe con cinco reglas, de las cuales cuatro se ejecutan correctamente y una falla, razón por la cual el estado se muestra como Parcial. • Fallido: si en un informe con varias reglas, todas las ejecuciones del calendario de reglas fallan, el estado del informe se muestra como fallido. • Completado: Si el programa del informe se ejecuta correctamente, el estado del informe se muestra como completado. • Cancelado: cuando se completa una solicitud de cancelación, el estado del informe se muestra como cancelado. • Inactivo: si el calendario del informe está desactivado, el estado del informe se muestra como inactivo. • No disponible: Si la información de ejecución del programa del informe no está disponible, el estado del informe se muestra como no disponible.
Ver informe	El hipervínculo a Ver un informe en pantalla completa.
Cerrar	Cierra la vista del historial de ejecución.

Cuadro de diálogo Generar lista

El cuadro de diálogo Generar lista permite generar y personalizar una lista.

La siguiente figura es un ejemplo del cuadro de diálogo Generar lista.

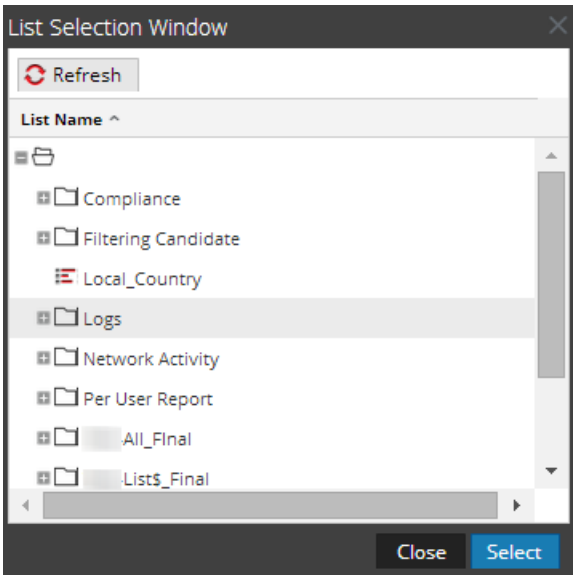


Características

Campo	Descripción
Nombre de lista	El nombre de la lista seleccionada en el panel Selección de lista.
Examinar	Haga clic en este botón para seleccionar una lista en el cuadro de diálogo Ventana Selección de lista.
Regla	Seleccione una regla que se usará para crear la lista.
Columna	Seleccione un valor para la columna.
¿Desea sobrescribir la lista existente?	Sobrescribe la lista existente.
Guardar	Agrega la lista deseada al panel Generar lista de la vista Calendarizar informe.

En la siguiente tabla se indican las funciones del cuadro de diálogo Generar lista.

El cuadro de diálogo Ventana Selección de lista consta de listas que se definen en el panel Listas. Aquí, puede seleccionar una lista para asociarla con el informe. En la siguiente figura se muestra el cuadro de diálogo.



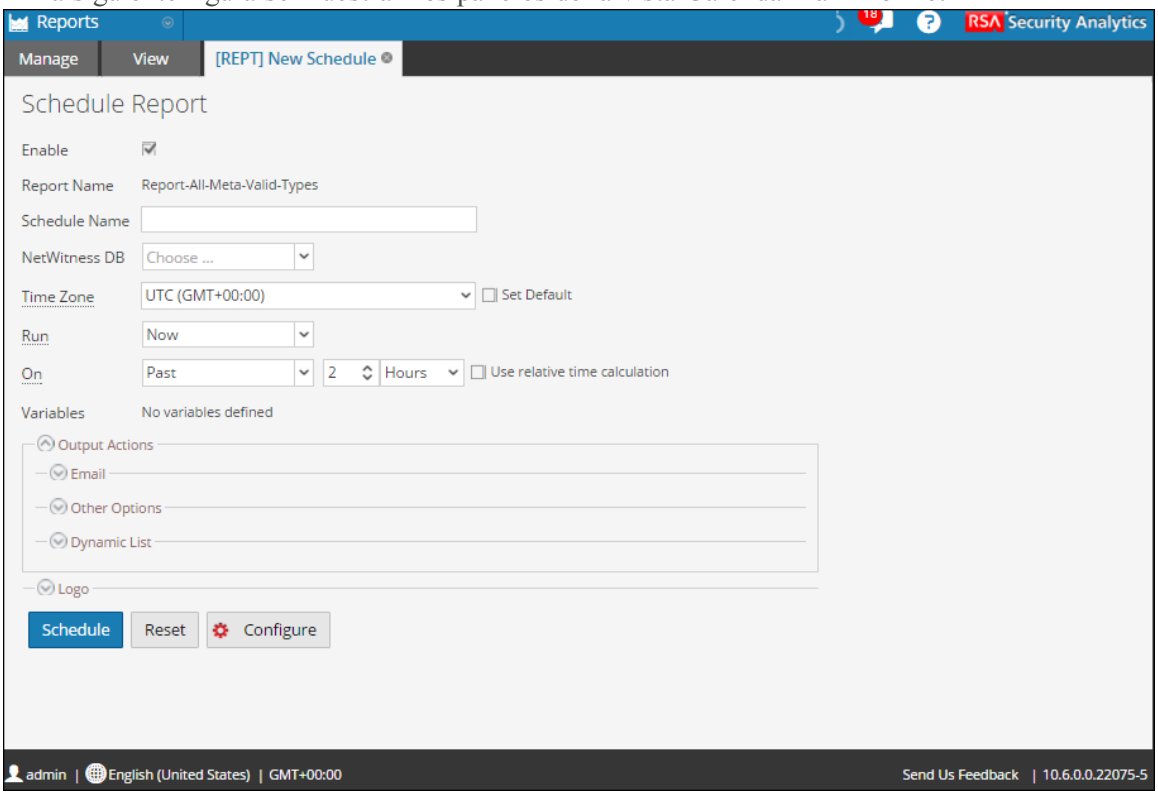
Panel Calendarizar informe

El panel Calendarizar informe le permite programar un informe personalizado. Antes de programar un informe, tiene que crear una lista dinámica (con la opción de sobrescritura seleccionada) con servicios agregados. Para obtener más información, consulte Requisitos previos. Posteriormente, use la lista para generar un informe con detalles en el informe, como servicios y nombres de host.

Para acceder a esta vista:

1. En el menú de Security Analytics, haga clic en Administration > Informes.
   Se muestra la pestaña Administrar.
2. Haga clic en Informes.
   Se muestra la vista Informe.
3. En el panel **Lista de informes**, haga clic en  > **Calendarizar informe**.

En la siguiente figura se muestran los paneles de la vista Calendarizar informe.



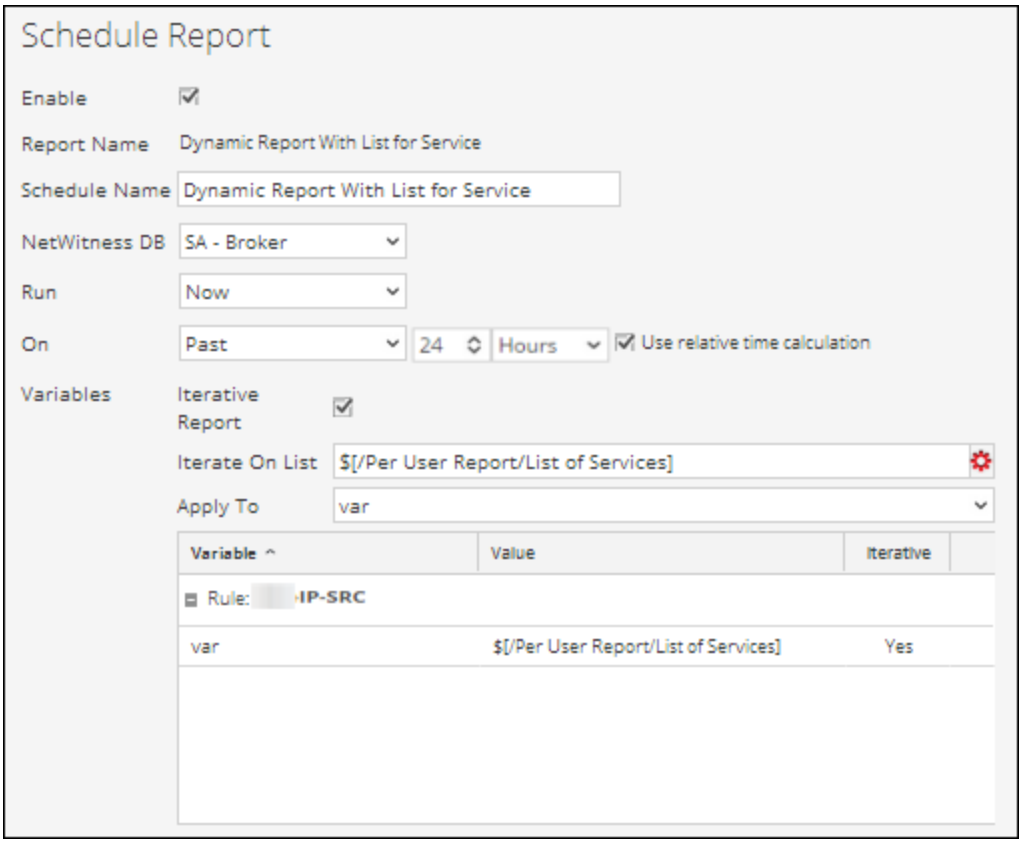
Características

La vista Calendarizar informe se compone de los siguientes paneles:

- Calendarizar informe
- Acciones de salida
- Lista dinámica
- Logotipo

Panel Calendarizar informe

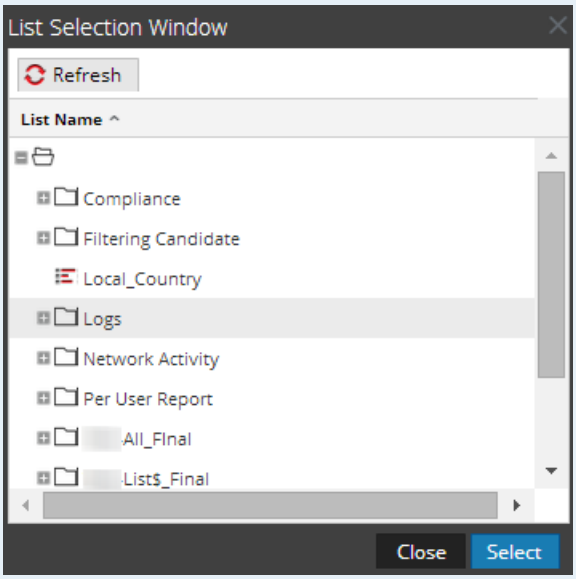
El panel Calendarizar informe permite programar informes.



En la siguiente tabla se indican los campos del panel Calendarizar informe.

Campo	Descripción
Habilitar	Activa los calendarios de informes y ejecuta el informe.
Nombre de informe	Es el nombre del informe.
Nombre de calendario	El nombre de la configuración de informes calendarizados.
Base de datos de NetWitness	La base de datos puede ser de NWDB, de IPDB o de una base de datos de Warehouse, según el tipo de base de datos que seleccionó en la definición de la regla. Si el informe tiene reglas de tipos de base de datos de NWDB, IPDB y Warehouse, se muestran todos los tipos de base de datos o tipos de reglas.

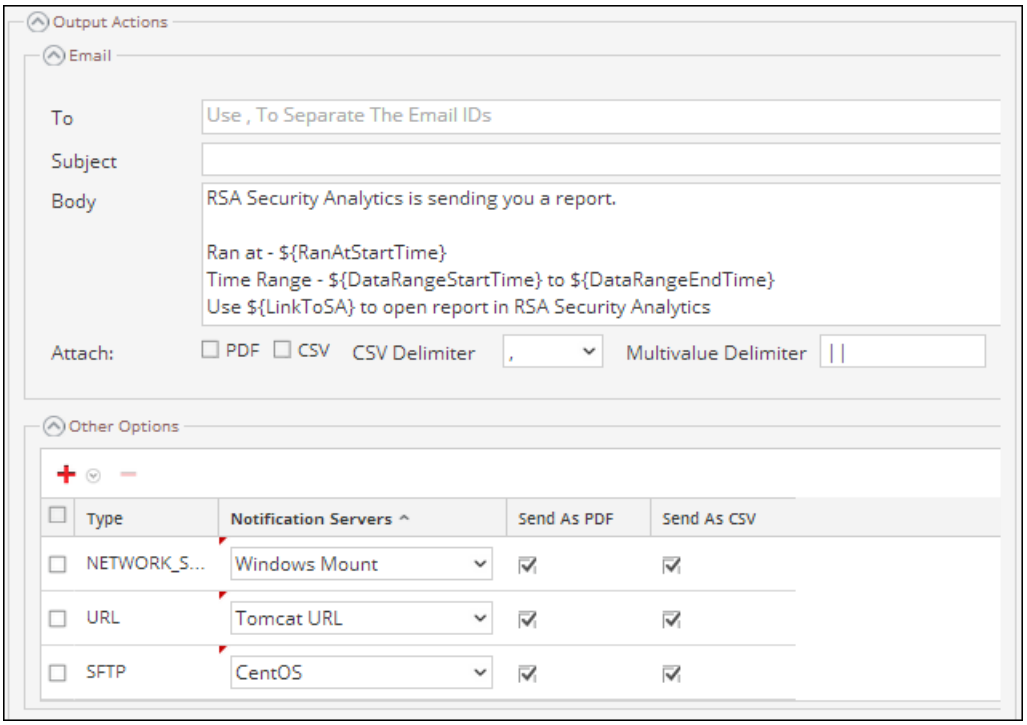
Campo	Descripción
Pool de recursos de Warehouse	Si el informe tiene reglas de base de datos de Warehouse, se muestra el menú desplegable Pool de recursos de Warehouse para seleccionar los pools o las líneas de espera disponibles en el clúster. Si no se ingresan pools o líneas de espera para Reporting Engine, este campo estará deshabilitado. Para obtener más información, consulte Paso 5: Configurar un programador de tareas para Reporting Engine en la *Guía de configuración de hosts y servicios*.
Ejecutar	Proporciona el tipo de calendario para la configuración de la ejecución: • Ejecución ad hoc • Ejecución cada una hora • Ejecución diaria • Ejecución semanal • Ejecución mensual
Encendido	El rango de datos en el cual se ejecuta la consulta.
Usar cálculo de tiempo relativo	Usa la duración del tiempo relativo para programar un informe.
Informe iterativo	Seleccione la casilla de verificación para programar un informe para el valor de la lista seleccionada.

Campo	Descripción
Iterar en lista 	Haga clic en este botón para navegar al panel Selección de lista y seleccione una lista. En la siguiente figura se muestra este panel:  El panel Selección de lista es una recopilación de listas. Reporting Engine mantiene una lista activa de los nombres de lista disponibles mediante la sincronización continua con la recopilación a la cual está conectado.
Aplicar a	Aplica valores de lista en la variable seleccionada.
Variables	Muestra las variables de reglas junto con sus valores asociados y las propiedades iterativas que se incluyen en el informe. **Nota:** Según la regla elegida cuando se creó el informe, puede ver las variables dinámicas definidas para la regla en el campo **Variables** del panel Calendarizar informe. Por ejemplo, Test-Country es la regla que tiene un var de variable dinámica.
Calendario	Calendariza el informe.
Restablecer	Restablece el informe calendarizado.

Campo	Descripción
Configurar	Permite modificar los detalles de configuración de Reporting Engine, como se menciona en el tema Pestaña General de Reporting Engine de la *Guía de configuración de hosts y servicios*. **Nota:** Este botón solo está visible en el panel Calendarizar informe cuando dispone de permisos de acceso "Administrar dispositivo" en el módulo Reporting.

Panel Acciones de salida

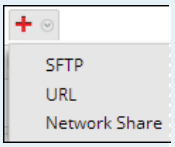
El panel Acciones de salida especifica acciones de salida para notificar al destinatario del correo electrónico cuando se completa la ejecución del informe y también envía informes en los formatos PDF y CSV como archivos adjuntos en el correo electrónico, de acuerdo con su selección.



En la siguiente tabla se indican los campos del panel Acciones de salida.

Campo	Descripción
Para	Una lista separada por comas de las direcciones de correo electrónico que recibirán la salida.

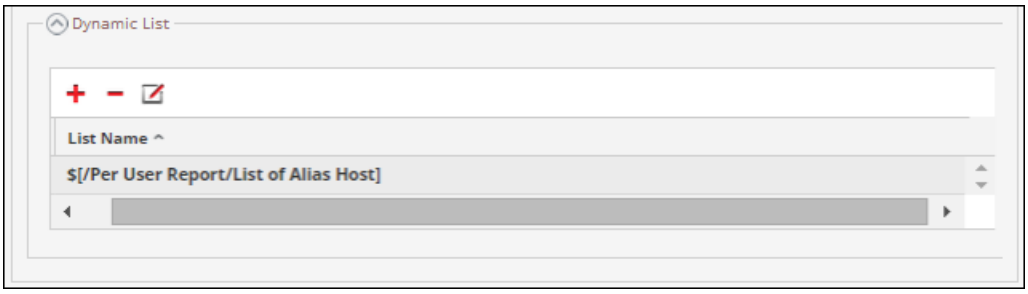
Campo	Descripción
Asunto	El asunto ingresado en el correo.
Cuerpo	El cuerpo del correo electrónico. De manera predeterminada, el campo de contenido se llena con texto predefinido que tiene ciertas variables y que agregará metadatos adecuados para el informe generado. En Reporting Engine, estas variables se reemplazan por valores reales. • `${RanAtStartTime}`: La hora de inicio del informe. • `${DataRangeStartTime}`: La hora de inicio del rango de tiempo de los datos. • `${DataRangeEndTime}`: La hora de finalización del rango de tiempo de los datos. • `${LinkToSA}`: El vínculo al host de Security Analytics desde el correo electrónico, el cual, a la vez, abre el informe en la interfaz de Security Analytics. • `${ReportName}`: El nombre del informe. • `${DataSource}`: El nombre del origen de datos.
Asociar:	El formato de salida en el cual se adjunta el informe al correo electrónico, como PDF o CSV, según lo configurado en el cuadro de diálogo Calendarizar informe.

Campo	Descripción
Delimitador de CSV	El delimitador de CSV predeterminado es la coma (,). Si el contenido de CSV contiene una coma, debe identificar un separador único para que el contenido se almacene en su forma original. Por ejemplo, si msg es una columna en el informe que se guardará como CSV y el contenido de msg presenta estas características: `ASA-SSM-CSC-20 Module in slot 1," application reloading ""CSC SSM""," version ""6.2.1599.0"" CSC SSM scan services are reloading because of a pattern file or configuration update` El contenido anterior se incluirá en tres columnas debido a las comas (,). Para evitar esto, debe especificar un delimitador distinto, como un carácter de tubería "|". **Nota:** Para importar el archivo CSV en Microsoft Excel, use la opción Datos > Desde texto en la aplicación de Excel. Cuando importe el archivo CSV debeespecificar el tipo del archivo que va a importar como Delimitado y usar el mismo delimitador que especifica para generar el archivo CSV.
Delimitador de varios valores	Los datos en los campos de varios valores se separan con un delimitador de varios valores. El delimitador de varios valores predeterminado corresponde a dos caracteres de barra vertical (||).
Otras opciones	Puede seleccionar un SFTP, una URL o una ubicación de recurso compartido de red configurada en ((RE}} y luego enviar el informe en formato PDF o CSV según el requisito.
	Seleccione esta opción para enviar el informe a la ubicación de SFTP, URL o recurso compartido de red configurada en la vista Configuración de servicios de Reporting Engine.
Tipo	El tipo de acción de salida elegido. Por ejemplo, SFTP, URL o recurso compartido de red.

Campo	Descripción
Acciones de salida	Seleccione el nombre de SFTP, URL o recurso compartido de red configurado en la vista Configuración de servicios de Reporting Engine.
Enviar como PDF / Enviar como CSV	Seleccione estas opciones para enviar el informe en formato PDF, CSV o ambos al servidor de notificación configurado (SFTP, URL o recurso compartido de red).

Panel Lista dinámica

El panel Lista dinámica completa las listas creadas. Es posible agregar, editar o eliminar la lista. La lista se genera en función del informe calendarizado, el cual se puede ver en la vista Listas.



En la siguiente tabla se indican las operaciones disponibles en el panel Generar lista.

Operation	Descripción
+	Agrega una nueva lista al informe.
−	Elimina todas las listas agregadas al informe.
✎	Muestra el cuadro de diálogo Generar lista.
Nombre de lista	El nombre de la lista seleccionada en el panel Selección de lista. Para obtener más información acerca del panel Selección de lista, consulte Características.

Panel Logotipo

El panel Logotipo completa el logotipo predeterminado desde el panel Seleccionar un logotipo. Para obtener más información sobre la elección de un logotipo desde este panel, consulte Administrar y seleccionar un logotipo de informe.

Puede establecer el logotipo predeterminado para un Reporting Engine. Este es el logotipo que se utiliza en los informes generados. Para obtener más información sobre la elección de un logotipo, consulte Cuadro de diálogo Seleccionar un logotipo.

Nota: Si no seleccionó ningún logotipo, se usa el logotipo predeterminado de RSA en el informe. La opción **Guardar como PDF** para los informes ejecutados con anterioridad no es compatible con un nuevo logotipo del cliente. Muestra el logotipo predeterminado de RSA si el logotipo del cliente se debe mostrar en la vista Programar un informe.

Vista Informes calendarizados

La vista Informes calendarizados permite crear, ver y administrar informes calendarizados. Los procedimientos asociados se proporcionan en Calendarizar informes yEstablecer el control de acceso para un informe. Puede:

- Activar o desactivar un informe calendarizado.
- Iniciar o detener un informe programado
- Editar un informe programado
- Eliminar un informe calendarizado.
- Establecer permisos de acceso para un informe.
- Ver el historial de ejecución de un informe calendarizado.

Para acceder a esta vista:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.

   Se muestra la pestaña Administrar.

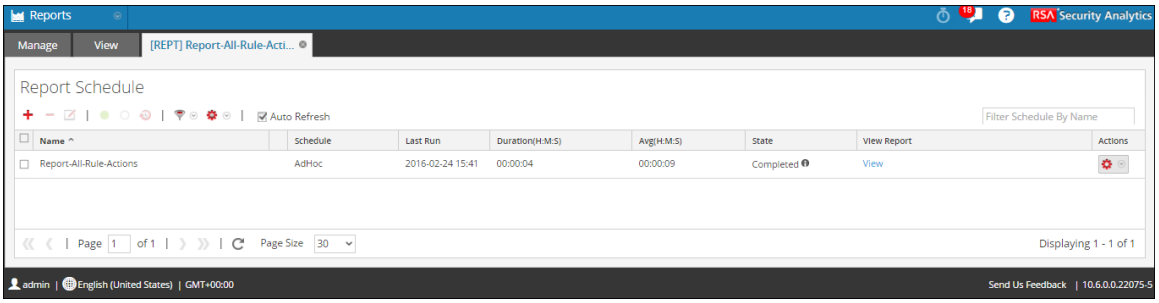
2. Haga clic en **Informes**.

   Se muestra la vista Informe.

3. En el panel **Lista de informes**, realice una de las siguientes acciones:

   - Haga clic en  > **Ver informes calendarizados**.
   - Haga clic en la columna **N.º de calendarios**.

En la siguiente figura se muestran los diferentes paneles de esta vista:



Características

Ver informes calendarizados incluye las siguientes funciones:

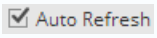
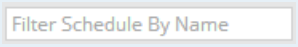
- Barra de herramientas Informes calendarizados
- Panel Lista de informes calendarizados

Barra de herramientas Informes calendarizados

La barra de herramientas Informes calendarizados permite agregar, modificar y eliminar el informe calendarizado, además de habilitar o deshabilitar la configuración de ejecución seleccionada.

En la siguiente tabla se indican las operaciones de la barra de herramientas Informes calendarizados.

Operation	Descripción
	Crear un nuevo calendario de informes o informe calendarizado.
	Elimina el calendario de informes seleccionado.
	Edita el calendario de informes seleccionado. **Nota:** Haga doble clic en un calendario de informes deseado para editarlo.
	Activa el calendario de informes seleccionado.
	Desactiva el calendario de informes seleccionado.
	Vea el historial del informe calendarizado.

Operation	Descripción
	Filtre calendarios basándose en el tipo de calendario. (Por ejemplo, Ad Hoc)
	Le permite establecer permisos para el informe programado seleccionado.
	Actualiza automáticamente la lista de informes calendarizados.
	Busca calendarios basándose en el nombre del calendario.

Panel Lista de informes calendarizados

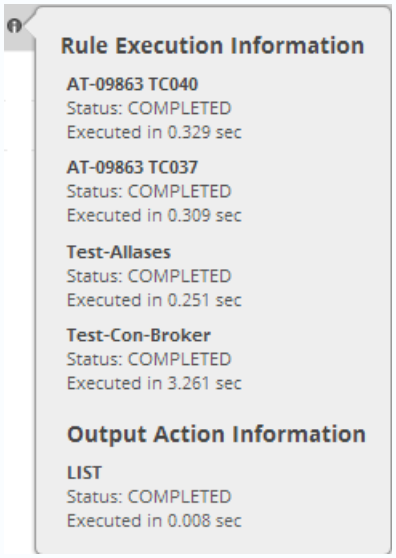
En el panel Lista de informes calendarizados se muestran los informes calendarizados en formato tabular. En este panel puede realizar las siguientes acciones.

En la siguiente tabla se indican las columnas del panel Lista de informes calendarizados:

Columna	Descripción
Nombre	El nombre del informe calendarizado.
Calendario	El tipo de calendario para la configuración de la ejecución: • Ejecución ad hoc • Ejecución cada una hora • Ejecución diaria • Ejecución semanal • Ejecución mensual
Última ejecución	Muestra la última vez que se ejecutó el informe.
Última ejecución en (s)	Muestra la cantidad de veces que se calendarizó el mismo informe.
Promedios	Muestra el tiempo promedio que tardó la ejecución del informe.

Columna	Descripción
State	Indica el estado del informe calendarizado. • Programado: si un informe está calendarizado para ejecutarse cada una hora, de forma diaria, semanal o mensual o más adelante, su estado se muestra como calendarizado para la primera ejecución. • En línea de espera: si un informe aún espera su ejecución, su estado se muestra como en línea de espera. • En ejecución: Si el programa del informe está en curso, su estado se muestra como en ejecución. • Parcial: si en un informe con varias reglas se produce una falla en una única ejecución de regla, en una acción de salida o en la creación de PDF/CSV, el estado del informe se muestra como parcial. Por ejemplo, considere un informe con cinco reglas, • de las cuales cuatro se ejecutan correctamente y una falla, razón por la cual el estado se muestra como Parcial. • Fallido: si en un informe con varias reglas, todas las ejecuciones del calendario de reglas fallan, el estado del informe se muestra como fallido. • Completado: Si el programa del informe se ejecuta correctamente, el estado del informe se muestra como completado. • Cancelado: cuando se completa una solicitud de cancelación, el estado del informe se muestra como cancelado. **Nota:** Es posible que la opción de cancelación no funcione para los trabajos de Warehouse Analytics. debe interrumpir manualmente la tarea. Los siguientes son los pasos necesarios para interrumpir

Columna	Descripción
	la tarea: **Para MapR**: 1. Obtenga el Jobid en los registros de trabajos. 2. Inicie sesión en la interfaz del usuario de jobtracker y busque el Jobid que interrumpirá bajo "Tareas en ejecución". URL de ejemplo: http://<job-tracker-host>:50030/jobtracker.jsp 3. Interrumpa el Jobid: • Seleccione Jobid en "Trabajos en ejecución" y haga clic en Interrumpir trabajos seleccionados. (o) • Haga clic en el vínculo Jobid, desplácese hacia abajo y haga clic en el vínculo Interrumpir este trabajo. **Para Pivotal**: 1. Obtenga el Jobid en los registros de trabajos. 2. Interrumpa el Jobid. Por ejemplo: mapred job -list mapred job -kill job_1406294496331_0385 (o) yarn application -list yarn application -kill application_1406294496331_0385 • Inactivo: si el calendario del informe está desactivado, el estado del informe se muestra como inactivo. • No disponible: si la información de ejecución del calendario del informe no está disponible, el estado del informe se muestra como no disponible.

Columna	Descripción
	Haga clic para ver la información de ejecución y la información de acción de salida. Esta ventana emergente notifica el estado de múltiples reglas en un informe y el tiempo que tardó su ejecución. **Nota:** Puede ver la ejecución de regla y la información de acción de salida de un informe programado que tenga el estado **Finalizada**, **En ejecución**, **Parcial** o **Falla**. De forma predeterminada, la página Acciones de salida para informes finalizados en Configuración de Reporting Engine se establece en habilitar para que se reciba un correo electrónico cuando el estado del informe sea finalizado. Para recibir un correo electrónico para informes con estado **Falla** o **Parcial**, debe deshabilitar esta opción.
Ver informe	Haga clic para ver la información de ejecución de una regla en el Panel Ver un informe. Puede ver la información de ejecución de una regla para un informe programado que también tenga el estado “en ejecución”.

Programador de tareas para Warehouse Reporting

Un programador de tareas en un clúster de hadoop calendariza los trabajos que se componen de tareas y asigna recursos específicos a cada trabajo que se ejecuta en un clúster. De manera predeterminada, el programador de tareas asigna una cantidad igual de recursos a todos los trabajos. Por ejemplo, si hay 10 trabajos ejecutándose, compartirán los recursos del clúster de manera igualitaria. Sin embargo, puede configurar el programador de tareas para controlar la ejecución de trabajos de modo que un trabajo se ejecute de manera más rápida que otros asignando más recursos (pools o líneas de espera) al trabajo. Esto ayuda a priorizar para ejecutar algunos informes por sobre otros.

Características

Security Analytics es compatible con dos programadores de tareas:

- Fair Scheduler (`org.apache.hadoop.mapred.FairScheduler`)
- Capacity Scheduler (`org.apache.hadoop.mapred.CapacityTaskScheduler`)

Fair Scheduler

Este programador divide la capacidad total del clúster en pools lógicos. Puede enviar un trabajo a cualquiera de estos pools. Todos los trabajos enviados a un pool comparten únicamente los recursos asignados al pool. Una vez que un pool cuenta con recursos libres, los recursos liberados se entregan a otros pools con trabajos en ejecución. Por ejemplo, un programador justo tiene el 100 % de los recursos con dos pools, específicamente Pool A y Pool B, que comparten los recursos totales con un 40 % y 60 % respectivamente. Si Pool A cuenta con cuatro trabajos en ejecución, asigna el 10 % de los recursos a cada trabajo. Cuando se completan cuatro trabajos, los recursos liberados se asignan al Pool B.

Nota: Puede configurar un pool para ejecutar más de un trabajo en paralelo.

Capacity Scheduler

Este programador divide la capacidad total del clúster en líneas de espera. A cada línea de espera se le asigna una parte preconfigurada de la capacidad total. Se puede enviar un trabajo a cualquiera de estas líneas de espera. Si se envía más de un trabajo a la misma línea de espera, los trabajos se ejecutarán de manera secuencial. Por ejemplo, si un analizador de capacidad tiene el 100 % de los recursos con tres líneas de espera, específicamente Predeterminada, Baja y Alta, que comparten los recursos totales con 20 %, 30 % y 50 % respectivamente. Si Predeterminada tiene dos trabajos, D1 y D2, Baja tiene tres trabajos, L1, L2 y L3, y Alta tiene cuatro trabajos, H1, H2, H3 y H4, estos trabajos se ejecutan en sus líneas de espera respectivas de manera secuencial. Si se completan los trabajos de una línea de espera, los recursos liberados no se distribuirán a otras líneas de espera.

Vista Crear informe

La vista Crear informe permite crear un informe, calendarizarlo y agregar texto y reglas. Los procedimientos asociados se proporcionan en Agregar un informe y Requisitos previos

Para acceder a esta vista:

1. En el menú de Security Analytics, haga clic en **Administration > Informes**.

   Se muestra la pestaña Administrar.

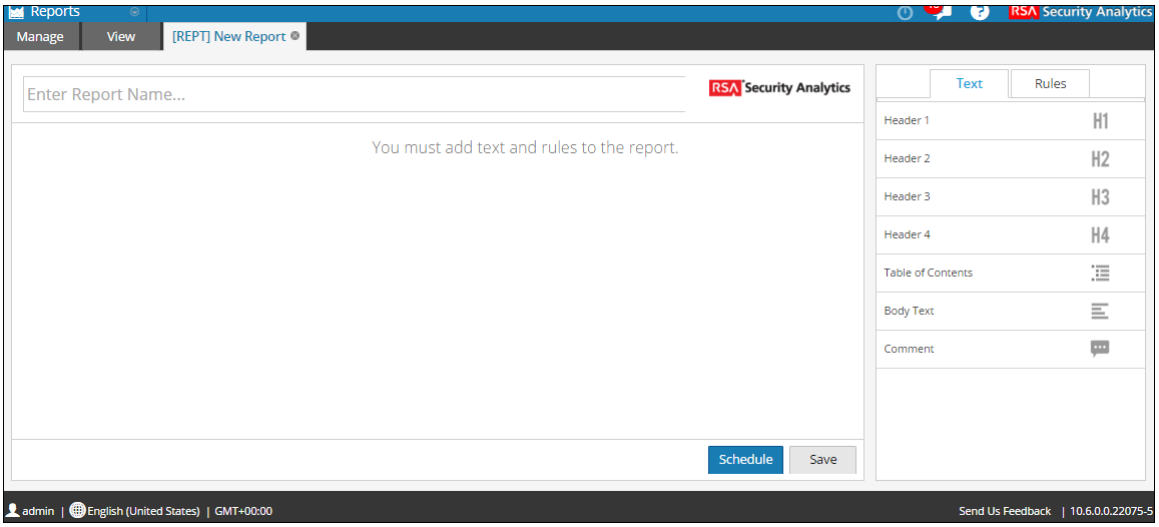
2. Haga clic en **Informes**.

   Se muestra la vista Informe.

3. En la barra de herramientas **Informe**, haga clic en  .

   Aparece la pestaña Crear informe.

La siguiente figura es un ejemplo de la vista Crear informe.

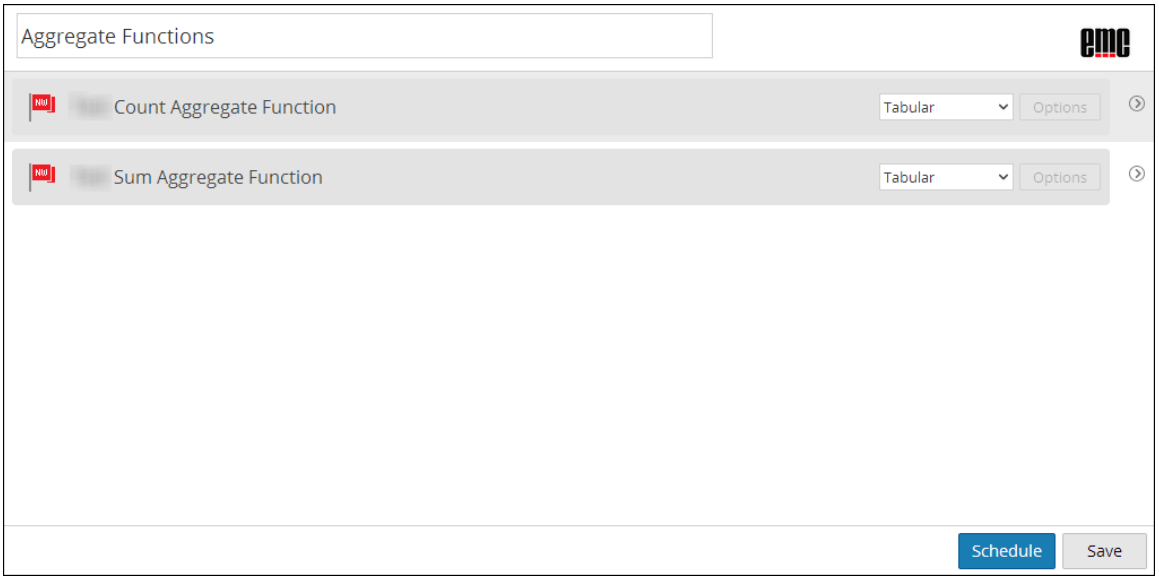


La vista Crear informe se compone de los siguientes paneles:

- Informe
- Texto
- Reglas

Panel Informe

El panel Informe permite crear un informe, para lo cual debe asignarle un nombre. El contenido de un informe depende de los elementos seleccionados en los paneles Texto y Reglas.



Cuando agrega reglas a un informe, puede cambiar el formato de salida de estas reglas a tabular, de áreas, de líneas o circular si hace clic en el botón ⌄.

En la siguiente tabla se indican las funciones del panel Informes y su descripción.

Característica	Descripción
Nombre	Este campo le permite ingresar el nombre del informe.
Opciones	Este campo le permite seleccionar el formato de salida del informe, como tabular, área, barra, burbujas, columna, línea, circular, línea escalonada, área escalonada, área de spline y spline.
Calendario	Cuando hace clic en esta opción, se genera el informe.
Guardar	Cuando hace clic en esta opción, se guarda el informe.

Panel Texto

El panel Texto consta de una lista de elementos de texto que complementan la apariencia del informe. Puede usar estos elementos de texto para formatear el informe.

- Para agregar más estructura a informes, puede usar estos encabezados definidos en el panel Texto para modificar hasta cuatro niveles. Esto le permite identificar secciones específicas de un informe que se pueden incluir en la tabla de contenido para una navegación sencilla en el resultado de informe.
- Para agregar encabezados en el panel Informe, arrastre y suelte H1, H2, H3 o H4 en el panel Informe basado en el nivel deseado de modificación.

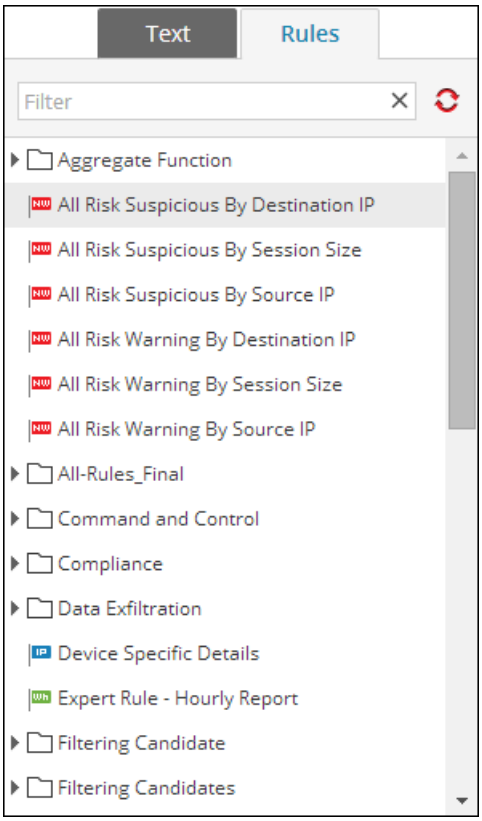
La siguiente tabla enumera los elementos de texto utilizados para formatear un informe:

Elementos de texto	Descripción
Encabezado 1 H1	El elemento Encabezado 1 agrega un encabezado en el primer nivel de la definición del informe.
Encabezado 2 H2	El elemento Encabezado 2 agrega un encabezado en el segundo nivel de la definición del informe.
Encabezado 3 H3	El elemento Encabezado 3 agrega un encabezado en el tercer nivel de la definición del informe.
Encabezado 4 H4	El elemento Encabezado 4 agrega un encabezado en el cuarto nivel de la definición del informe.
Tabla de contenido	La Tabla de contenido agrega una tabla de contenido a la definición del informe.
Texto del cuerpo	El elemento Texto del cuerpo agrega texto del cuerpo a la definición del informe.
Comentario	El elemento Comentario agrega comentarios a la definición del informe. **Nota:** El elemento Comentario no se muestra cuando ve todos los informes.

Panel Reglas

El panel Reglas consta de una lista de reglas que se definen en el panel Reglas. Desde la lista de reglas, puede arrastrar y soltar reglas en el panel Informe para asociarlas al informe.

Puede buscar una regla específica mediante el cuadro de texto de búsqueda que se proporciona en el panel Reglas.



En la siguiente tabla se indican las funciones del panel Reglas y su descripción.

Característica	Descripción
Texto	Esta opción le permite seleccionar los elementos de texto que puede usar para formatear un informe:
Reglas	Esta opción le permite seleccionar la regla que desea usar para crear el informe.

Cuadro de diálogo Importar informe

En este tema se describen las funciones de la vista Crear informe. En este cuadro de diálogo, puede importar grupos que contienen subgrupos e informes de otras instancias de Security Analytics en el panel Grupos de informes. Los informes deben estar en un archivo binario válido que se haya exportado desde otra instancia de Security Analytics.

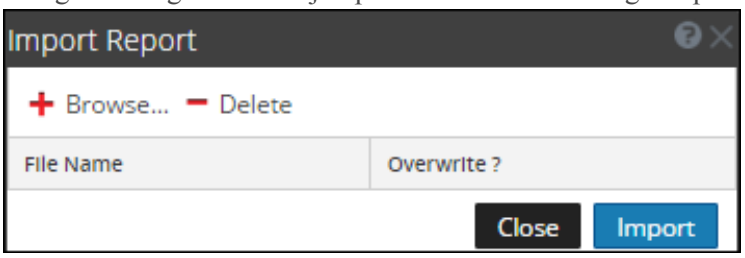
Los procedimientos relacionados con este cuadro de diálogo se describen en Importar informes y grupos de informes.

Para acceder al cuadro de diálogo:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Informes**.
   Se muestra la vista Informe.
3. En el panel **Grupos de informes**, seleccione una carpeta para importar el archivo.
4. Realice una de las siguientes acciones

   - En el panel **Grupos de informes**, haga clic en  > **Importar** para importar un grupo.
   - En la barra de herramientas **Informe**, haga clic en  > **Importar** para importar un informe.

La siguiente figura es un ejemplo del cuadro de diálogo Importar informe.



Característica	Descripción
Examinar	Esta opción muestra una vista del sistema de archivos local para que pueda seleccionar el informe que desea importar.
Delete	Esta opción elimina un informe importado de la lista de informes importados.
Nombre de archivo	Muestra una lista de archivos de informes que se importarán al módulo Informes cuando hace clic en Importar.
¿Sobrescribir?	Le permite seleccionar la opción para sobrescribir una versión existente del informe que se va a importar. Si no selecciona la opción de sobrescritura, se importa un archivo duplicado y no se muestra ningún mensaje de error.

Característica	Descripción
Cerrar	Esta opción cierra el cuadro de diálogo. Si tiene informes para seleccionar para importación, pero no ha hecho clic en Importar. Los informes nose importan y no se guardan en este cuadro de diálogo.
Importar	Esta opción importa los informes seleccionados al módulo Informes.

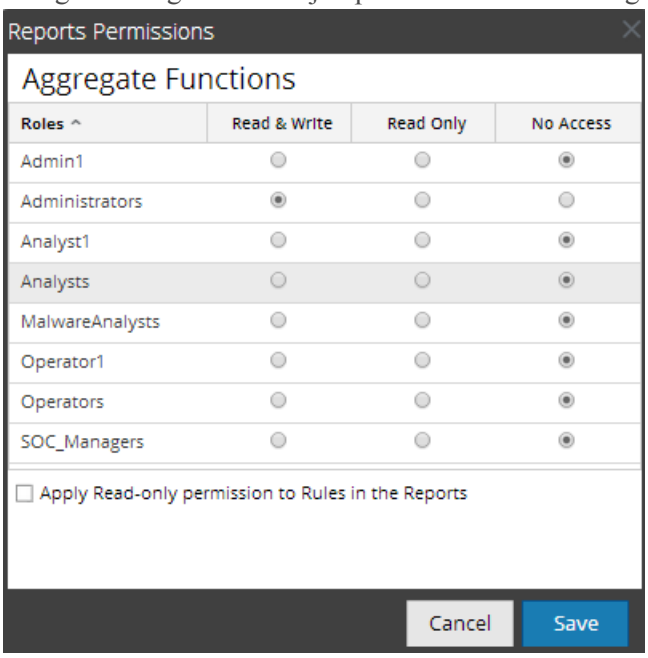
Cuadro de diálogo Permisos de informes

En este tema se describen las funciones del cuadro de diálogo Permisos de informes. Los usuarios que tienen permiso de acceso de "Lectura y escritura" para configurar permisos de acceso para un informe pueden configurar los permisos en el cuadro de diálogo Permisos de informes. Los procedimientos asociados se proporcionan en Administrar el acceso para un informe o un grupo de informes

Para mostrar el cuadro de diálogo Permisos de informes:

1. En el menú de Security Analytics, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Informes**.
   Se muestra la vista Informe.
3. En el panel **Lista de informes**, seleccione un informe.
4. Haga clic en  > **Permisos**.
   Aparece el cuadro de diálogo Permisos de informes.

La siguiente figura es un ejemplo del cuadro de diálogo Permisos de informes.



Nota: Cuando se selecciona la casilla de verificación, se otorga permiso de acceso de LECTURA a todas las reglas dependientes, siempre que los permisos para el informe sean más altos que los permisos de las reglas.

En la siguiente tabla se describen las funciones del cuadro de diálogo Permisos de informes.

Característica	Descripción
Funciones	Muestra todas las funciones que pueden obtener acceso a los permisos.
Lectura y escritura	Le permite obtener acceso de lectura y escritura a las reglas en los informes.
De solo lectura	Le permite obtener permisos de solo lectura a las reglas en los informes.
Sin acceso	Si selecciona esta opción, no obtendrá permiso para las reglas en los informes.
Aplicar permisos de solo lectura a las reglas de los informes	Permite configurar permisos de solo lectura a las reglas en los informes para todas las funciones.

Característica	Descripción
Cancelar	Esta opción cancela todos los cambios realizados a los permisos.
Guardar	Esta opción guarda las selecciones y proporciona acceso a las funciones de acuerdo con las selecciones.

Vista Informe

La vista Informe permite crear y organizar grupos de informes. Los procedimientos asociados con esta vista se proporcionan en Definir grupos de informes e informes.

En este panel puede realizar las siguientes acciones:

- Actualizar una lista de grupos o informes.
- Agregar un grupo de informes.
- Eliminar un grupo de informes.
- Importar informes y grupos de informes.
- Exportar un grupo de informes.
- Establecer permisos de acceso para un grupo de informes.

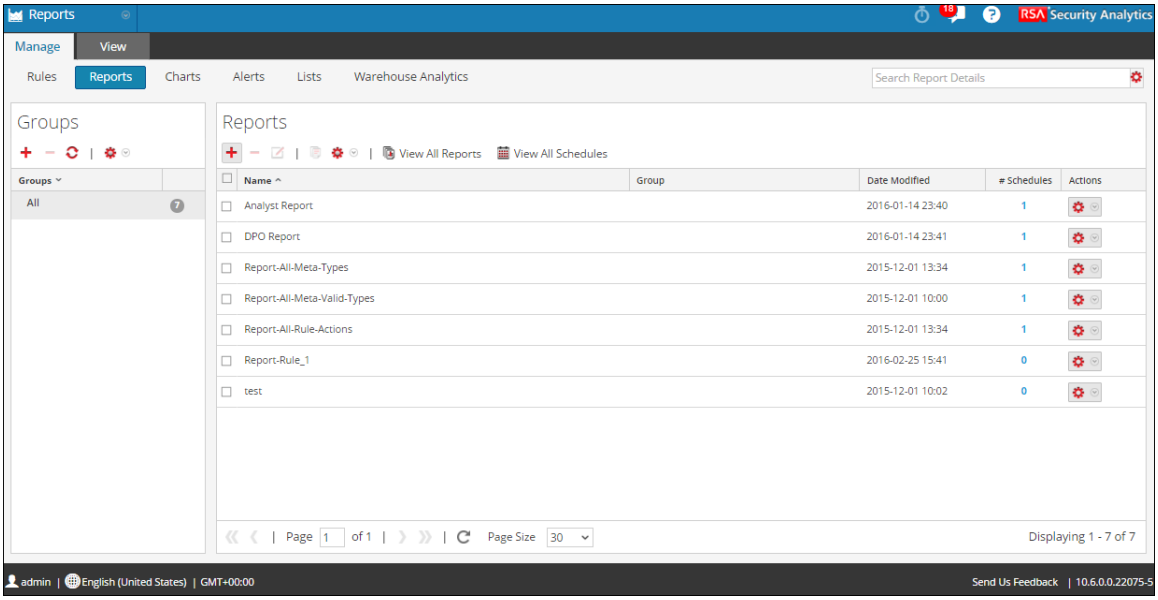
La barra de herramientas tiene las siguientes opciones:

- Agregar un informe
- Editar un informe
- Eliminar un informe
- Duplicar un informe
- Importar informes y grupos de informes
- Exportar un informe
- Establecer el control de acceso para un informe
- Requisitos previos
- Requisitos previos

Para acceder a esta vista:

1. En el menú de Security Analytics, haga clic en Administration > Informes.
   Se muestra la pestaña Administrar.
2. Haga clic en **Informes**.
   Se muestra la vista Informe.

En la siguiente figura se muestran los diferentes paneles de la vista Informe.



Características

La vista Informe incluye las siguientes secciones:

- Panel Grupos de informes
- Barra de herramientas Informe
- Panel Lista de informes

Panel Grupos de informes

El panel Grupos de informes permite organizar informes en un grupo. Puede crear un grupo de informes, agregar informes al grupo y transferir informes entre grupos. Puede ver todos los informes si selecciona la opción Todo bajo la columna Grupos.

Característica	Descripción

	Esta opción le permite agregar un nuevo informe al módulo Reporting.
	Esta opción le permite eliminar uno o más informes seleccionados.
	Esta opción actualiza la vista.
	El menú Acciones tiene las siguientes opciones: Importar, exportar y permisos.

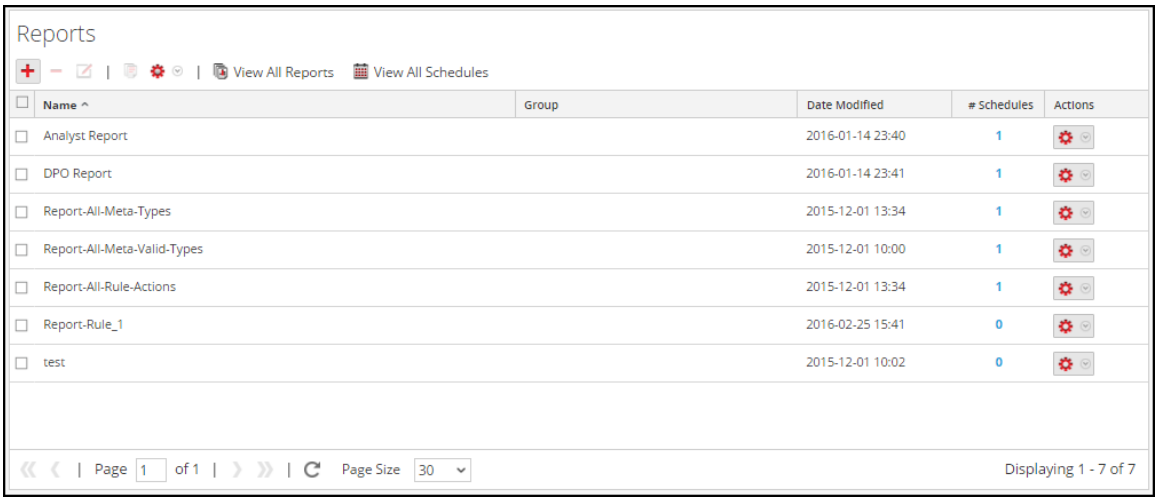
Barra de herramientas Informe

La barra de herramientas Informe permite agregar, modificar, eliminar, duplicar, importar y exportar informes. También puede establecer permisos de acceso para un informe en un grupo.

Característica	Descripción
	Esta opción le permite agregar un nuevo informe al módulo Reporting.
	Esta opción le permite eliminar uno o más informes seleccionados.
	Esta opción le permite editar un gráfico.
	Esta opción crea una copia duplicada del informe seleccionado.
	El menú Acciones tiene las siguientes opciones: Importar, exportar y permisos.

Panel Lista de informes

El panel Lista de informes muestra todos los informes en formato tabular.



En la siguiente tabla se describen las columnas del panel Lista de informes.

Columna	Descripción
Nombre	Es el nombre del informe.
Grupo	Grupo de informes al cual pertenece el informe.
Fecha de modificación	La fecha y la hora en que se modificó el informe.
N.º de calendarios	El conteo indica la cantidad de calendarios creados para un informe.
Acciones	El menú Acciones tiene las siguientes opciones: Calendarizar informe, ver informes calendarizados, eliminar, editar y exportar.

Referencias de calendarios

La interfaz del usuario del módulo Reporting proporciona acceso a los informes programados de Security Analytics. En este tema hay descripciones de la interfaz del usuario, además de otra información de referencia, para ayudar a los usuarios a programar informes.

Temas

- Características
- Características
- Características

- Características
- Características

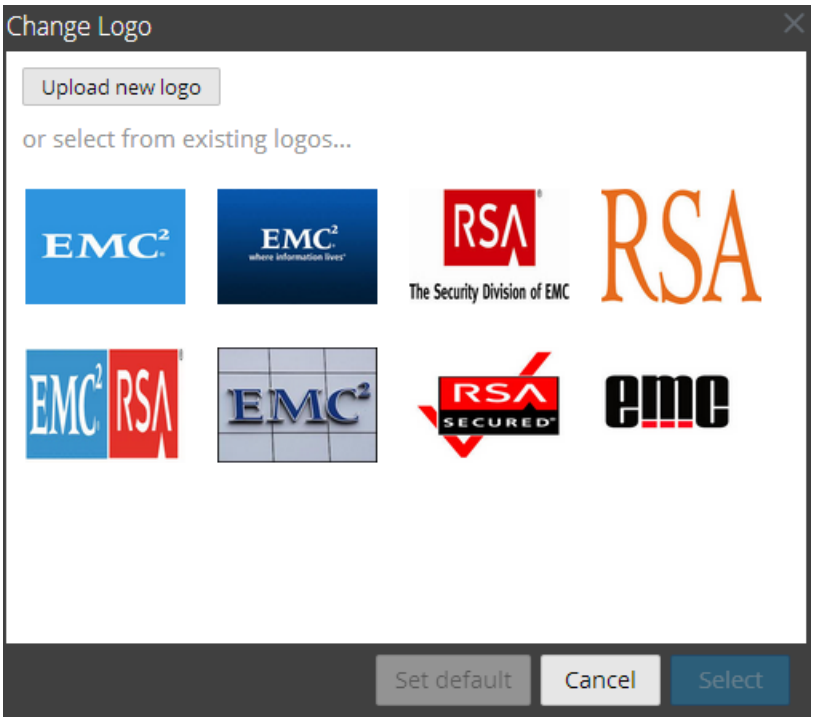
Cuadro de diálogo Seleccionar un logotipo

El cuadro de diálogo Seleccionar un logotipo permite cargar un nuevo logotipo que no está disponible en la vista Configuración de servicios de Reporting Engine o elegir un logotipo existente en la vista Configuración de servicios de Reporting Engine. Los procedimientos asociados con esta vista se describen en Seleccionar un logotipo.

Para acceder a este cuadro de diálogo:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Informes**.
   Se muestra la vista Informe.
3. En el panel **Lista de informes**, seleccione un informe.
4. Haga clic en  > **Ver informes calendarizados**.
   Se muestra la pestaña de la vista Ver informes calendarizados.
5. Seleccione un informe programado y haga clic en  > **Editar calendario**.
   Se muestra la pestaña de la vista Programar un informe.
6. Haga clic en el panel **Logotipo**.
   Se abre el cuadro de diálogo Cambiar un logotipo.

La siguiente figura es un ejemplo del cuadro de diálogo Seleccionar un logotipo.



En la siguiente tabla se indican los campos del cuadro de diálogo Seleccionar un logotipo.

Campo	Descripción
Cargar nuevo logotipo	Haga clic en el ícono para cargar un nuevo logotipo desde el directorio local.
Seleccionar	Seleccione un logotipo en la lista existente para usar como logotipo en el informe calendarizado.
Cancelar	Cancela la selección del logotipo y vuelve al panel Programar un informe.
Establecer valor predeterminado	Seleccione un logotipo para configurar como el logotipo predeterminado.

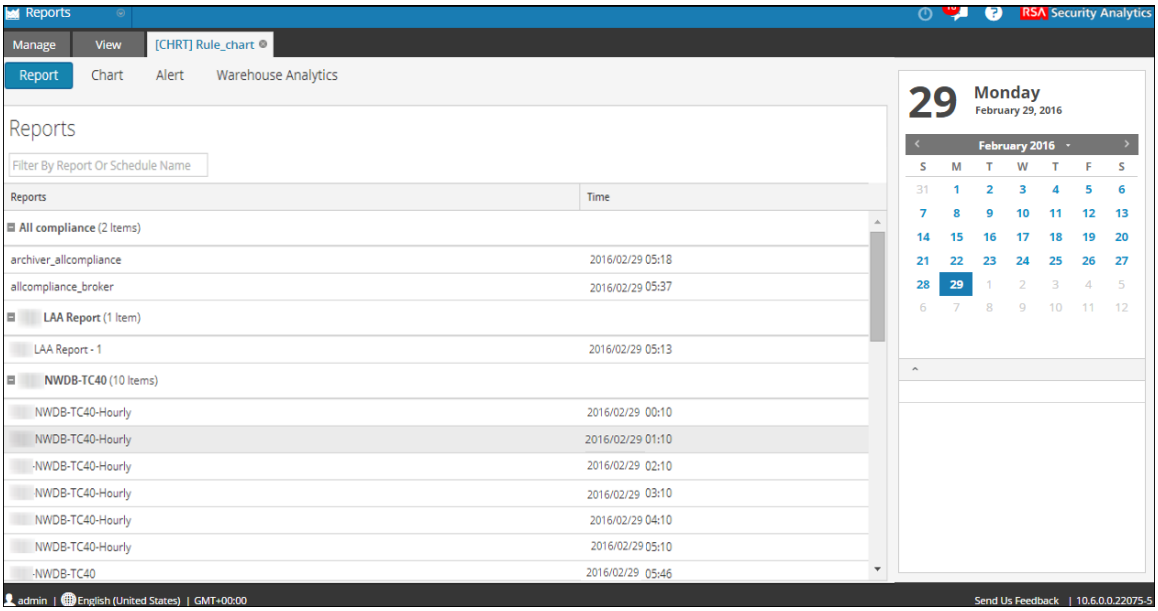
Panel Ver todos los informes

La vista Ver todos los informes le permite mostrar, imprimir, guardar y enviar informes por correo electrónico. Los procedimientos asociados a esta vista se describen en Ver una lista de todos los informes.

Para acceder a esta vista:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Informes**.
   Se muestra la vista Informe.
3. En el panel **Informe**, haga clic en **Ver todos los informes**.

En la siguiente figura se muestra un ejemplo de este panel.



Características

El panel Ver todos los informes incluye las siguientes funciones:

- Barra de herramientas Informes
- Salida de informes
- Calendario de informes
- Hora de informes

En la siguiente tabla se indican las opciones de la barra de herramientas Ver todos los informes:

Operation	Descripción
Filter By Report Or Schedule Name	Busca calendarios en función del nombre del calendario o del informe para un día calendario seleccionado.

Haga clic en cualquiera de los informes mostrados para verlo.

Barra de herramientas Informes

La barra de herramientas Informes permite imprimir, guardar, enviar por correo electrónico y ver informes en pantalla completa.

Nota: Reporting Engine es el responsable de generar una salida en formato PDF y CSV de los informes, según la definición del informe. El tamaño de los archivos PDF de un informe no debe superar las 50,000 celdas.

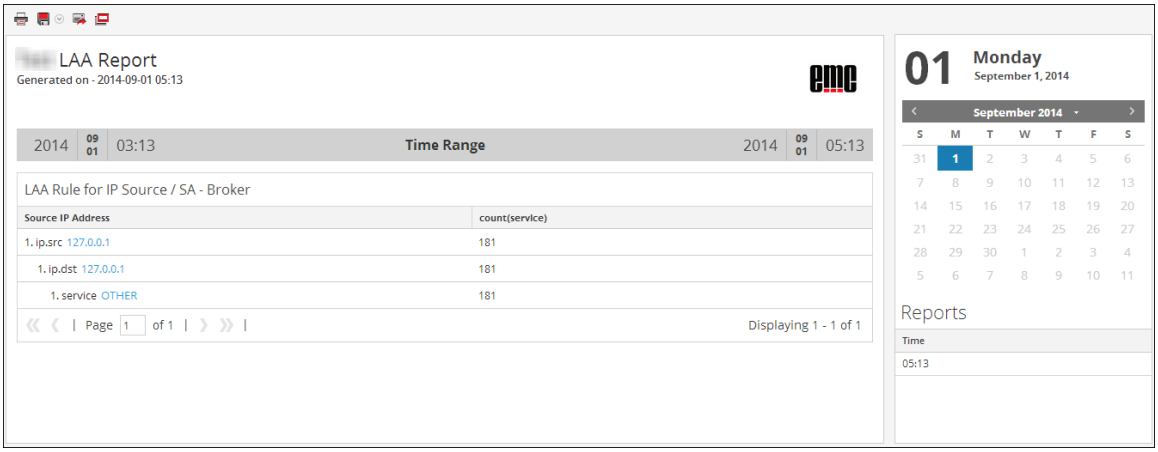
En la siguiente tabla se indican las opciones de la barra de herramientas Informes.

Operation	Descripción
	Imprime el informe generado.
	Guarda el informe como un archivo PDF y CSV. **Nota:** La opción **Guardar como PDF** no está disponible para un informe grande. Si la generación de un archivo PDF de un informe tarda más de lo previsto, se muestra un mensaje de advertencia que señala **La generación del archivo PDF está en curso; inténtelo más adelante**. Cuando hace clic en la opción para descargar como un archivo CSV, se muestra el cuadro de diálogo Seleccionar regla para descargar. Debe seleccionar una regla en este cuadro de diálogo para descargar su resultado en un archivo CSV. Si la generación del archivo tarda, puede hacer clic en la opción **Notificarme** para que se le informe cuando el archivo PDF o CSV se haya generado. Tras la generación del archivo PDF o CSV, puede ver el estado en Notificaciones.
	Envía el informe por correo electrónico con el archivo PDF o CSV adjunto.

Operation	Descripción
	Abre el informe generado en una nueva ventana.

Panel Salida de informes

El panel Salida de informes muestra el informe con el nombre del calendario de informes, la hora de generación del informe y el informe real con las variables de regla seleccionadas.



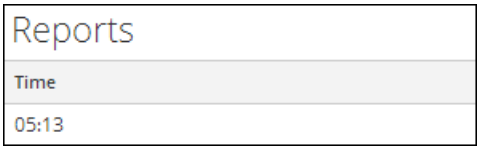
Característica	Descripción
Nombre	Este campo muestra el nombre del informe calendarizado.
Hora	Este campo muestra la hora en que se generó el informe.
Informe	Este campo muestra el informe de detalles con las variables de la regla seleccionada.

Panel Calendario de informes

El panel Calendario de informes se usa para seleccionar una fecha en el calendario. De acuerdo con la fecha que selecciona, se muestra la lista de informes que se ejecutaron correctamente en esa fecha.

Panel Hora de informes

El panel Hora de informes muestra la hora en que se ejecutó realmente el informe.



Panel Ver un informe

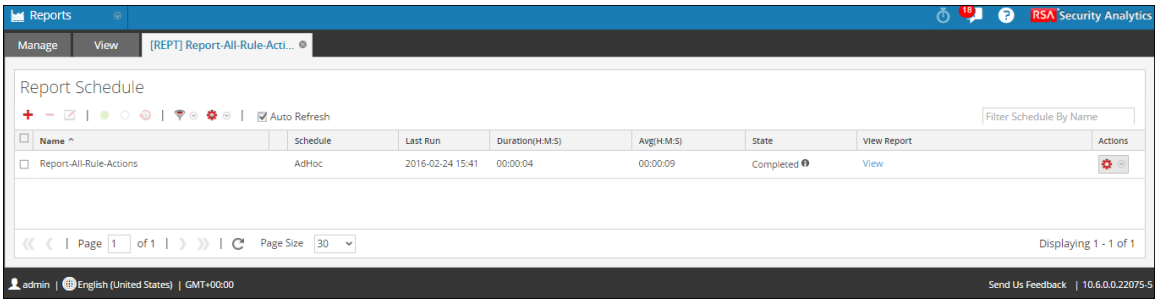
El panel Ver un informe se usa para revisar los informes. El procedimiento asociado a esto se describe en Ver un informe.

Para acceder a esta vista:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Informes**.
   Se muestra la vista Informe.
3. En el panel **Lista de informes**, realice una de las siguientes acciones:

   - Haga clic en  > **Ver informes calendarizados**.
   - Haga clic en la columna **N.º de calendarios**.

En la siguiente figura se muestra la vista Ver informes calendarizados.

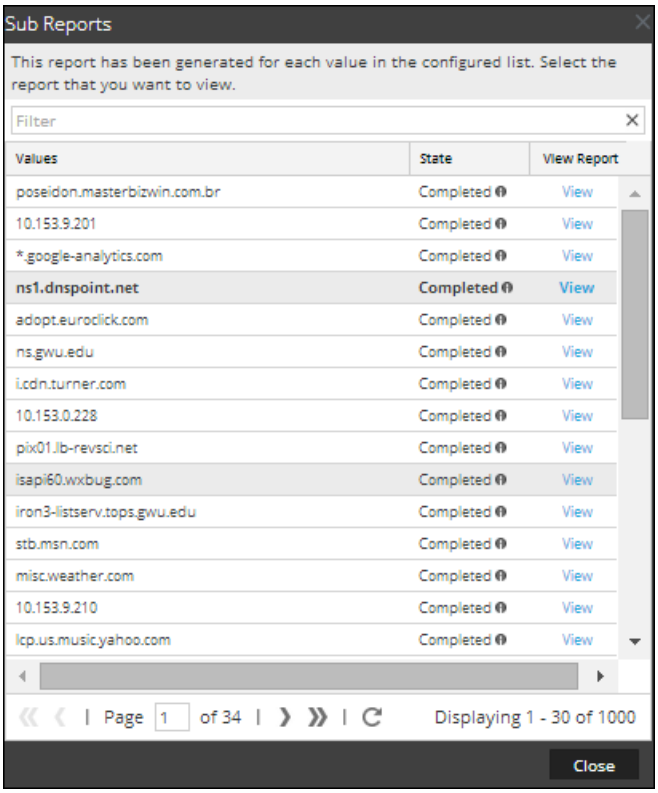


Características

El panel Ver un informe incluye las siguientes secciones:

- Barra de herramientas Informes
- Panel Salida de informes
- Panel Calendario de informes
- Panel Hora de informes

Cuando hace clic en **Ver** en el informe calendarizado que tiene seleccionada la opción **Iterativo**, se muestra el panel **Subinformes**. Se genera un informe para cada valor de la lista configurada.



En la siguiente tabla se indican las columnas del panel Subinformes.

Columna	Descripción
Valores	Los valores de la lista elegidos para una variable dinámica en el panel Selección de lista.
State	Indica el estado del informe calendarizado para cada uno de los valores de la lista. • Parcial: Si en un informe con varias reglas se produce una falla en una única ejecución de regla, en una acción de salida o en la creación de PDF/CSV, el estado del informe se muestra como parcial. Por ejemplo, considere un informe con cinco reglas, de las cuales cuatro se ejecutan correctamente y una falla. En este caso, el estado se muestra como Parcial. • Fallido: si en un informe con varias reglas, todas las ejecuciones de reglas fallan, el estado del informe se muestra como fallido. • Completado: si un informe se ejecuta correctamente, su estado se muestra como finalizado.

Columna	Descripción
Ver	Haga clic en cualquiera de los programas de informes o subinformes enumerados y, a continuación, haga clic en **Ver** para ver el informe deseado. **Nota:** puede ver las reglas completadas en la página **Ver un informe**, incluso mientras el informe se está "ejecutando".

Para obtener más información sobre cada uno de estos paneles, consulte Panel Ver todos los informes.

Referencias de reglas

La interfaz del usuario del módulo Reporting proporciona acceso a reglas de Security Analytics. Este tema contiene descripciones de la interfaz del usuario que pertenecen a reglas definidas para informes y alertas, así como otra información de referencia para ayudar a los usuarios a administrar las reglas.

Temas

- Vista Crear regla
- Agregados de consulta
- Cuadro de diálogo Permisos de regla
- Vista Regla
- Especificación de orígenes de eventos de IPDB
- Modos de definición de reglas de la base de datos de Warehouse
  - Sintaxis general de una regla avanzada
  - Informe Todas las categorías de eventos

Reglas avanzadas de la base de datos de Warehouse

En este tema se proporcionan ejemplos de reglas de origen de datos de Warehouse. Puede definir reglas de base de datos de Warehouse mediante consultas de HIVE. Puede definir reglas simples y avanzadas para el origen de datos de Warehouse mediante los siguientes modos:

- Modo Predeterminado
- Modo experto

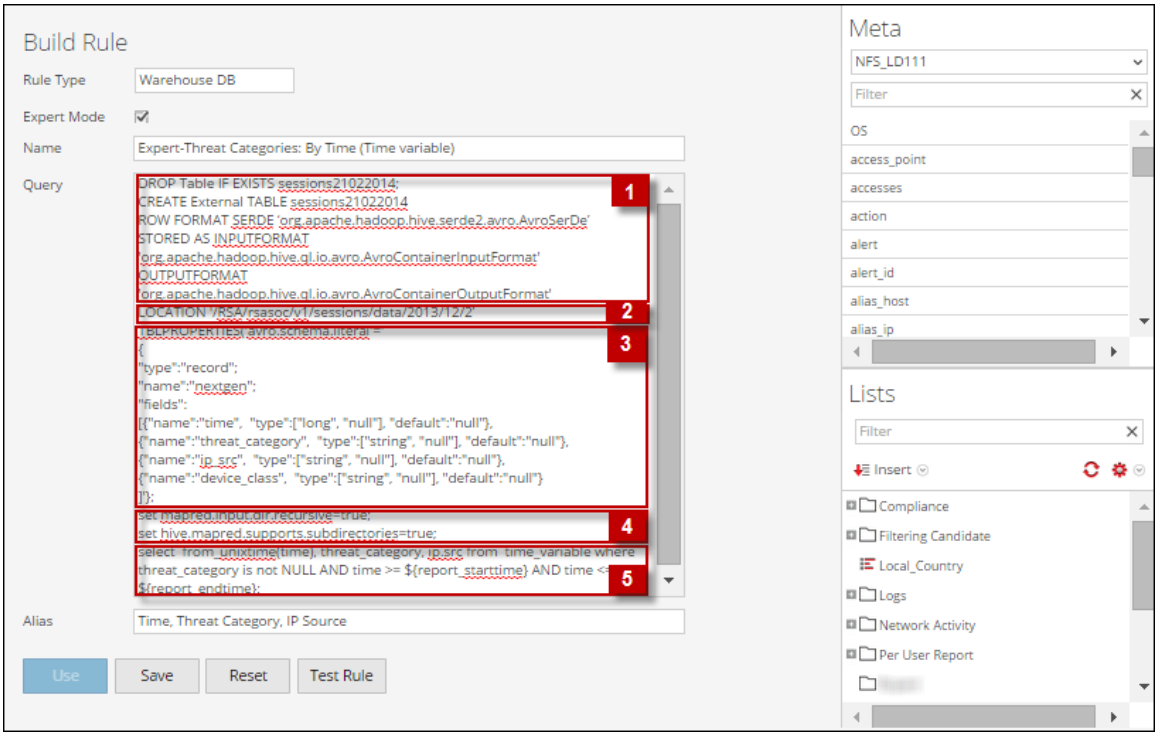
Las reglas avanzadas se definen mediante consultas HIVE complejas que se crean con las cláusulas DROP, CREATE, etc. A diferencia de las reglas simples, los resultados se insertan siempre en una tabla. Para obtener más información sobre el lenguaje de consulta HIVE avanzado, consulte Manual de lenguaje HIVE.

En los siguientes ejemplos se ilustran las reglas avanzadas en el modo experto:

- Informe por hora, diario, semanal y mensual
- Partición de la tabla basada en informe de ubicación
- Registros de combinación y sesiones basados en informe unique_id
- Informe de lista
- Informe con parámetros
- Tabla basada en partición con varias ubicaciones
- Partición automatizada mediante función personalizada (10.5.1 en adelante)

Sintaxis general de una regla avanzada

En la figura siguiente se muestra cómo definir una consulta avanzada.



La siguiente sintaxis es un ejemplo de una consulta avanzada:

```
DROP Table IF EXISTS sessions21022014;
```

```
CREATE External TABLE sessions21022014
ROW FORMAT SERDE 'org.apache.hadoop.hive.serde2.avro.AvroSerDe'
STORED AS INPUTFORMAT
'org.apache.hadoop.hive.ql.io.avro.AvroContainerInputFormat'
 OUTPUTFORMAT
'org.apache.hadoop.hive.ql.io.avro.AvroContainerOutputFormat'
LOCATION '/RSA/rsasoc/v1/sessions/data/2013/12/2'
TBLPROPERTIES('avro.schema.literal'='
 {
"type":"record";
"name":"nextgen";
"fields":
 [
 {"name":"time",  "type":["long", "null"], "default":"null"},
{"name":"threat_category",  "type":["string", "null"],
"default":"null"},
{"name":"ip_src",  "type":["string", "null"], "default":"null"},
{"name":"device_class",  "type":["string", "null"], "default":"null"}
 ]
 '};
set mapred.input.dir.recursive=true;
 set hive.mapred.supports.subdirectories=true;
```

seleccione `from_unixtime(time), threat_category, ip.src` desde `time_variable` , donde `threat_category` no es `NULL` y `time >= ${report_starttime}` y `time <= ${report_endtime};`

Nota: Reporting Engine considera como comentario una línea que comienza con <guion> <guion> en una regla de Expert Warehouse.
Por ejemplo,

```
set mapred.input.dir.recursive=true;
-- This is an Expert comment
 set hive.mapred.supports.subdirectories=true;
```

A continuación se explica la sintaxis general de una consulta avanzada:

1. Desplegar y crear una tabla externa, y luego formatear la fila:
   Primero, la tabla se descarta si ya existe y se crea una tabla externa **sessions21022014**

   ```
   DROP TABLE IF EXISTS sessions21022014
    CREATE EXTERNAL TABLE sessions21022014
   ```

Nota: Solo debe crear una tabla externa si usa otra tabla. Por ejemplo, si usa otra tabla además de **sessions21022014**, debe descartar la tabla y crear una tabla externa.

A continuación, especifique el formato de fila como interfaz Avro.SerDe para instruir a HIVE en cuanto a cómo procesar un registro. Avro.SerDe le permite leer o escribir datos Avro como tablas HIVE y almacenarlos como formato de entrada y formato de salida.

```
ROW FORMAT SERDE 'org.apache.hadoop.hive.serde2.avro.Avro.SerDe'
 STORED AS INPUTFORMAT
'org.apache.hadoop.hive.ql.io.avro.AvroContainerInputFormat'
 OUTPUTFORMAT
'org.apache.hadoop.hive.ql.io.avro.AvroContainerOutputFormat'
```

2. Especificar la ubicación de HDFS:
   En segundo lugar, debe especificar la ubicación de HDFS "/RSA/rsasoc/v1/sessions/data/2013/12/2" desde donde se consultan los datos antes de ejecutar las declaraciones HIVE. El parámetro de ubicación especifica los datos que se van a buscar en función de la entrada de fecha proporcionada. Este es un parámetro variable, por tanto, se puede buscar valores en función de la fecha introducida.
3. Definir el esquema de la tabla:
   En tercer lugar, defina el esquema de la tabla mediante la definición de columnas con un tipo de datos específico y el valor predeterminado como "nulo".

```
TBLPROPERTIES('avro.schema.literal'='
 {"type":"record";
 "name":"nextgen";
 "fields":
 [
 {"name":"ip_src",  "type":["string", "null"], "default":"null"}
 ]
 '};
```

4. Importar datos de un directorio que contiene subdirectorios:
   A continuación, debe permitir que HIVE escanee recurrentemente todos los subdirectorios y busque todos los datos de todos los subdirectorios.

```
set mapred.input.dir.recursive=true;
 set hive.mapred.supports.subdirectories=true;
```

5. Buscar datos de la tabla HIVE:
   Una vez que ejecute todas las declaraciones anteriores, puede consultar la base de datos con la cláusula **select** de la consulta HIVE para buscar los datos de la tabla HIVE.

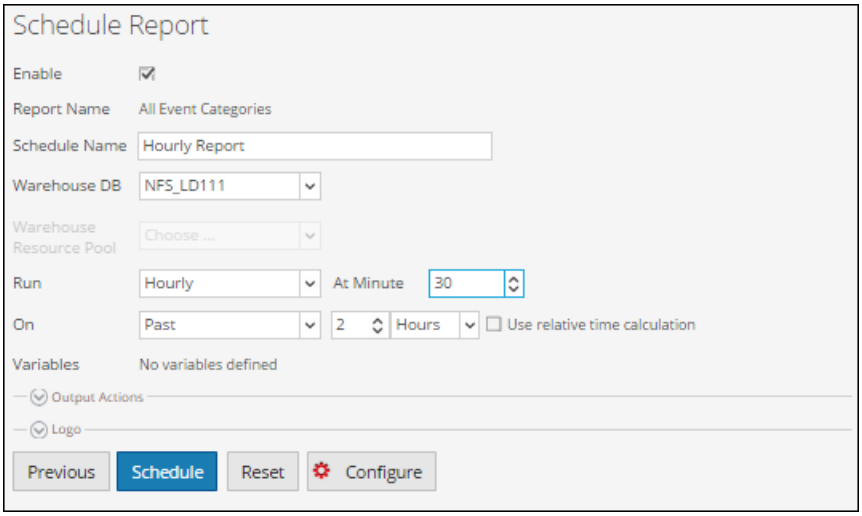
Informe por hora, diario, semanal y mensual

En estas reglas de ejemplo, puede crear varios informes para 2 de diciembre de 2013 (como en la figura de abajo). La variable de fecha en la declaración LOCATION puede modificarse, según lo cual puede crear un informe por hora, diario, semanal y mensual.

Informes por hora

En esta regla de ejemplo, puede crear un informe por hora para 2 de diciembre de 2013. La declaración LOCATION se puede modificar para generar un informe por hora

LOCATION '/RSA/rsasoc/v1/sessions/data/2013/12/2' : la entrada de fecha (2013/12/2) indica año/mes/día. La totalidad de los datos correspondiente a 2 de diciembre de 2013 se recupera con esta declaración de ubicación.

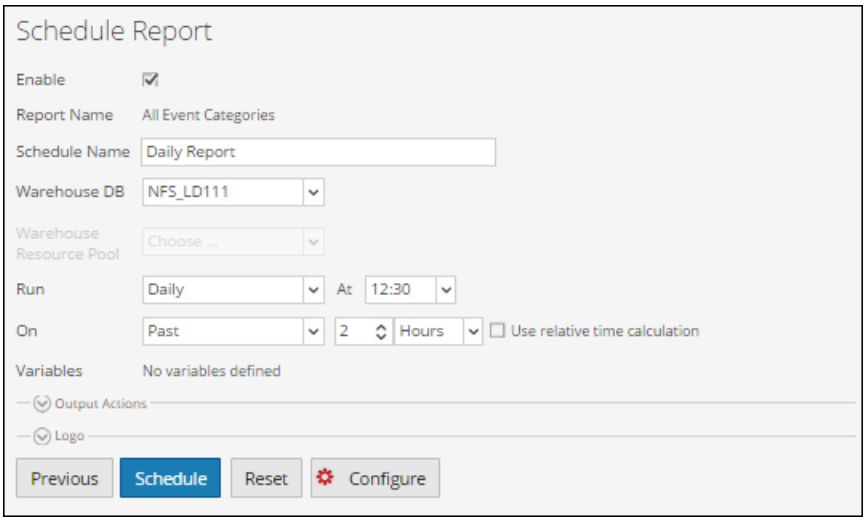


El conjunto de resultados de esta consulta será un informe por hora.

Informe diario

En esta regla de ejemplo, puede crear un informe diario para diciembre de 2013. La declaración LOCATION se puede modificar para generar un informe diario.

LOCATION '/RSA/rsasoc/v1/sessions/data/2013/12': la entrada de fecha (2013/12) indica año/mes. La totalidad de los datos correspondiente a diciembre de 2013 se recupera con esta declaración de ubicación.

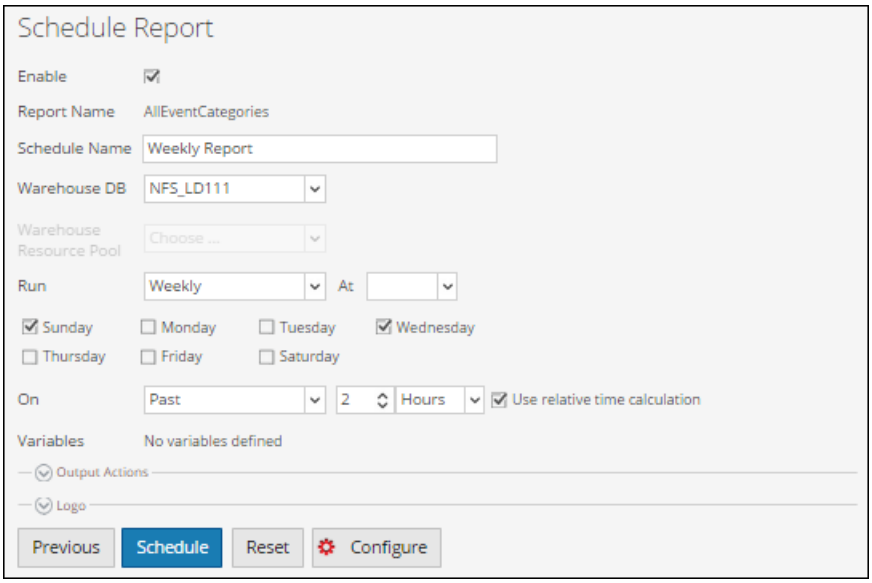


El conjunto de resultados de esta consulta será un informe diario.

Informe semanal

En esta regla de ejemplo, puede crear un informe semanal para diciembre de 2013. La declaración LOCATION se puede modificar para generar un informe semanal.

LOCATION '/RSA/rsasoc/v1/sessions/data/2013/12': la entrada de fecha (2013/12) indica año/mes. La totalidad de los datos correspondiente a diciembre de 2013 se recupera con esta declaración de ubicación.

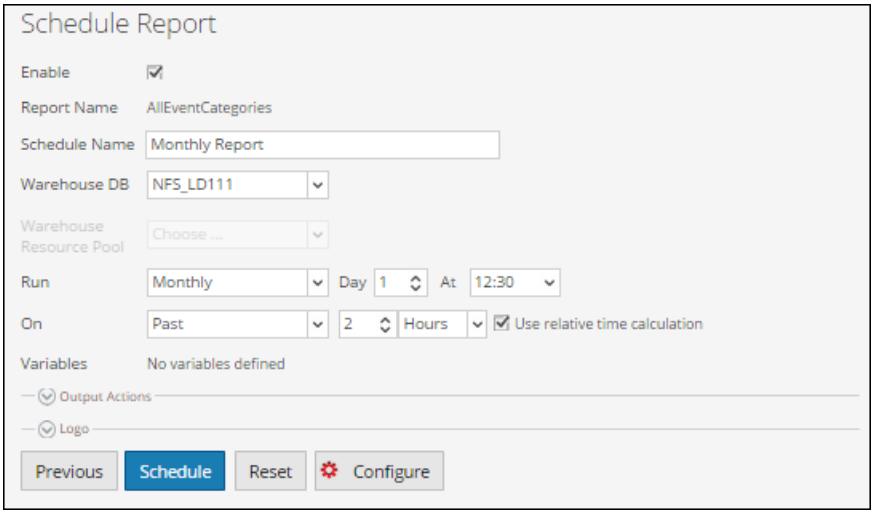


El conjunto de resultados de esta consulta será un informe semanal.

Informe mensual

En esta regla de ejemplo, puede crear un informe mensual para el año 2013. La declaración LOCATION se puede modificar para generar un informe mensual.

LOCATION '/RSA/rsasoc/v1/sessions/data/2013' : la entrada de fecha (2013) indica el año. La totalidad de los datos correspondiente al año 2013 se recupera con esta declaración de ubicación.



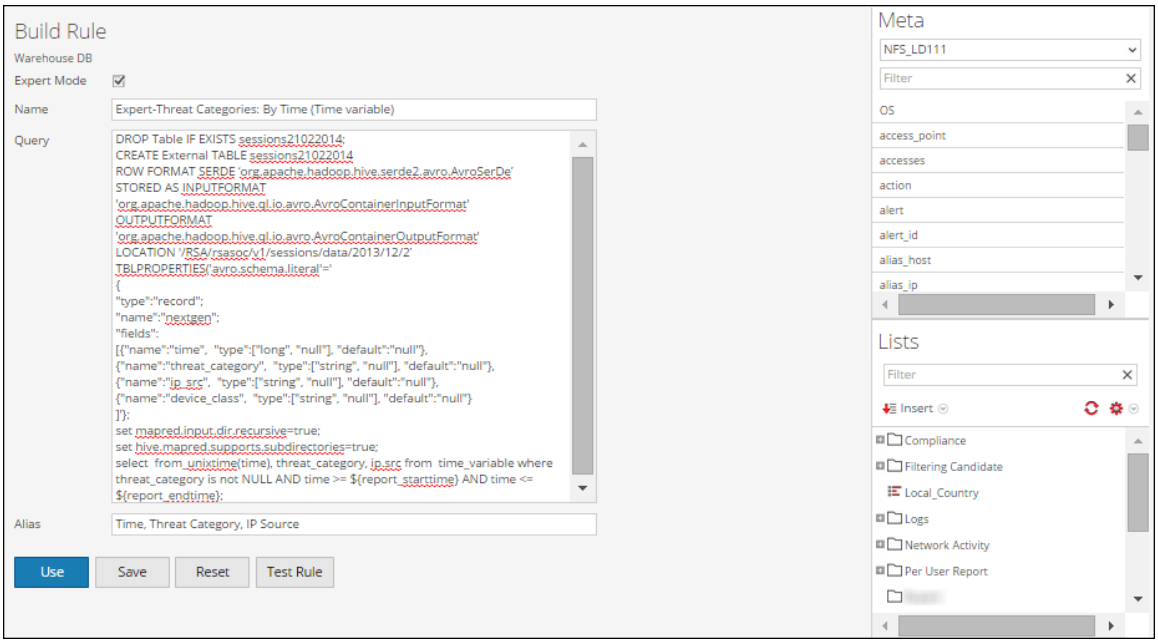
El conjunto de resultados de esta consulta será un informe mensual.

Para obtener más información sobre la definición de LOCATION, consulte **Especificar la ubicación de HDFS** en la sección **Sintaxis general de una regla avanzada**.

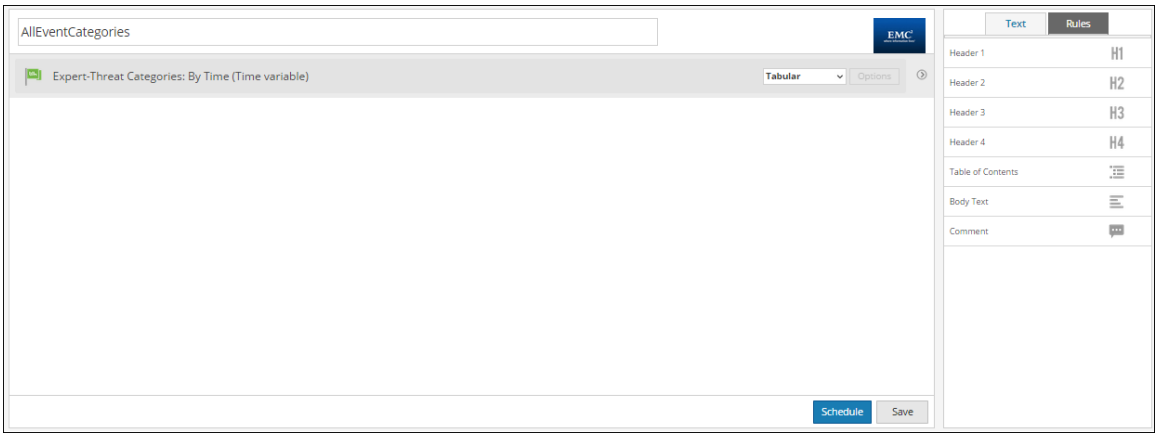
Debe realizar los siguientes pasos en secuencia para ver el conjunto de resultados de una regla avanzada:

1. Definir una regla avanzada
2. Agrega una regla avanzada a un informe
3. Programar un informe
4. Ver un informe programado

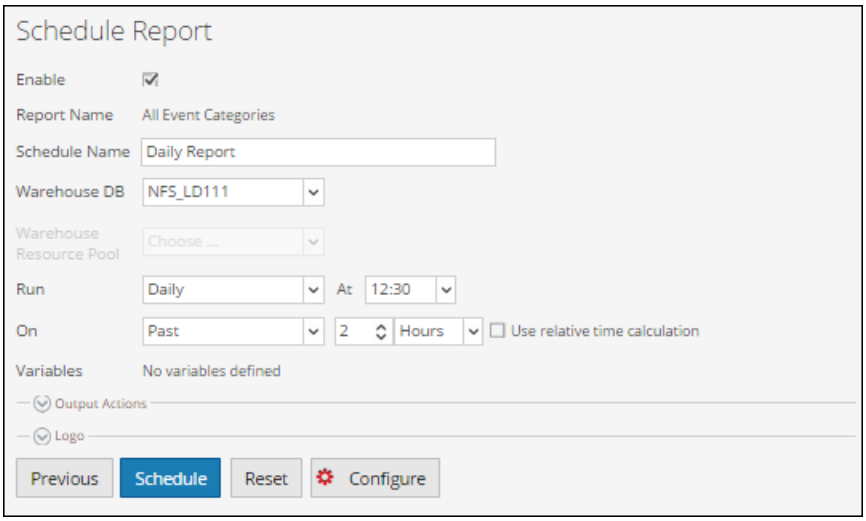
En la figura siguiente se muestra cómo definir una regla avanzada.



En la figura siguiente se muestra cómo agregar una regla avanzada a un informe (por ejemplo, **AllEventCategories**).



En la figura siguiente se muestra cómo programar un informe diario.

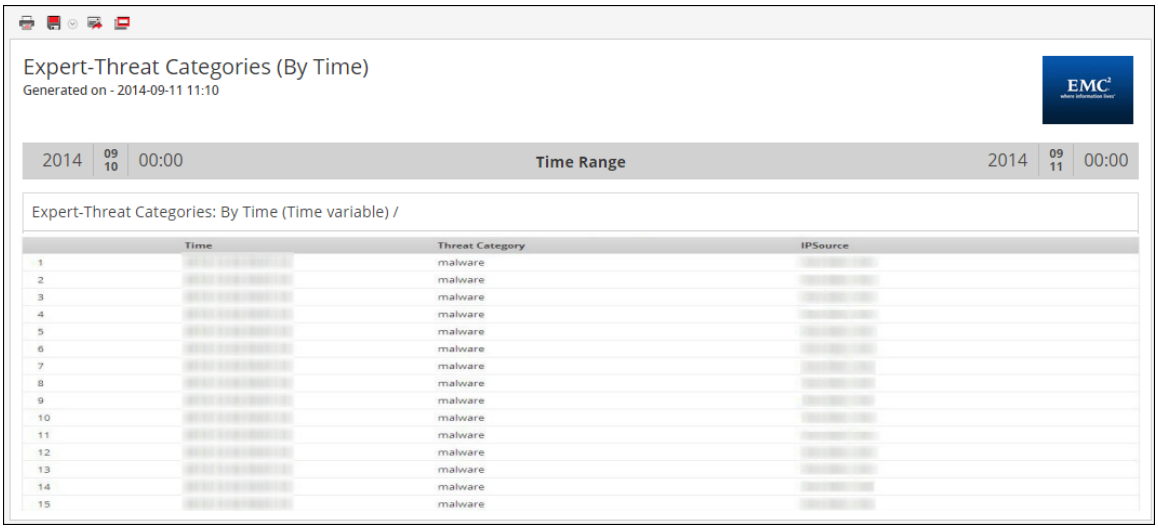


Si desea generar un informe con un rango de tiempo específico, debe definir manualmente el rango de tiempo en la consulta utilizando las siguientes dos variables:

`${report_starttime} - The starting time of the range in seconds.`
`${report_endtime} - The ending time of the range in seconds.`

Por ejemplo,`SELECT from_unixtime(time), threat_category, ip.src FROM time_variable WHERE threat_category is not NULL AND time >= ${report_starttime} AND time <= ${report_endtime};`

En la siguiente figura se muestra el conjunto de resultados de la calendarización de un informe diario.

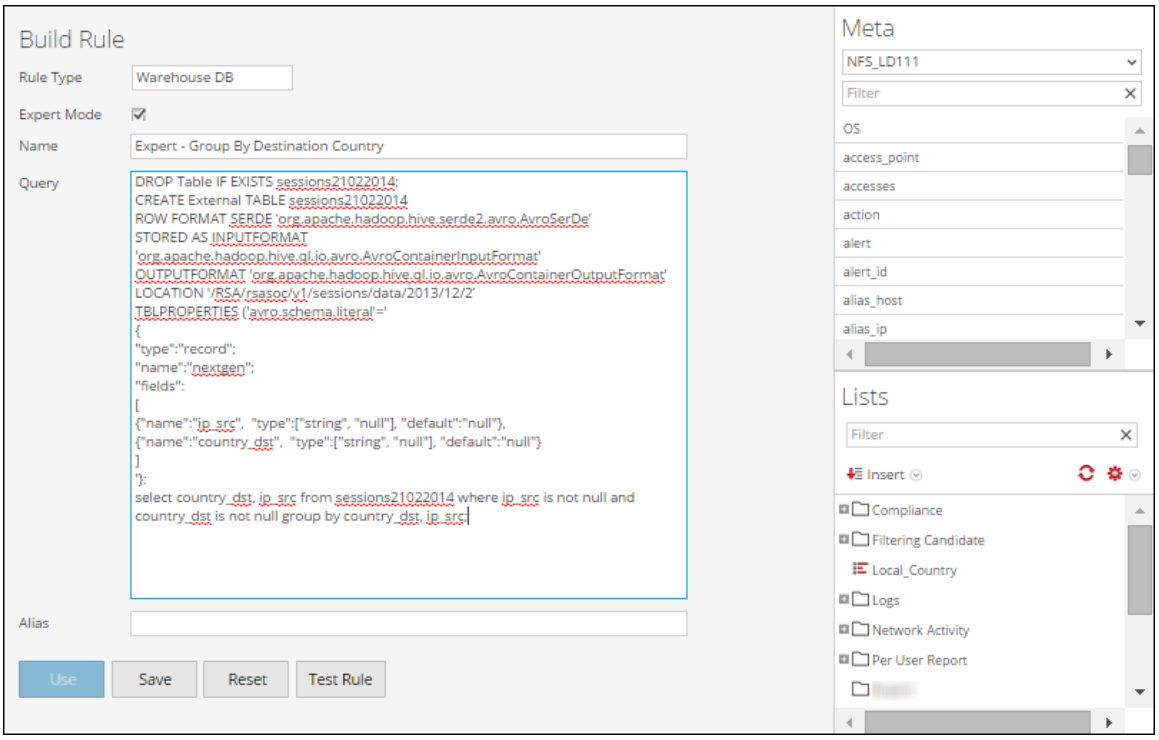


Partición de la tabla basada en informe de ubicación

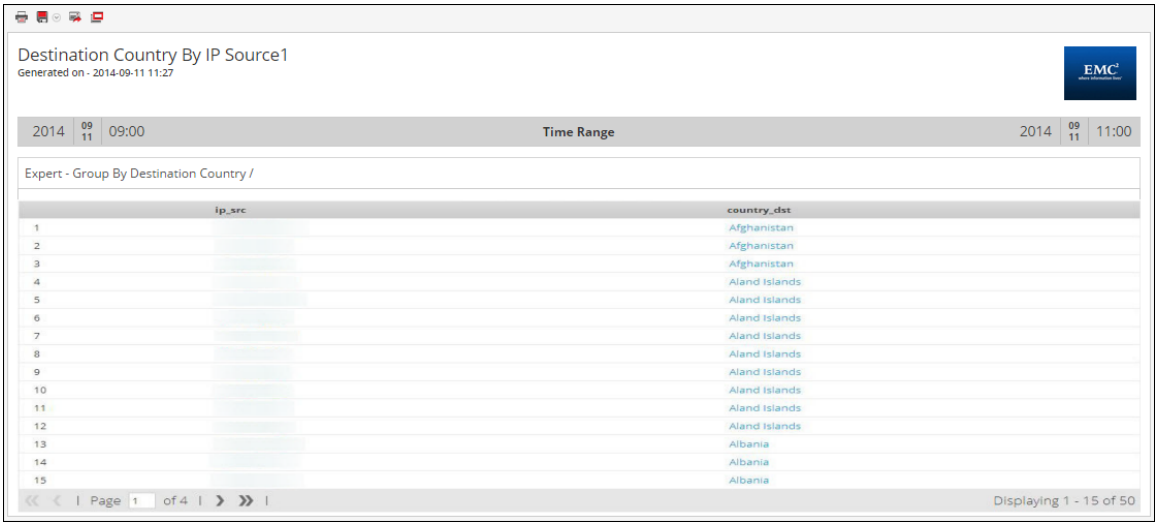
En esta regla de ejemplo, puede crear una partición de la tabla basándose en la ubicación. Cada tabla puede tener una o más claves de partición, que determinan cómo se almacenan los datos. Por ejemplo, un country_dst de tipo STRING y un ip_src de tipo STRING. Cada valor único de las claves de partición define una partición de la tabla.

En el ejemplo, ejecutamos una consulta HIVE a buscar el país de destino y la dirección IP de origen de la tabla sessions05032014 y agrupamos el conjunto de resultados según estos campos.

Esta regla proporciona información sobre la tabla creada, la fila formateada y la ubicación (ruta del directorio) de archivos de datos avro en Warehouse, y devuelve un conjunto de resultados de acuerdo con la consulta HIVE para indicar que la consulta devolvió un conjunto de resultados. Para obtener más información sobre estas declaraciones, consulte la sección **Sintaxis general de una regla avanzada**.



En la siguiente figura se muestra el conjunto de resultados de la creación de una partición de tabla en función del informe de ubicación.

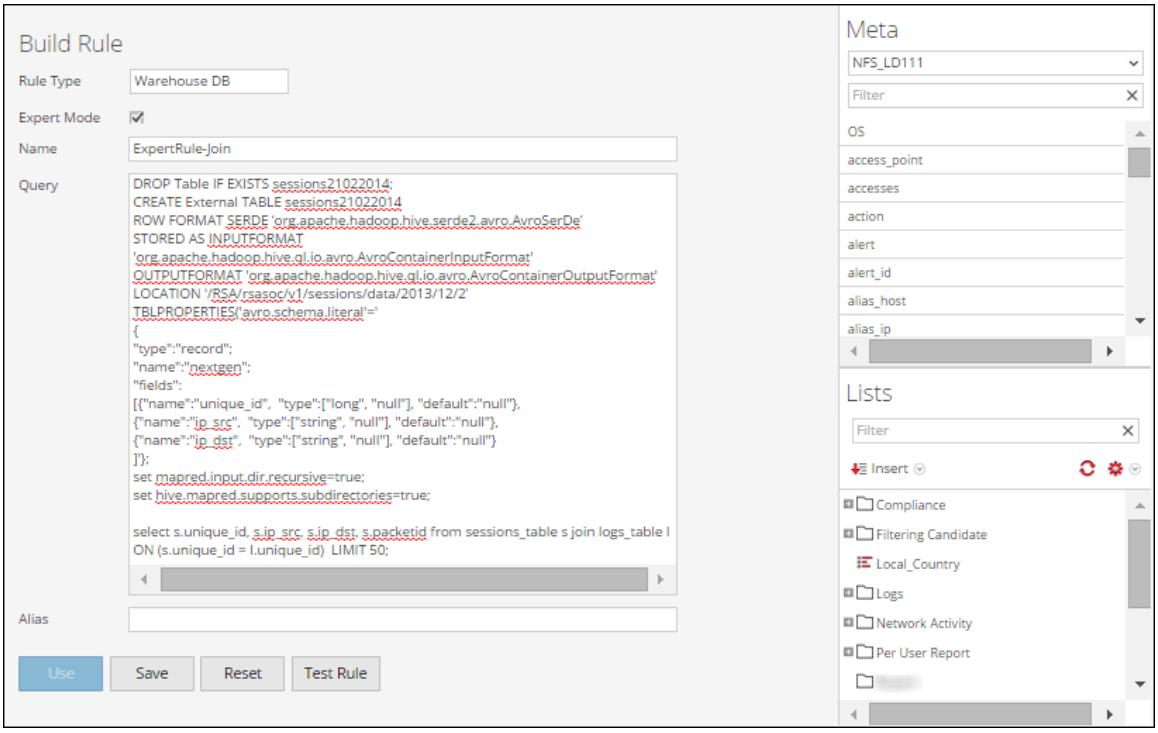


Registros de combinación y sesiones basados en informe unique_id

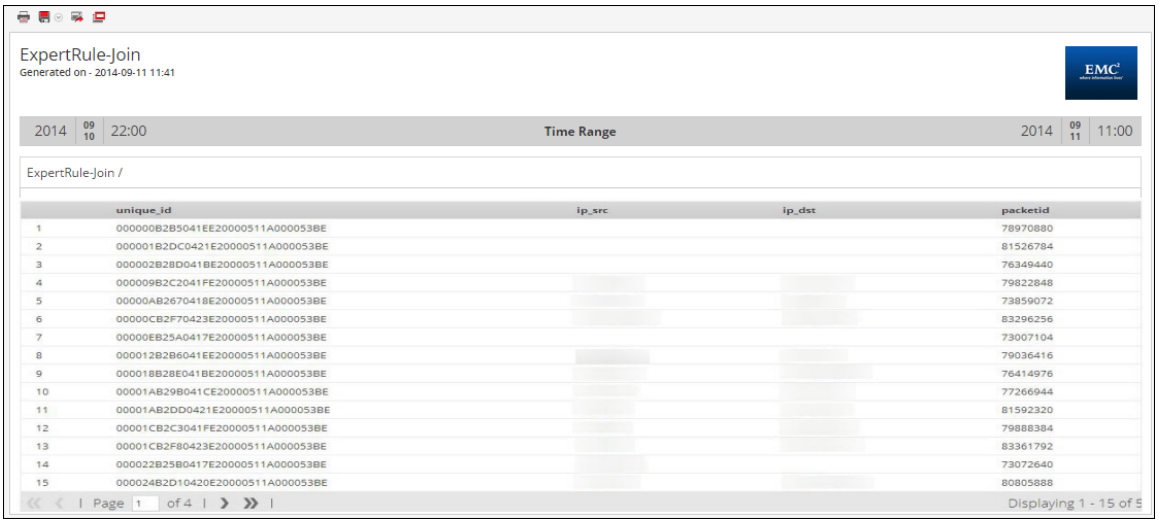
En esta regla de ejemplo, puede crear una regla para combinar registros y tablas de sesiones para buscar unique_id, la dirección IP de origen y destino, y el ID de paquete en función de unique_id.

En el ejemplo dado, ejecutamos una consulta HIVE para buscar ciertos campos, tanto de la sessions_table como de la logs_table mediante la realización de una combinación basada en el campo “unique_id”.

Esta regla proporciona información sobre la tabla creada, la fila formateada y la ubicación (ruta del directorio) de archivos de datos avro en Warehouse, y devuelve un conjunto de resultados de acuerdo con la consulta HIVE para indicar que la consulta devolvió un conjunto de resultados. Para obtener más información sobre estas declaraciones, consulte la sección **Sintaxis general de una regla avanzada**.



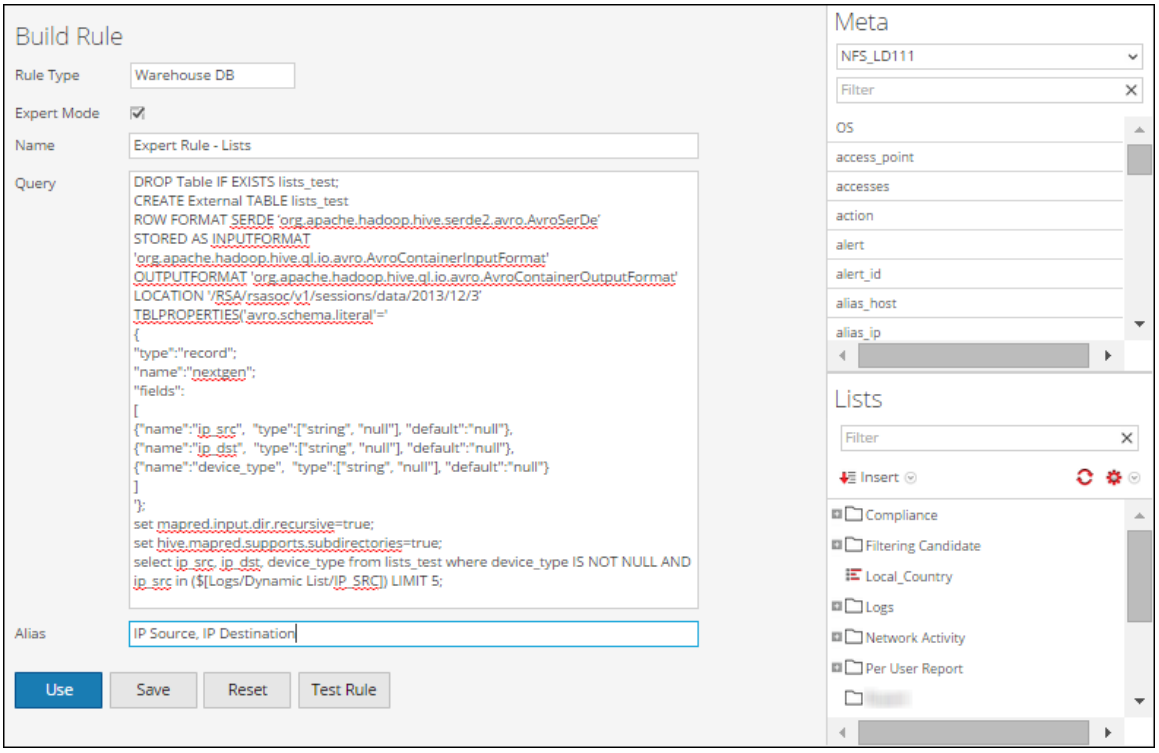
En la siguiente figura se muestra el conjunto de resultados de la combinación de registros y tablas de sesiones basadas en unique_id.



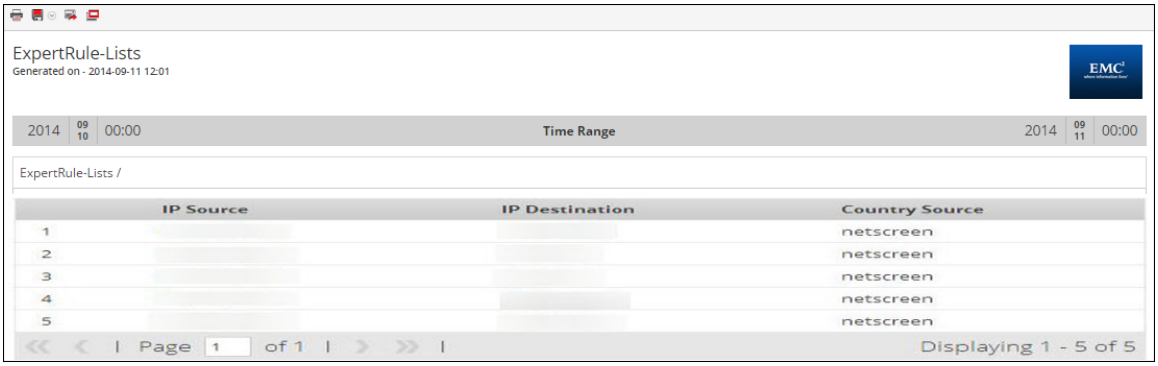
Informe de lista

En esta regla de ejemplo, puede crear un informe de lista para buscar la dirección IP de origen y destino, y el tipo de dispositivo de la tabla **lists_test**, donde el tipo de dispositivo no es nulo y la dirección IP de origen se obtiene de la lista de eventos correspondiente.

Esta regla proporciona información sobre la tabla creada, la fila formateada y la ubicación (ruta del directorio) de archivos de datos avro en Warehouse, y devuelve un conjunto de resultados de acuerdo con la consulta HIVE para indicar que la consulta devolvió un conjunto de resultados. Para obtener más información sobre estas declaraciones, consulte la sección **Sintaxis general de una regla avanzada**.



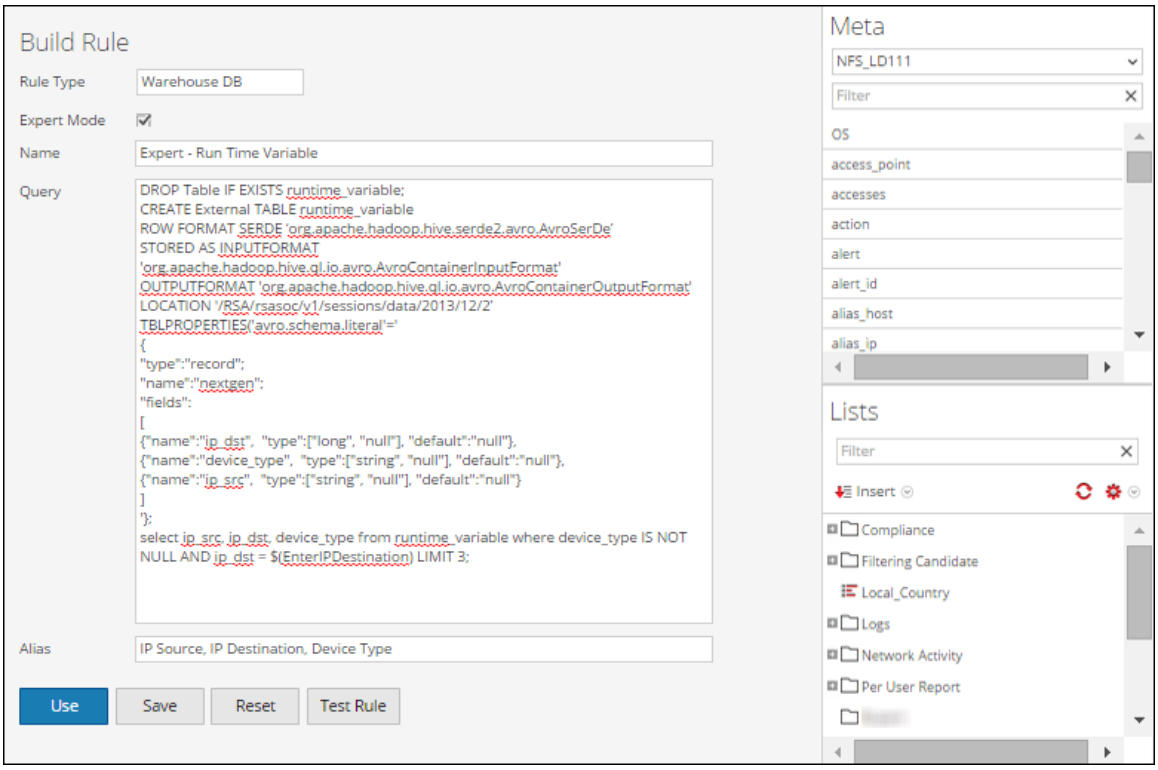
En la siguiente figura se muestra el conjunto de resultados de la ejecución de un informe de lista.



Informe con parámetros

En este ejemplo de regla, puede crear una regla para buscar direcciones IP de origen y destino, y el tipo de dispositivo de la tabla **runtime_variable** en función de la variable de hora de ejecución especificada `${EnterIPDestination}`. En tiempo de ejecución, se le pedirá que introduzca un valor para la dirección IP de destino, ip_dst. El conjunto de resultados se muestra según el valor que se ingresó.

Esta regla proporciona información sobre la tabla creada, la fila formateada y la ubicación (ruta del directorio) de archivos de datos avro en Warehouse, y devuelve un conjunto de resultados de acuerdo con la consulta HIVE para indicar que la consulta devolvió un conjunto de resultados. Para obtener más información sobre estas declaraciones, consulte la sección **Sintaxis general de una regla avanzada**.



En la siguiente figura se muestra el conjunto de resultados de la ejecución de un informe con parámetros.

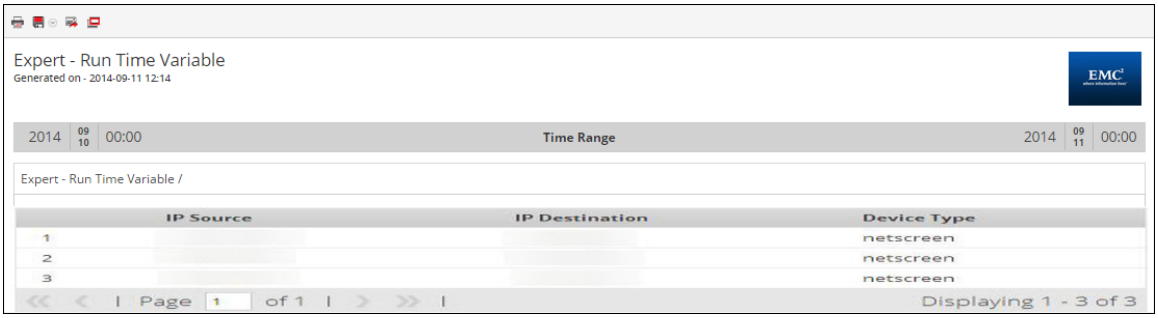


Tabla basada en partición con varias ubicaciones

El siguiente es un ejemplo de la tabla basada en partición con varias ubicaciones:

```
set mapred.input.dir.recursive=true;
 set hive.mapred.supports.subdirectories=true;
 DROP TABLE IF EXISTS AVRO_COUNT;
 CREATE EXTERNAL TABLE AVRO_COUNT
 PARTITIONED BY (partition_id int)
 ROW FORMAT SERDE 'org.apache.hadoop.hive.serde2.avro.AvroSerDe'
 WITH SERDEPROPERTIES (
 'avro.schema.literal'='{
 "name": "my_record", "type": "record",
 "fields": [
```

```
 {"name":"sessionid", "type":["null", "long"], "default" :
null},
 {"name":"time", "type":["null", "long"], "default" : null}
 ]}'
 )
 STORED AS
 INPUTFORMAT
 'org.apache.hadoop.hive.ql.io.avro.AvroContainerInputFormat'
 OUTPUTFORMAT
 'org.apache.hadoop.hive.ql.io.avro.AvroContainerOutputFormat';
 ALTER TABLE AVRO_COUNT ADD PARTITION(partition_id=0) LOCATION
'/rsasoc/v1/sessions/data/2015/07/22/8';
 ALTER TABLE AVRO_COUNT ADD PARTITION(partition_id=1) LOCATION
'/rsasoc/v1/sessions/data/2015/07/22/9';
 ALTER TABLE AVRO_COUNT ADD PARTITION(partition_id=2) LOCATION
'/rsasoc/v1/sessions/data/2015/07/22/10/';
 ALTER TABLE AVRO_COUNT ADD PARTITION(partition_id=3) LOCATION
'/rsasoc/v1/sessions/data/2015/07/22/11/';
 ALTER TABLE AVRO_COUNT ADD PARTITION(partition_id=4) LOCATION
'/rsasoc/v1/sessions/data/2015/07/22/12/';
 SELECT COUNT(*) as TOTAL FROM AVRO_COUNT WHERE time >=
${report_starttime} AND time
 <= ${report_endtime};
```

La tabla basada en partición con varias ubicaciones es como se explica a continuación:

1. Permita que HIVE escanee recurrentemente todos los subdirectorios y que lea todos sus datos.

   ```
   set mapred.input.dir.recursive=true;
    set hive.mapred.supports.subdirectories=true;
   ```

2. Descarte y cree una tabla externa y formatee las filas:

   ```
   DROP TABLE IF EXISTS AVRO_COUNT;
    CREATE EXTERNAL TABLE AVRO_COUNT
    PARTITIONED BY (partition_id int)
    ROW FORMAT SERDE
   'org.apache.hadoop.hive.serde2.avro.AvroSerDe'
    WITH SERDEPROPERTIES (
    'avro.schema.literal'='{
    "name": "my_record", "type": "record",
    "fields": [
    {"name":"sessionid", "type":["null", "long"], "default" :
   ```

```
null},
 {"name":"time", "type":["null", "long"], "default" : null}
 ]}'
 )
 STORED AS
 INPUTFORMAT
 'org.apache.hadoop.hive.ql.io.avro.AvroContainerInputFormat'
 OUTPUTFORMAT

'org.apache.hadoop.hive.ql.io.avro.AvroContainerOutputForma
t';
```

Nota: Solo debe crear una tabla externa si usa otra tabla. Por ejemplo, si usa otra tabla además de **AVRO_COUNT**, debe descartar la tabla y crear una tabla externa.

Nota: Puntos que debe recordar cuando crea una tabla:
- Si descarta una tabla “no externa”, se eliminan los datos.
- La tabla está particionada en una sola columna denominada partition_id, que es la columna estándar para Reporting Engine.
- El valor predeterminado de cualquier columna es nulo, porque es probable que el archivo AVRO no contenga la columna especificada.
- Los nombres de las columnas deben estar en minúscula, porque HIVE no distingue mayúsculas de minúsculas, a diferencia de AVRO.
- Debe especificar **avro.schema.literal** en *SERDEPROPERTIES*.

Para obtener más información sobre la sintaxis de regla, consulte Apache HIVE.

3. Agregar particiones:
   Una vez que define una tabla, debe especificar las ubicaciones de HDFS desde donde se deben consultar los datos antes de ejecutar las declaraciones HIVE. El parámetro de ubicación especifica los datos que se buscarán según la fecha que se especifique. Los datos se distribuyen entre varias ubicaciones o directorios de HDFS. Para cada ubicación debe agregar una partición con valores únicos asignados a la columna de la partición. Las ubicaciones pueden ser cualquier directorio en HDFS

```
 ALTER TABLE AVRO_COUNT ADD PARTITION(partition_id=0) LOCATION
'/rsasoc/v1/sessions/data/2015/07/22/8';
 ALTER TABLE AVRO_COUNT ADD PARTITION(partition_id=1)
LOCATION '/rsasoc/v1/sessions/data/2015/07/22/9';
 ALTER TABLE AVRO_COUNT ADD PARTITION(partition_id=2)
```

```
LOCATION '/rsasoc/v1/sessions/data/2015/07/22/10/';
 ALTER TABLE AVRO_COUNT ADD PARTITION(partition_id=3)
LOCATION '/rsasoc/v1/sessions/data/2015/07/22/11/';
 ALTER TABLE AVRO_COUNT ADD PARTITION(partition_id=4)
LOCATION '/rsasoc/v1/sessions/data/2015/07/22/12/';
```

Nota: HIVE lee cada archivo en estas ubicaciones como AVRO. Si en una de estas ubicaciones está disponible un archivo no AVRO, la consulta puede fallar.

4. Ejecute la consulta

```
SELECT COUNT(*) as TOTAL FROM AVRO_COUNT WHERE time >=
${report_starttime} AND time
 <= ${report_endtime};
```

Cuando se crea una tabla, puede ejecutar consultas específicas para filtrar los datos. Por ejemplo, después de crear la tabla, puede filtrar los datos como se muestra en los siguientes ejemplos:

Sesiones con una dirección IP de origen específica:

```
SELECT * FROM AVRO_COUNT WHERE time >= ${report_starttime}
AND time <= ${report_endtime}  AND ip_src = '127.0.0.1';
```

Agrupar por en función del destino del usuario:

```
SELECT * FROM AVRO_COUNT WHERE time >= ${report_starttime}
AND time <= ${report_endtime}  GROUP BY usr_dst;
```

Partición automatizada mediante función personalizada

En la versión 10.5.1, puede usar la función personalizada para automatizar la adición de particiones en una tabla definida por el usuario en el modo experto.

Sintaxis general

```
RE WH CUSTOM ADDPARTITIONS(table, namespace, rollup, [starttime,
endtime])
```

En la siguiente tabla se describe la sintaxis de la función personalizada:

Número	Nombre	Descripción
1	Tabla	El nombre de la tabla para el cual se debe agregar la partición.
2	namespace	El espacio de nombres puede ser sesiones o registros.

Número	Nombre	Descripción
3	rollup	Este valor determina el nivel de ruta del directorio que se incluirá en las particiones. El valor puede ser HORA, DÍA o MINUTO. Si Warehouse Connector está configurado para acumulación por día, la configuración de este valor como HORA genera CERO resultados. El número y la ubicación de cada partición se basa en el rango de tiempo que se utiliza para ejecutar la regla y el valor de acumulación.
4	(Opcional) starttime, endtime	Para generar particiones para un rango de tiempo determinado que no sea el rango de tiempo que se menciona en la regla, debe especificar starttime y endtime en **segundos Epoch**. **Nota:** No se admiten expresiones para starttime y endtime.

La función personalizada se invoca cuando Reporting Engine ejecuta la regla durante la regla de prueba o el informe programado. Durante la ejecución de una regla experta, siempre que Reporting Engine identifica la declaración de función, extrae los argumentos requeridos, inserta *n* declaraciones ADD PARTITION HiveQL y las ejecuta en el servidor de Hive.

La ubicación y la estructura del directorio las determina el argumento transmitido en la regla y la configuración de origen de datos de Hive en Reporting Engine. La cantidad de particiones depende de la acumulación especificada y del rango de tiempo utilizado durante la ejecución de la regla. Por ejemplo, con la acumulación como HORA y el rango de tiempo como ÚLTIMOS 2 DÍAS, se generan 48 particiones para 48 horas, mientras que con la acumulación como DÍA, Reporting Engine crea 2 particiones, una para cada día.

La consulta de la partición se genera en la plantilla de sintaxis como se establece en el atributo de configuración de Hive de Reporting Engine, AlterTableTemplate.

Nota: De forma predeterminada, esta función inicia la adición de particiones a una tabla con ID de partición de 0 a n-1. Por lo tanto, esto requiere que la tabla se particione por la columna de número entero único denominada ID de partición.

El siguiente es un ejemplo de una partición automatizada mediante la función personalizada:

```
set mapred.input.dir.recursive=true;
 set hive.mapred.supports.subdirectories=true;
 DROP TABLE IF EXISTS AVRO_COUNT;
```

```
CREATE EXTERNAL TABLE AVRO_COUNT
 PARTITIONED BY (partition_id int)
 ROW FORMAT SERDE 'org.apache.hadoop.hive.serde2.avro.AvroSerDe'
 WITH SERDEPROPERTIES (
 'avro.schema.literal'='{
  "name": "my_record", "type": "record",
  "fields": [
  {"name":"sessionid", "type":["null", "long"], "default" :
null}
  ,{"name":"time", "type":[ "null" , "long"], "default" : null}
  ,{"name":"unique_id", "type":["null", "string"], "default" :
null}
  ]}'
 )
 STORED AS
 INPUTFORMAT
 'org.apache.hadoop.hive.ql.io.avro.AvroContainerInputFormat'
 OUTPUTFORMAT
 'org.apache.hadoop.hive.ql.io.avro.AvroContainerOutputFormat';
RE_WH_CUSTOM_ADDPARTITIONS(AVRO_COUNT, 'sessions', 'DAY');
 SELECT COUNT(*) as TotalSessions FROM AVRO_COUNT
 WHERE time >= ${report_starttime} AND time <= ${report_
endtime};
```

Reglas simples de la base de datos de Warehouse

En este tema se proporcionan ejemplos de reglas de origen de datos de Warehouse. Puede definir reglas de base de datos de Warehouse mediante consultas de HIVE. Puede definir reglas simples y avanzadas para el origen de datos de Warehouse mediante los siguientes modos:

- Modo Predeterminado
- Modo experto

En el modo Predeterminado, las reglas simples se definen con cláusulas como Select, Where, Group by y Having para consultar el origen de datos. De manera predeterminada, puede crear reglas para realizar consultas a las sesiones o registros crudos.

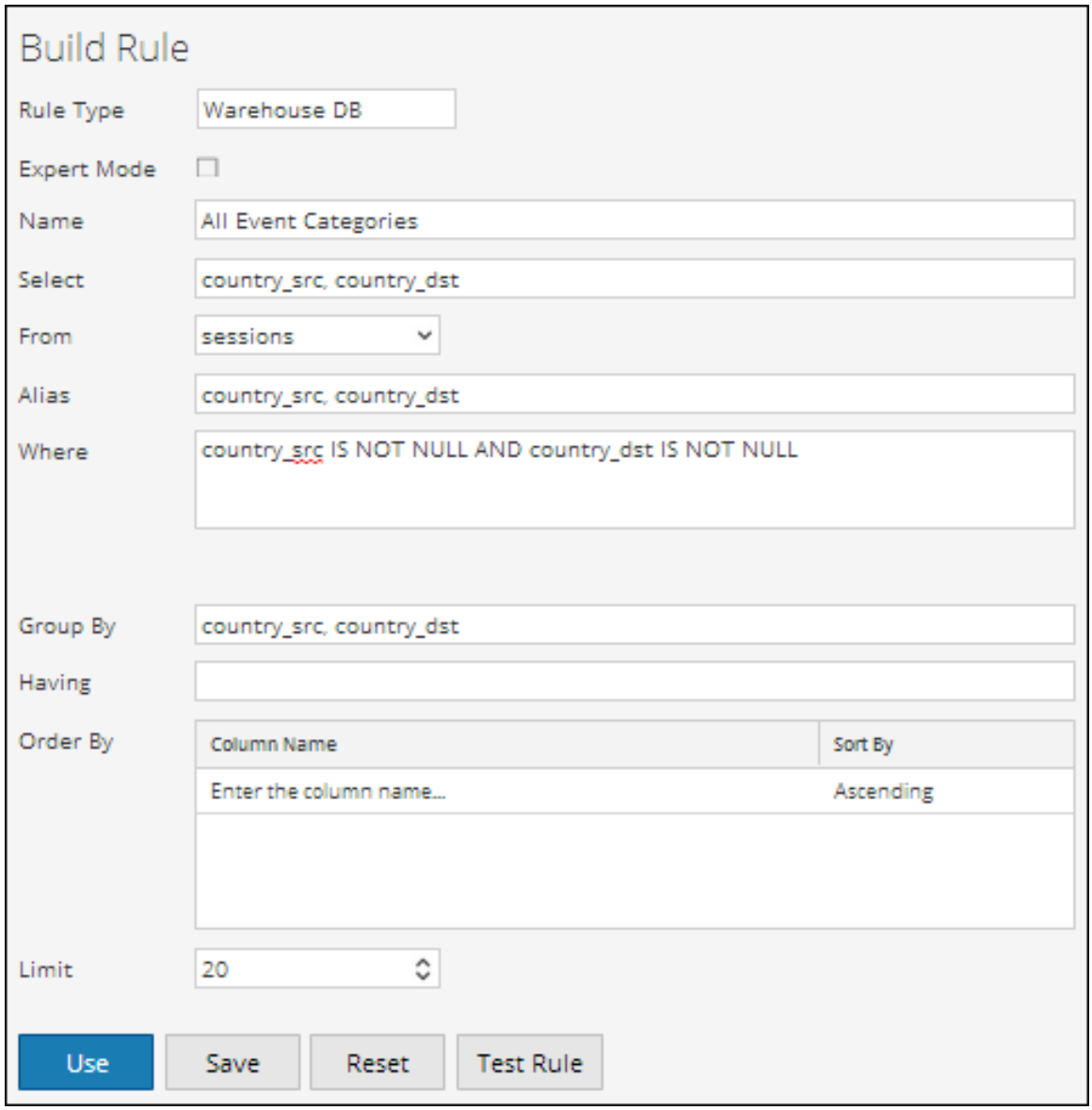
Los siguientes ejemplos ilustran reglas simples en el modo predeterminado:

- Informe Todas las categorías de eventos
- Informe Categorías de eventos de ataques

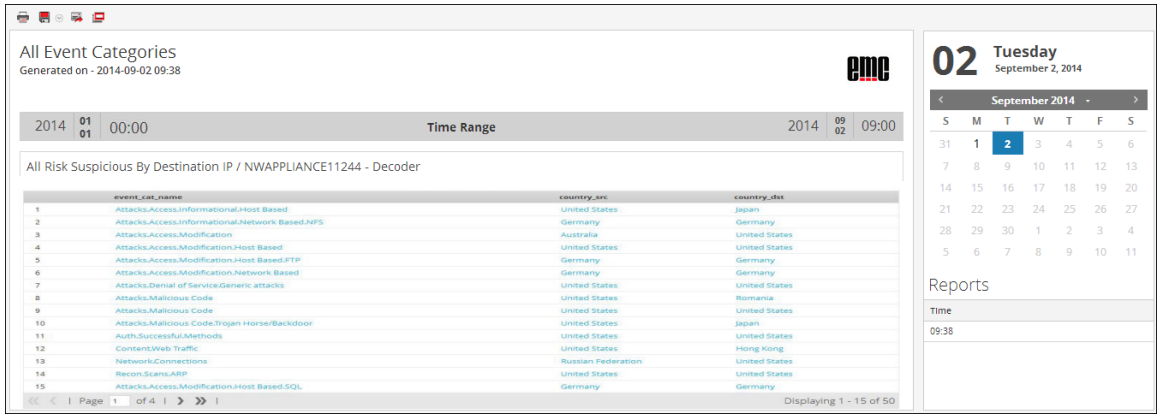
- Fuente: Informe Categorías de eventos de China
- Informe Categorías de eventos de direcciones IP de origen y destino
- Informe Categorías de amenazas por tiempo
- Informe Consulta de arreglo
- Informe Consulta de registro crudo

Informe Todas las categorías de eventos

Esta regla recupera todas las categorías de eventos, país de origen y país de destino desde la tabla **sesiones** con la definición de los nombres de alias (nombres de columna temporales) para cada uno de los campos que se recuperarán desde la tabla, es decir, **country_src** para el país de origen y **country_dst** para el país de destino.

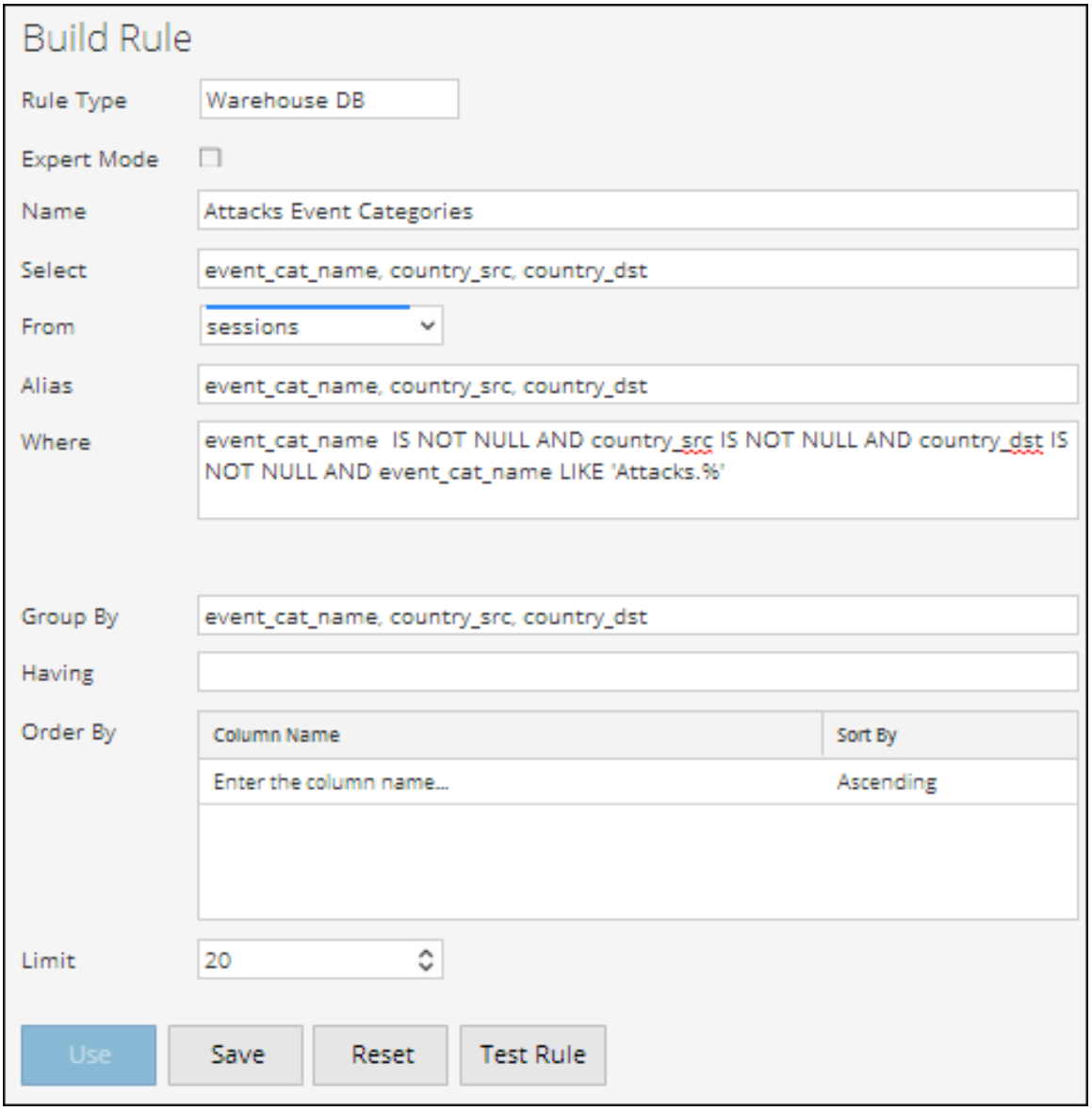


En la siguiente figura se muestra el conjunto de resultados de la regla Todas las categorías de eventos.

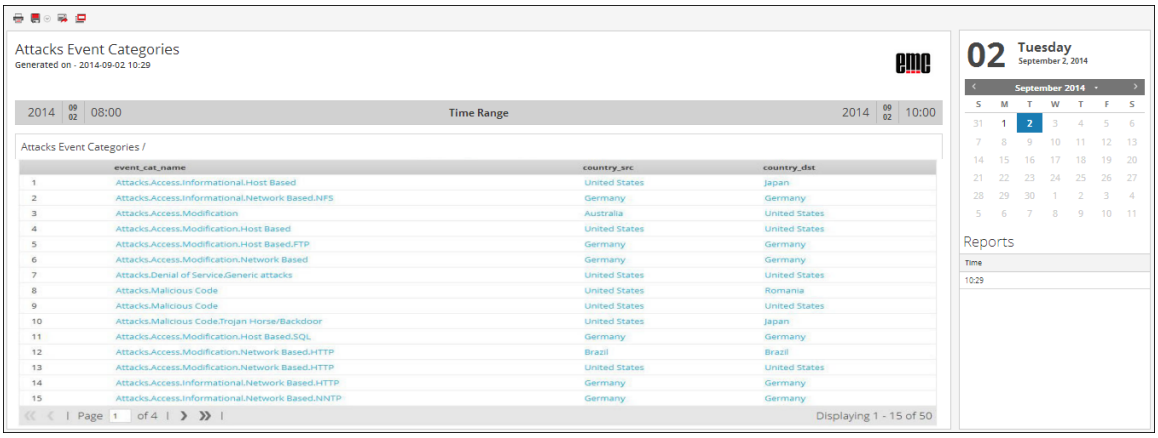


Informe Categorías de eventos de ataques

Esta regla recupera las categorías de eventos, el país de origen y el país de destino desde la tabla **sesiones** con la definición de los nombres de alias (nombres de columna temporales) para cada uno de los campos que se recuperarán desde la tabla y la selección solo de las columnas cuyo nombre de categoría de evento sea como “Attacks.%”.

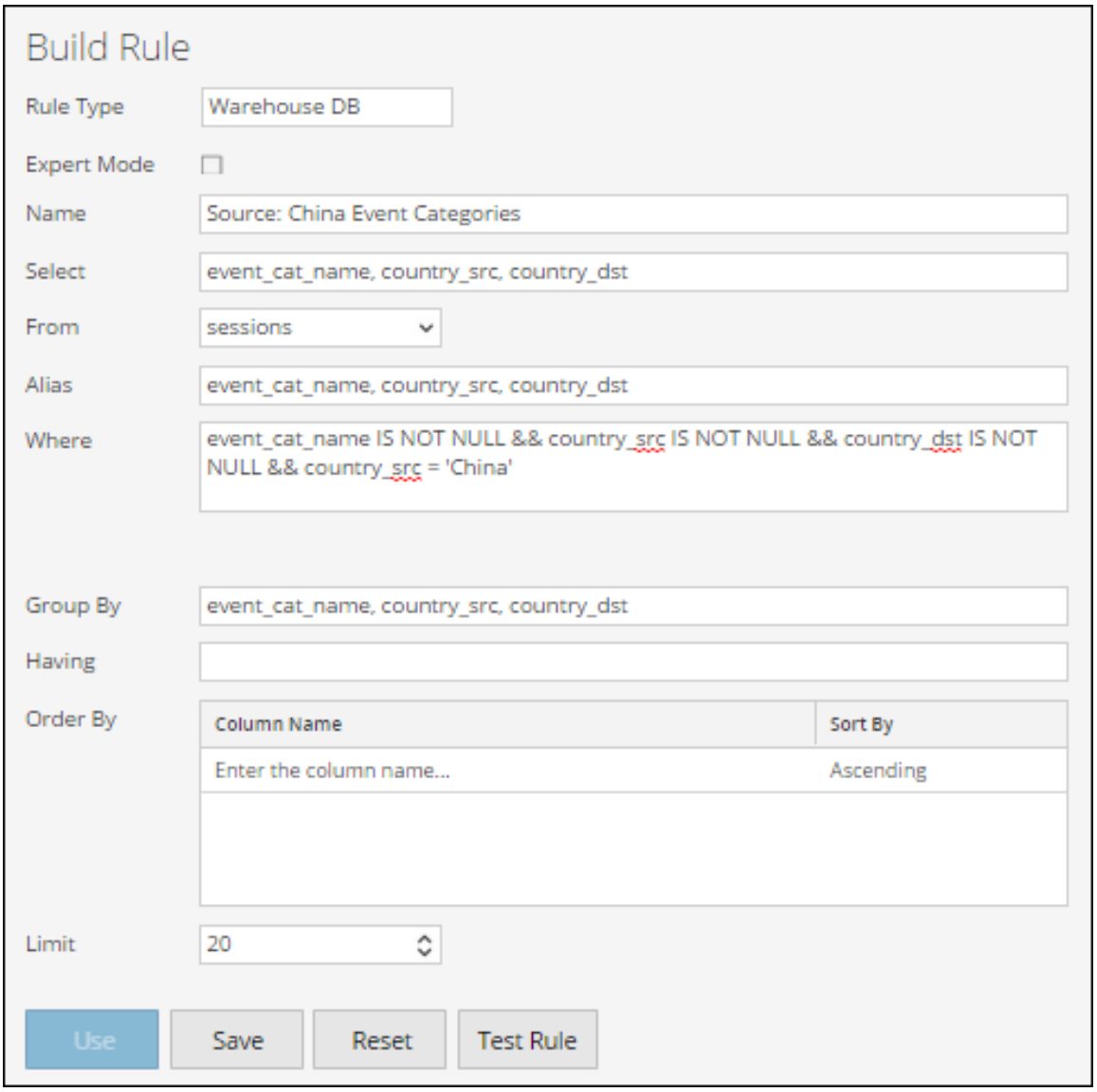


En la siguiente figura se muestra el conjunto de resultados de la regla Categorías de eventos de ataques.

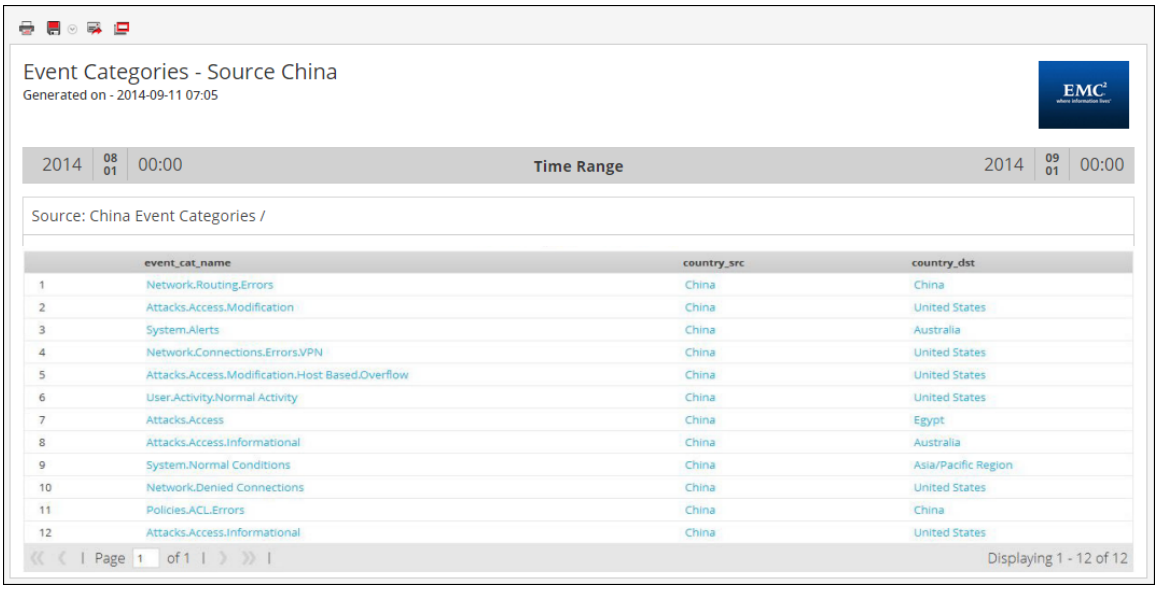


Fuente: Informe Categorías de eventos de China

Esta regla recupera las categorías de eventos, el país de origen y el país de destino desde la tabla **sesiones** con la definición de los nombres de alias (nombres de columna temporales) para cada uno de los campos que se recuperarán desde la tabla y la selección solo de las columnas cuyo país de origen sea “China”.



En la siguiente figura se muestra el conjunto de resultados de la regla Origen: Categorías de eventos de China.



Event Categories - Source China
Generated on - 2014-09-11 07:05

2014 08 01 00:00 **Time Range** 2014 09 01 00:00

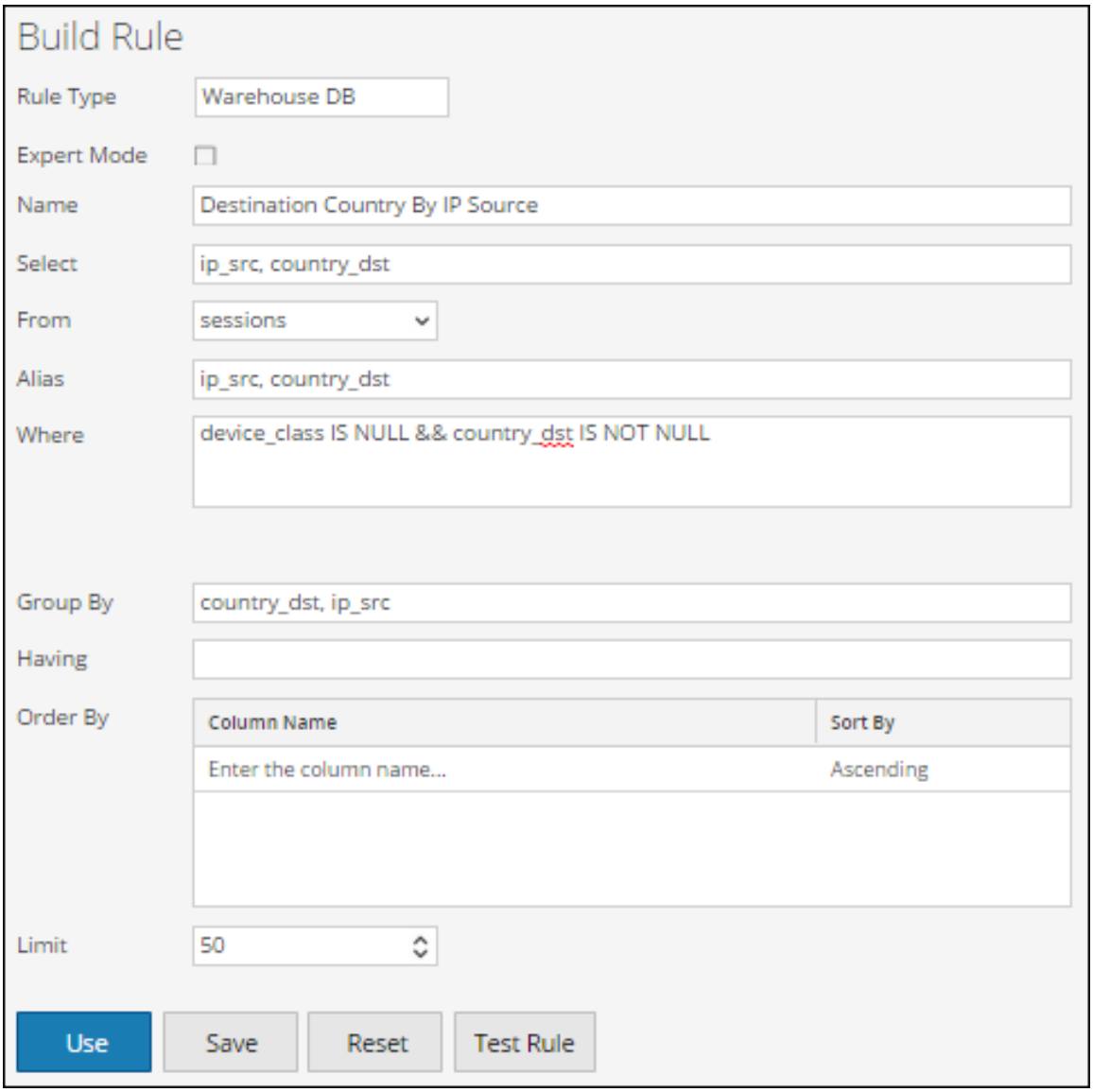
Source: China Event Categories /

	event_cat_name	country_src	country_dst
1	Network.Routing.Errors	China	China
2	Attacks.Access.Modification	China	United States
3	System.Alerts	China	Australia
4	Network.Connections.Errors.VPN	China	United States
5	Attacks.Access.Modification.Host Based.Overflow	China	United States
6	User.Activity.Normal Activity	China	United States
7	Attacks.Access	China	Egypt
8	Attacks.Access.Informational	China	Australia
9	System.Normal Conditions	China	Asia/Pacific Region
10	Network.Denied Connections	China	United States
11	Policies.ACL.Errors	China	China
12	Attacks.Access.Informational	China	United States

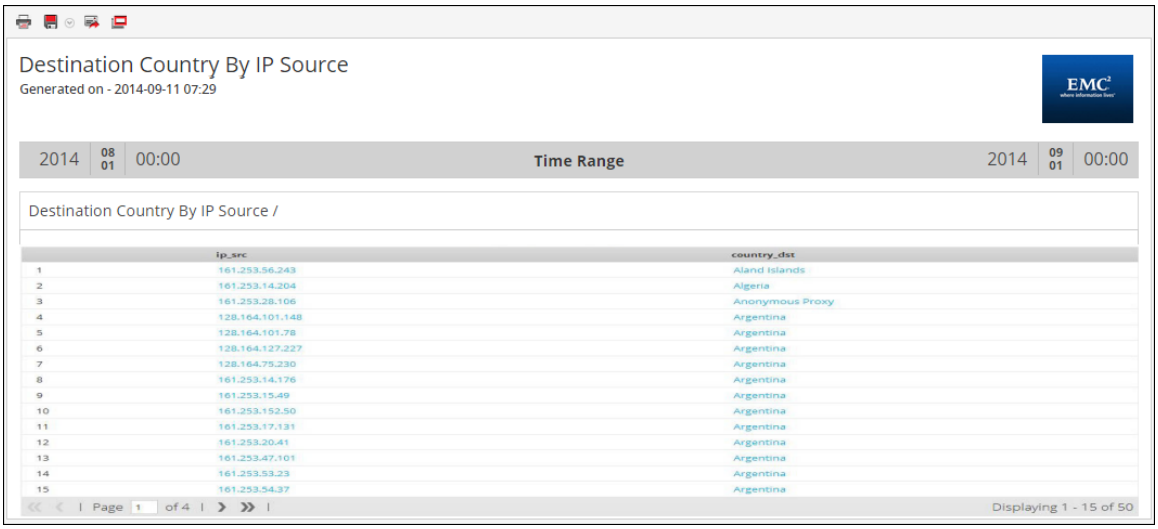
Page 1 of 1 Displaying 1 - 12 of 12

Informe Categorías de eventos de direcciones IP de origen y destino

Esta regla recupera la dirección IP del país de origen y de destino desde la tabla **sesiones** con la definición de los nombres de alias (nombres de columna temporales) para cada uno de los campos que se recuperarán desde la tabla y la selección solo de las columnas cuyo país de destino sea NO NULO.

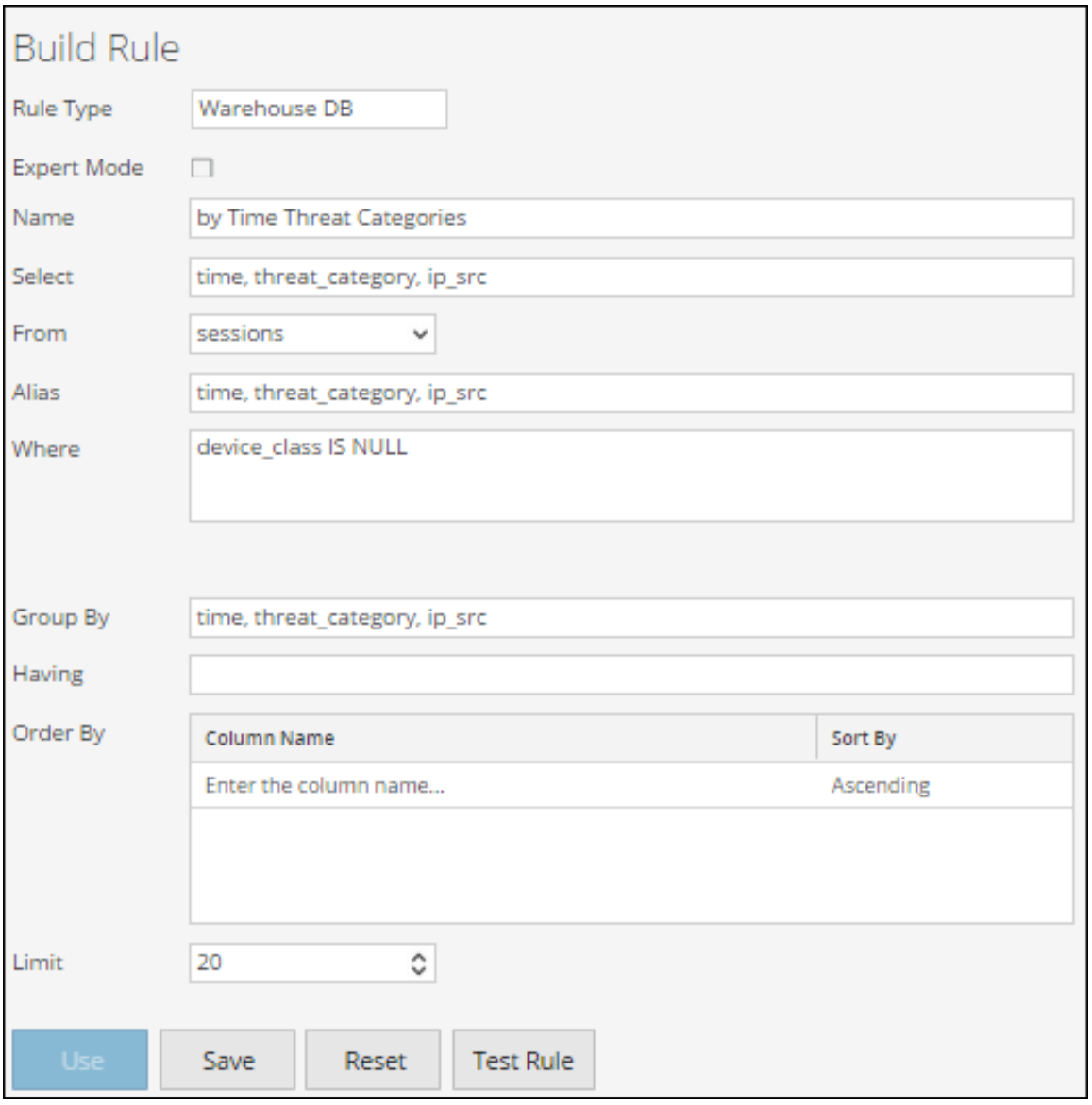


En la siguiente figura se muestra el conjunto de resultados de la regla Categorías de eventos de direcciones IP de origen y destino.



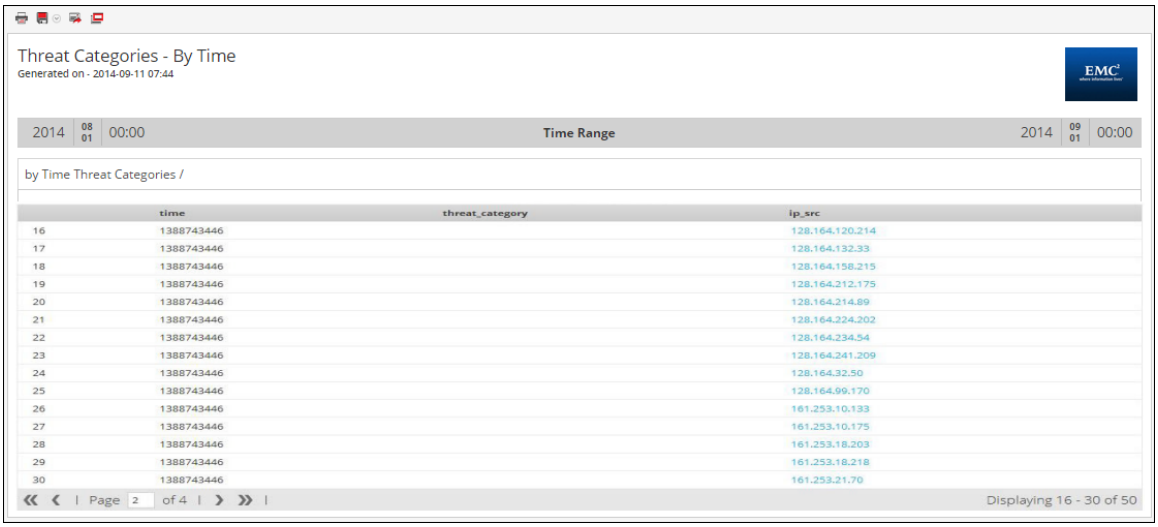
Informe Categorías de amenazas por tiempo

Esta regla recupera los eventos de la categoría de amenaza, la hora en que se recopiló el registro o el evento en Log Decoder/Decoder y las direcciones IP de origen desde la tabla **sesiones** con la definición de los nombres de alias (nombres de columna temporales) para cada uno de estos campos que se recuperarán desde la tabla.



En la siguiente figura se muestra el conjunto de resultados de la regla Categorías de amenazas por tiempo. El tiempo que aparece en el campo de tiempo es el tiempo UNIX (por ejemplo, 1388743446).

Nota: En la cláusula “Select” la sintaxis sería “UNIX time” para una conversión a la hora UTC en el informe. Por ejemplo, puede usar la herramienta de conversión de hora Epoch para convertir la hora UNIX (1388743446) en UTC (hora universal coordinada) (03/01/2014 15:34:06 h).



Threat Categories - By Time
Generated on - 2014-09-11 07:44

EMC²

2014 08 01 00:00 **Time Range** 2014 09 01 00:00

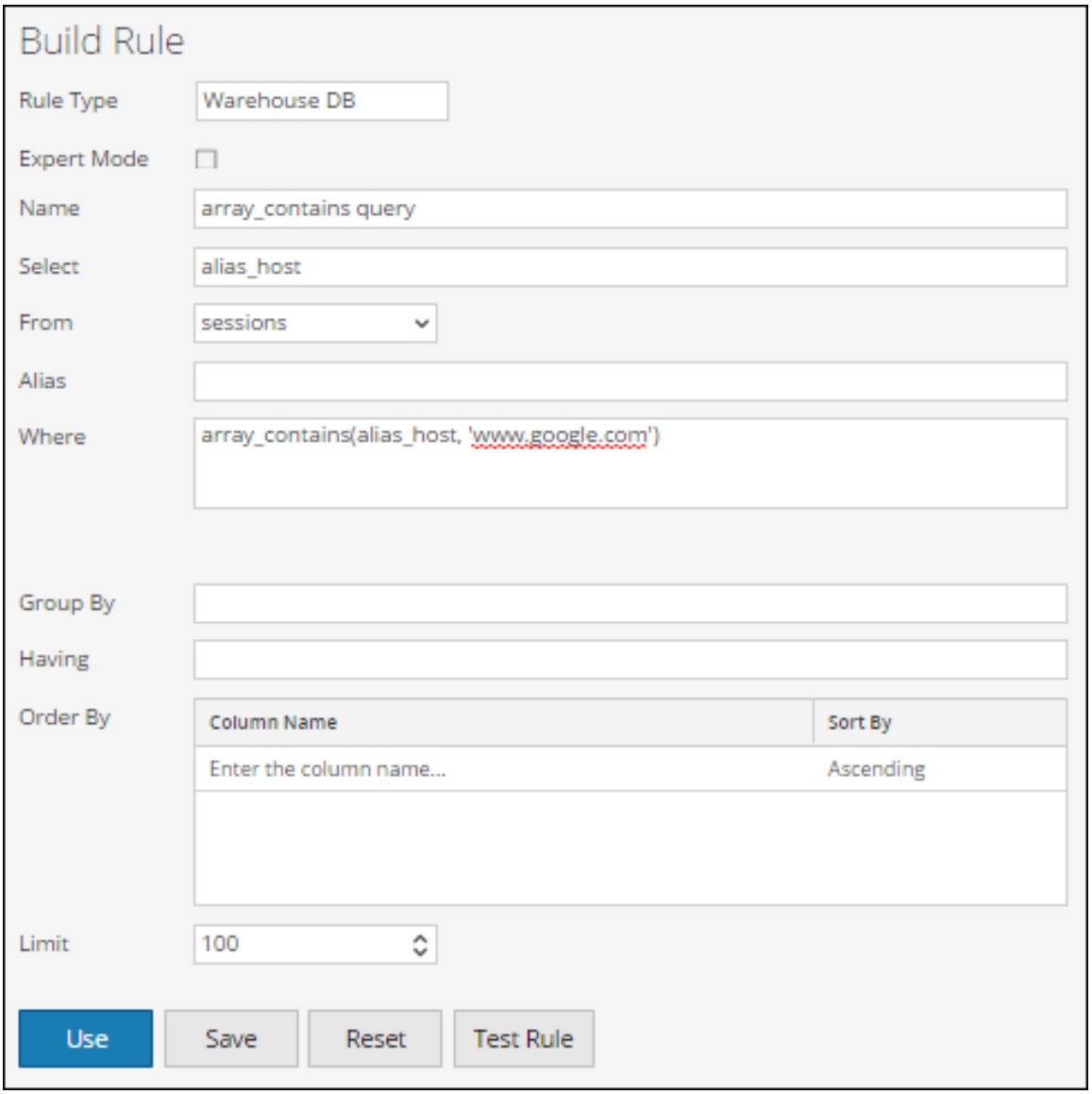
by Time Threat Categories /

	time	threat_category	ip_src
16	1388743446		128.164.120.214
17	1388743446		128.164.132.33
18	1388743446		128.164.158.215
19	1388743446		128.164.212.175
20	1388743446		128.164.214.89
21	1388743446		128.164.224.202
22	1388743446		128.164.234.54
23	1388743446		128.164.241.209
24	1388743446		128.164.32.50
25	1388743446		128.164.99.170
26	1388743446		161.253.10.133
27	1388743446		161.253.10.175
28	1388743446		161.253.18.203
29	1388743446		161.253.18.218
30	1388743446		161.253.21.70

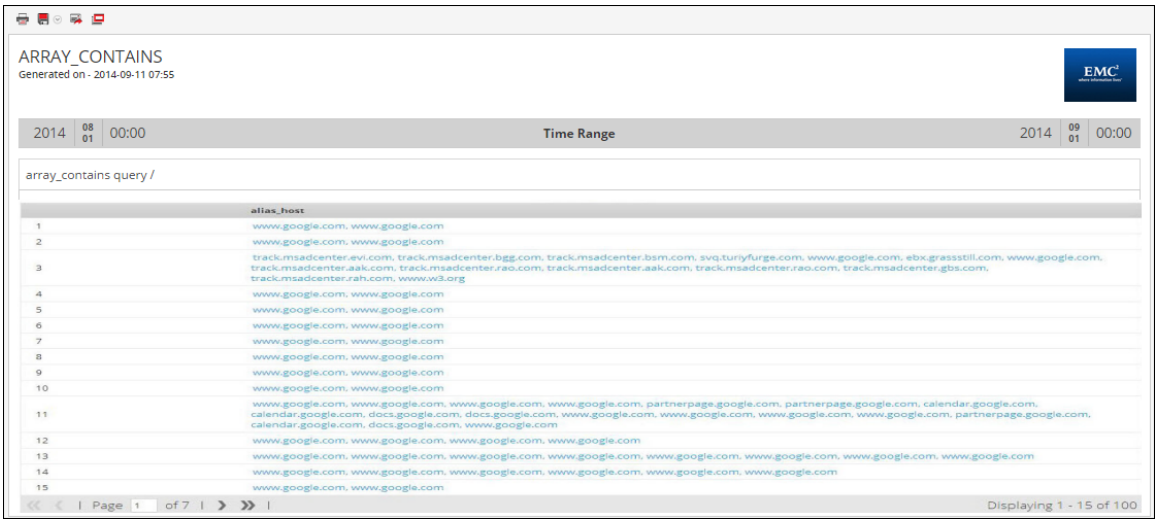
« ‹ | Page 2 of 4 | › » | Displaying 16 - 30 of 50

Informe Consulta de arreglo

Esta regla recupera un arreglo de nombres de host de alias desde la tabla **sesiones** que contiene el valor “www.google.com”.



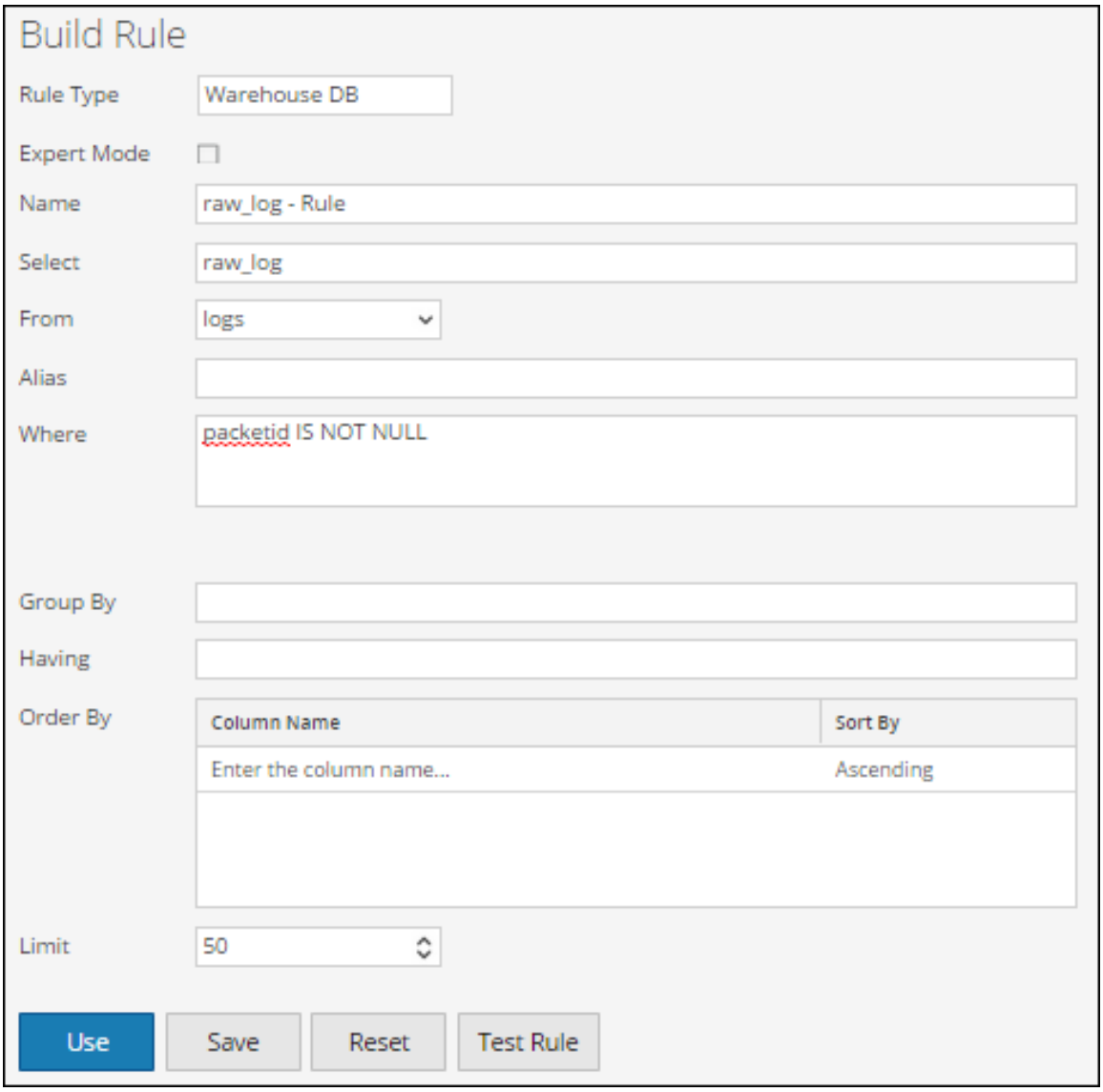
En la siguiente figura se muestra el conjunto de resultados para consultar un arreglo desde las sesiones.



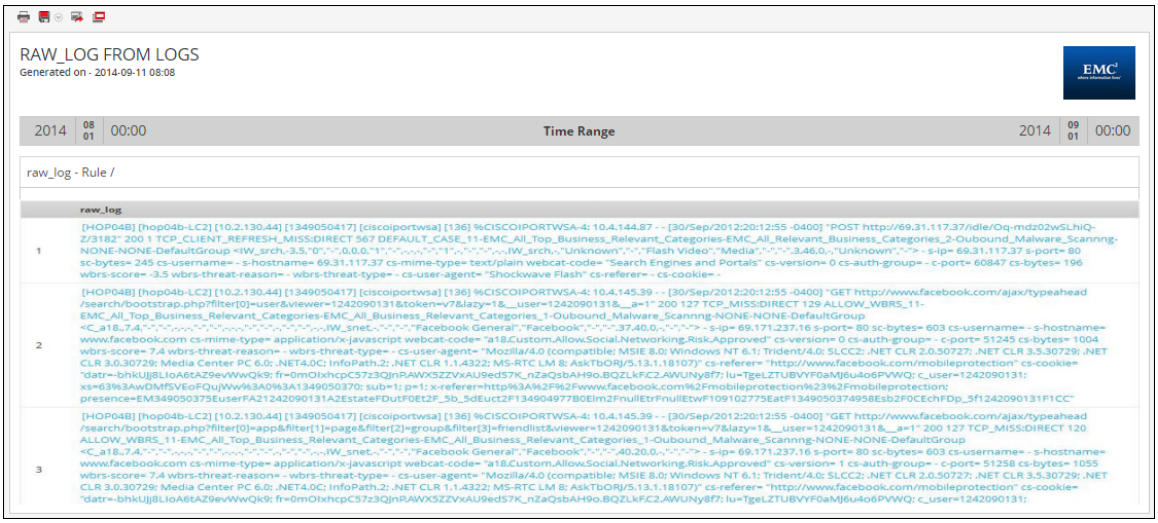
Informe Consulta de registro crudo

Se pueden consultar los registros crudos desde la tabla de registro o de sesiones.

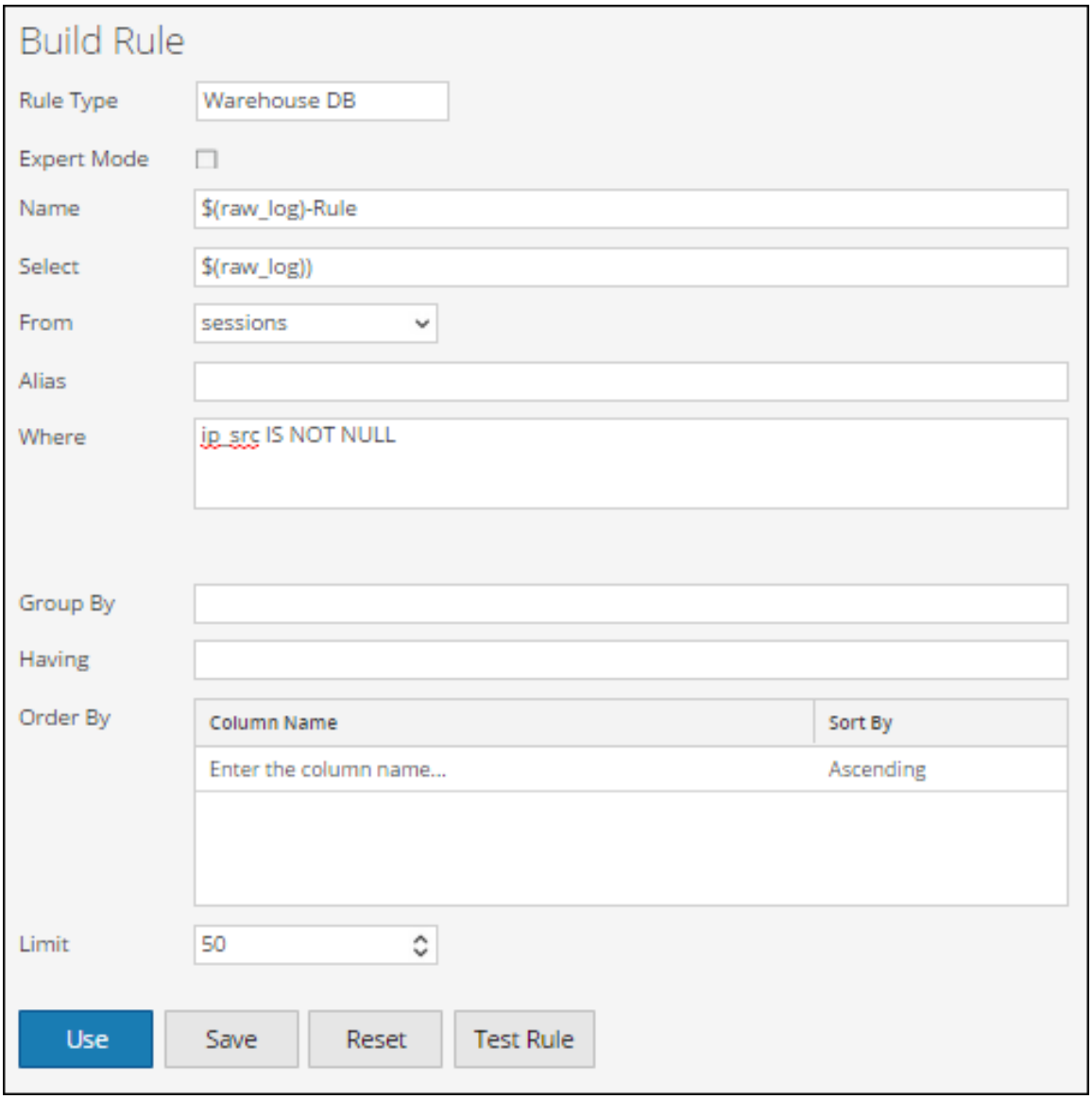
Esta regla usa **raw_log** como metadatos para consultar el registro crudo desde registros cuyo ID de paquete NO SEA NULO.



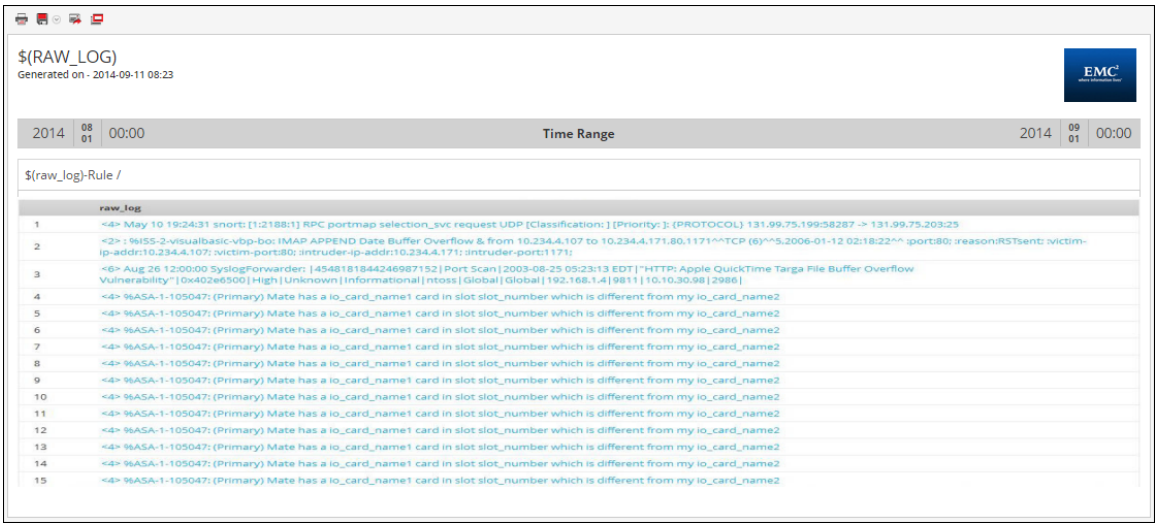
En la siguiente figura se muestra el conjunto de resultados para consultar registros crudos desde registros.



Esta regla usa **${raw_log}** como metadatos para consultar un registro crudo desde sesiones cuya dirección IP de origen NO SEA NULA.



En la siguiente figura se muestra el conjunto de resultados para consultar registros crudos desde sesiones.



Vista Crear regla

En este tema se describen las funciones de la vista Crear regla y las acciones que puede ejecutar. Los procedimientos asociados se proporcionan en Reglas.

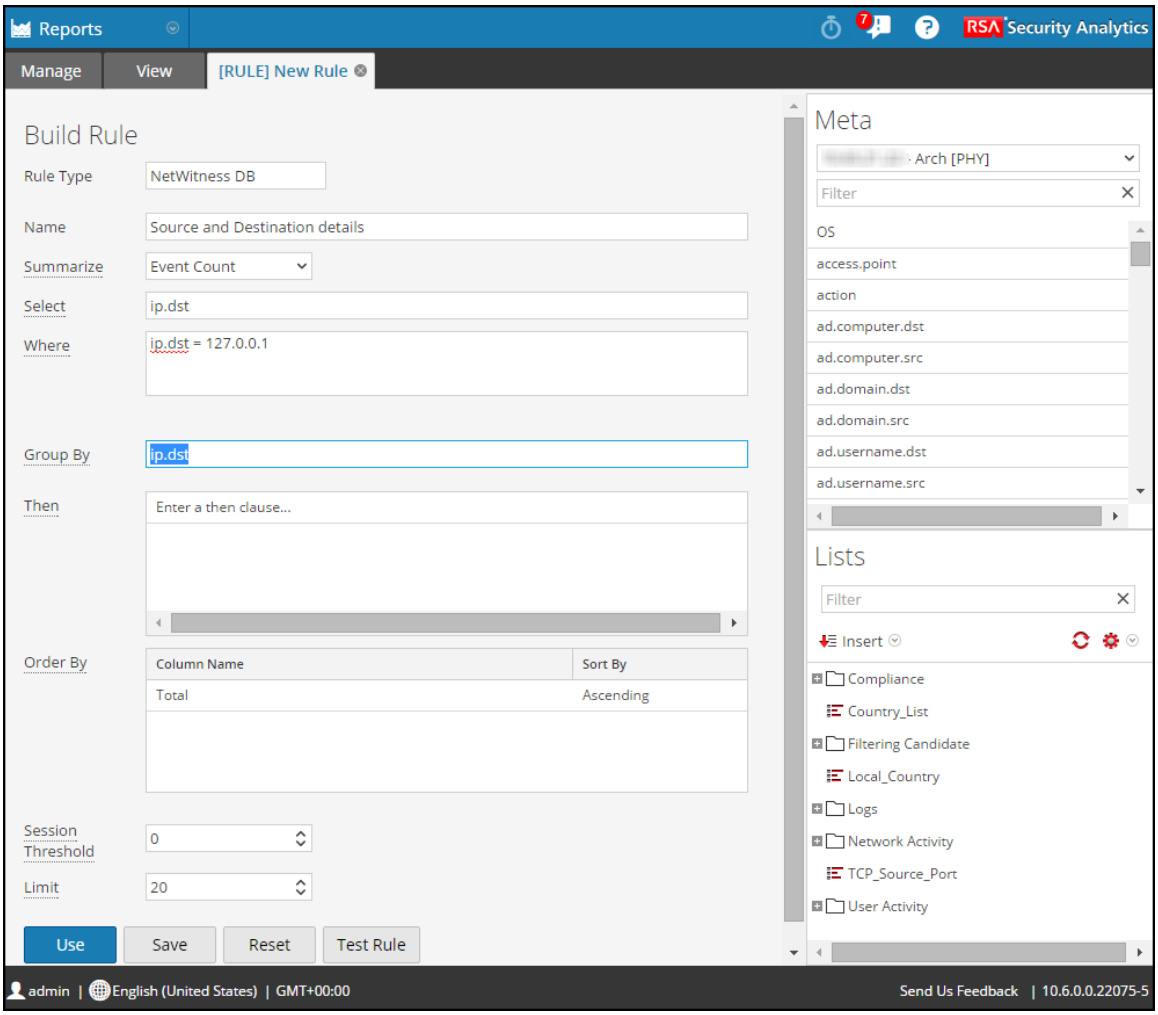
En el panel Reglas puede ejecutar las siguientes acciones:

- Definir y guardar una regla.
- Restablecer los valores de la regla.
- Probar la exactitud de la regla.
- Agregar la regla a un informe.
- Agrega la regla a la línea de espera de alertas.
- Agrega la regla a un gráfico.

Para acceder a la vista Crear regla:

1. En el menú de Security Analytics, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. En la barra de herramientas Regla, haga clic en  > **Base de datos de NetWitness**.
   Se muestra la pestaña de la vista Crear regla

La siguiente figura es un ejemplo de la vista Crear regla.



Características

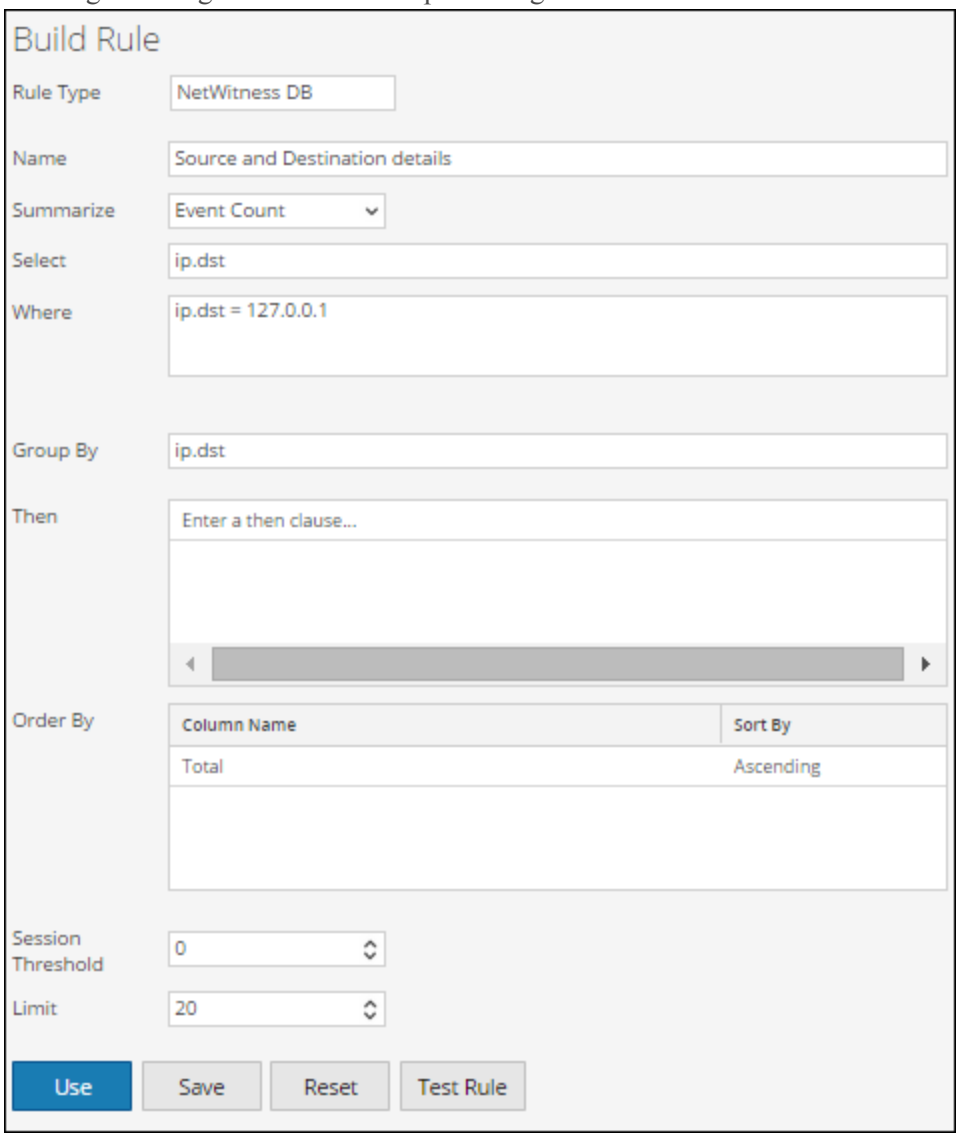
La vista Crear regla incluye los siguientes paneles:

- Panel Regla
- Panel Metadatos
- Panel Listas

Panel Regla

El panel Regla le permite crear una regla para el tipo de base de datos seleccionado.

En la siguiente figura se muestra el panel Regla.



En la siguiente tabla se describen las funciones del panel Regla.

Característica	Descripción
Tipo de regla	Una lista desplegable de tipos de base de datos compatibles para los cuales puede crear reglas. Las opciones son: Base de datos Netwitness, IPBD y base de datos de Warehouse.
Nombre	El nombre de la regla que se creará o editará.

Característica	Descripción
Resumen	Una lista desplegable de opciones de resumen. Las opciones son: Ninguno, conteo de eventos, conteo de paquetes, conteo de sesiones y personalizado.
Seleccionar	La clave de metadatos para la cual necesita los valores agregados; por ejemplo, ip.dest.
Donde	Una cláusula Where que define las condiciones que activan la ejecución de la regla; por ejemplo, ip.dest = 127.0.0.1.
Agrupar por	El método de agrupación de los resultados. Por ejemplo, la especificación de ip.dest genera un informe en el cual se agrupan valores semejantes a ip.dest.
A continuación	Una cláusula Then que define las acciones de regla para procesamiento adicional en la salida.
Ordenar por	El método de secuenciación utilizado para mostrar los resultados. Por ejemplo, si se especifica ordenar de forma ascendente el valor en la columna Total, se produce un informe en el cual los resultados se clasifican en orden ascendente según el valor de la columna Total.
Umbral de sesión	Una lista de selección para el umbral de sesión, la cual especifica la cantidad máxima de sesiones que se deben procesar para las funciones de agregado.
Límite	Una lista de selección para la cantidad máxima de filas de resultados que se recuperarán.
Usar	Cuando hace clic en Usar, se le permite usar la regla para generar un informe Alerta de gráfico.
Guardar	Cuando hace clic en Guardar, se guarda la regla que está editando y el panel Crear regla permanece abierto. Antes de probar una regla, debe guardarla si desea conservar sus cambios.

Característica	Descripción
Restablecer	Cuando hace clic en Restablecer, se borra toda la información del campo.
Probar regla	Cuando hace clic en Probar regla, se abre el cuadro de diálogo Probar regla.

Cuadro de diálogo Probar regla

Para acceder a la vista Probar regla:

1. En el menú de Security Analytics, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. En el panel Lista de reglas, realice una de las siguientes acciones:

   - Seleccione una regla y haga clic en en la barra de herramientas Reglas.
   - Haga clic en > **Editar**.
     Se muestra la pestaña de la vista Crear regla.
3. Haga clic en **Probar regla**.
   Se muestra la vista Probar regla.

En la siguiente tabla se describen las funciones del cuadro de diálogo Probar regla.

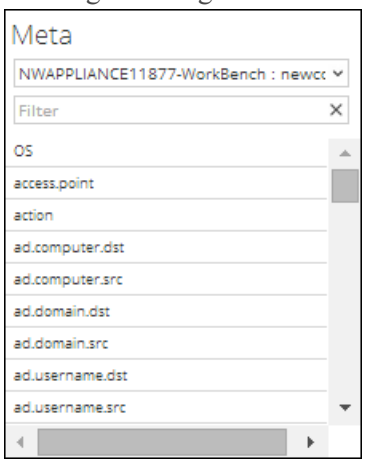
Característica	Descripción
Origen de datos	Una lista desplegable de orígenes de datos para el tipo de regla que se está probando. Posibles orígenes de datos son: Concentrator, Broker, Decoder o Log Decoder.
Formato	Una lista desplegable de los formatos para mostrar los resultados de la regla. Formatos posibles: Tabular, área, barras, burbujas, columna, línea, circular, línea escalonada, área escalonada, área de spline y spline.
Rango de tiempo	Una lista desplegable de métodos de especificación de rango de tiempo. • Seleccionar Pasado permite especificar una cantidad de años, meses, días, semanas u horas. Por ejemplo,horas, días, semanas, meses o años. • Seleccionar Rango permite especificar un rango de fechas y un período. Por ejemplo, fecha de inicio a fecha de finalización. En la interfaz del usuario, la fecha o la hora que se muestran dependen del perfil de zona horaria que seleccionó el usuario.
Usar cálculo de tiempo relativo	Si selecciona esta opción, calcula el rango de tiempo con respecto a la hora actual.
Eje X	Eje X y Eje Y especifican los metadatos que se trazarán en los gráficos. En la lista desplegable Eje X se enumeran los tipos de metadatos correspondientes a la configuración `Group by` de la regla. Cuando la regla tiene una sola configuración `Group by`, puede seleccionar varios tipos de metadatos. Para las reglas personalizadas con varios valores `Group by`, puede seleccionar solo el primer tipo de metadatos en el Eje X.

Característica	Descripción
Eje Y	En la lista desplegable de Eje y, se enumeran las funciones de agregado que se usan en la regla. Sum, Count, Countdistinct y Average son las funciones de agregado compatibles con la regla. Puede seleccionar una o más funciones de agregado.
Ejecutar prueba	Hacer clic en Ejecutar prueba ejecuta una prueba de la última regla que se guardó en el cuadro de diálogo Generador de reglas. Cuando finaliza la prueba, se muestran los datos de la regla (en caso de haberlos) para el rango de tiempo seleccionado.

Panel Metadatos

El panel Metadatos proporciona una lista de los tipos de metadatos disponibles que puede usar para crear la regla. Puede usar los tipos de metadatos en las cláusulas Select, Where y Then. Reporting Engine mantiene una lista activa de los nombres de metadatos disponibles mediante una sincronización constante con el origen de datos al cual está conectado.

En la siguiente figura se muestra el panel Metadatos.



En la siguiente tabla se describen las funciones del panel Metadatos.

Operation	Descripción
Elegir	De acuerdo con el tipo de regla que seleccionó, los orígenes de datos disponibles se muestran en la lista desplegable del panel Metadatos. Seleccione el origen de datos requerido. Se muestran los tipos de metadatos disponibles para el origen de datos. Seleccione metadatos.

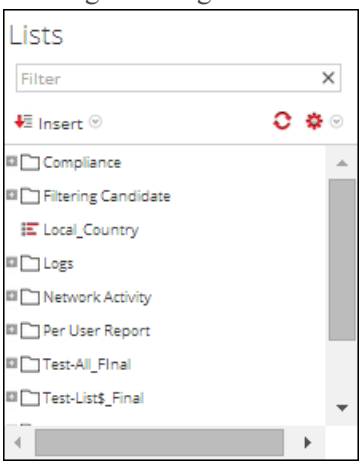
Operation	Descripción
Filtro	Filtre los metadatos para un valor de metadatos específico.

Panel Lista

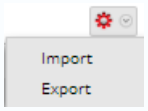
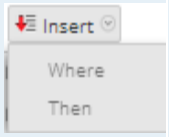
Una lista es un marcador de posición de un conjunto de valores que puede usar en los metadatos o en una variable. Por ejemplo, puede definir una lista con todas las direcciones IP de orígenes de eventos que están en una lista blanca. Una vez que la lista se ha definido, puede usar el nombre de la lista en la regla. Esto proporciona la flexibilidad para agregar, modificar y eliminar los valores de lista.

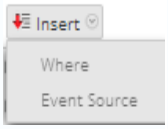
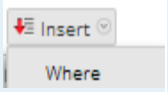
El panel Listas es una recopilación de listas. Reporting Engine mantiene una lista activa de los nombres de lista disponibles mediante la sincronización continua con la recopilación a la cual está conectado.

En la siguiente figura se muestra el panel Listas.



En la siguiente tabla se describen las funciones del panel Listas.

Operation	Descripción
	Importar o exportar una lista.
	Si selecciona el tipo de regla **Base de datos de NetWitness**, se muestran las opciones Where y Then. Inserte la lista en la cláusula Where o Then en la regla.

Operation	Descripción
	Si selecciona el tipo de regla **IPDB**, se muestran las opciones Where y Origen de evento. Inserte la lista en la cláusula Where u Origen de evento en la regla.
	Si selecciona el tipo de regla **Base de datos de Warehouse**, se muestra la opción Where. Inserte la lista en la cláusula Where en la regla.

Agregados de consulta

En este tema se describen los escenarios de los agregados de consulta de NWDB. Para usar agregados de consulta se requiere comprender la sintaxis de reglas de NWDB. Para obtener más información, consulte Sintaxis de reglas de NWDB.

Funciones adicionales compatibles

En la siguiente tabla se enumeran las funciones de agregado compatibles.

Función de agregado	Descripción	Tipos de datos de entrada	Tipos de datos de salida
count	Devuelve el conteo de valores de metadatos, el cual también incluye valores duplicados.	Numérico	Numérico
countdistinct	Devuelve la cantidad total de valores distintos o únicos.	Numérico	Numérico
distinct	Devuelve todos los valores únicos.	Cualquiera	Cualquiera
first	Devuelve la primera aparición del valor de metadatos.	Cualquiera	Igual que la entrada
last	Devuelve la última aparición del valor de metadatos.	Cualquiera	Igual que la entrada

Función de agregado	Descripción	Tipos de datos de entrada	Tipos de datos de salida
sum	Devuelve una suma de todos los valores no nulos de la clave de metadatos en un grupo.	Numérico	Numérico
avg (promedio)	Devuelve el valor promedio de todos los valores no nulos de la clave de metadatos dentro de un grupo.	Numérico	Numérico
min (mínimo)	Devuelve el mínimo de todos los valores de la clave de metadatos en cada grupo. Este valor se basa en el campo Ordenar por.	Cualquiera	Cualquiera
max (máximo)	Devuelve el máximo de todos los valores de la clave de metadatos en cada grupo. El valor máximo es el valor que devuelve el campo Ordenar por.	Cualquiera	Cualquiera
length	Devuelve la longitud de los valores de la clave de metadatos. A esto se denomina una “función escalar” en SQL.	Cualquiera	Numérico

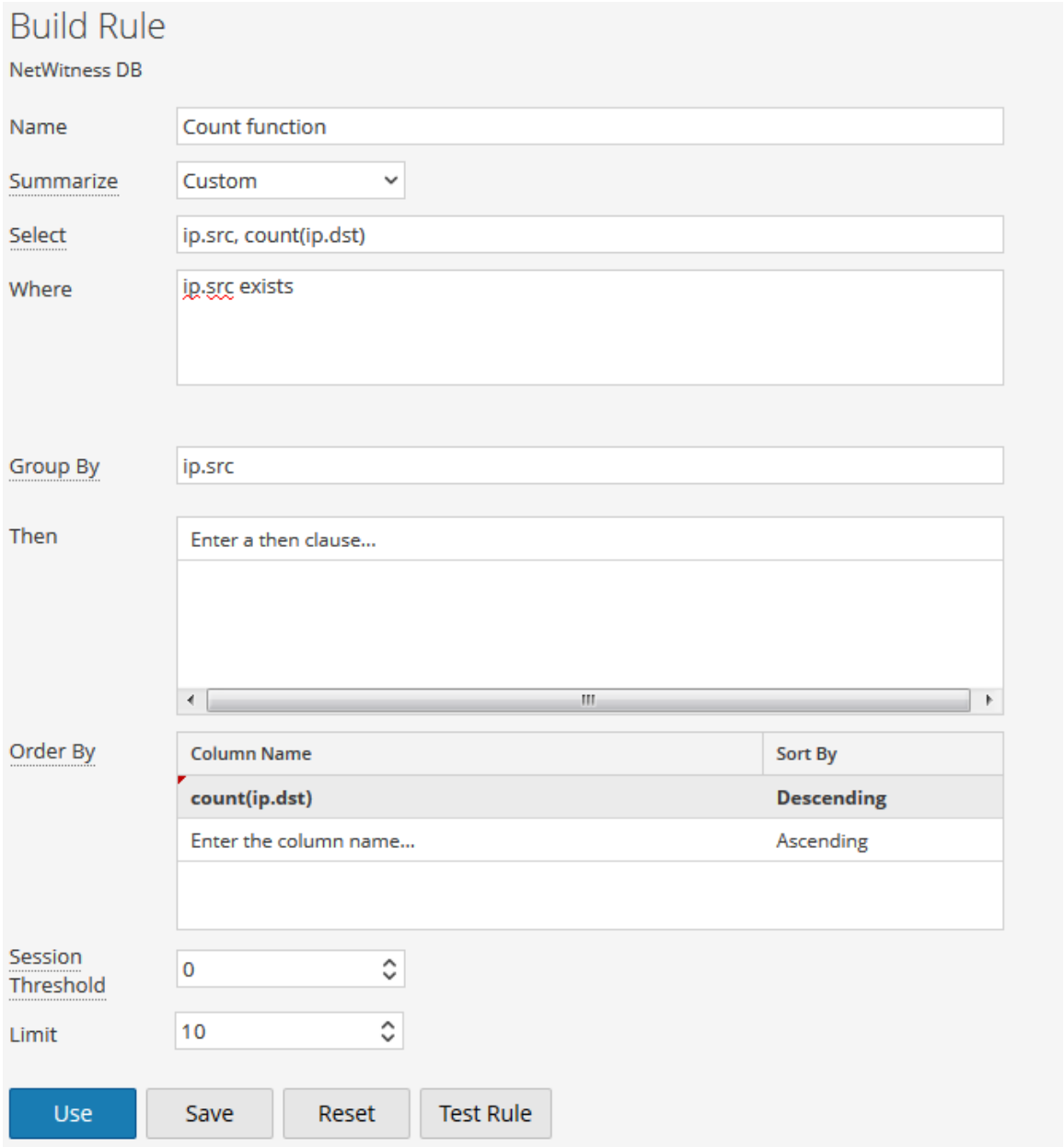
Ejemplos de consultas y resultados por función

Count

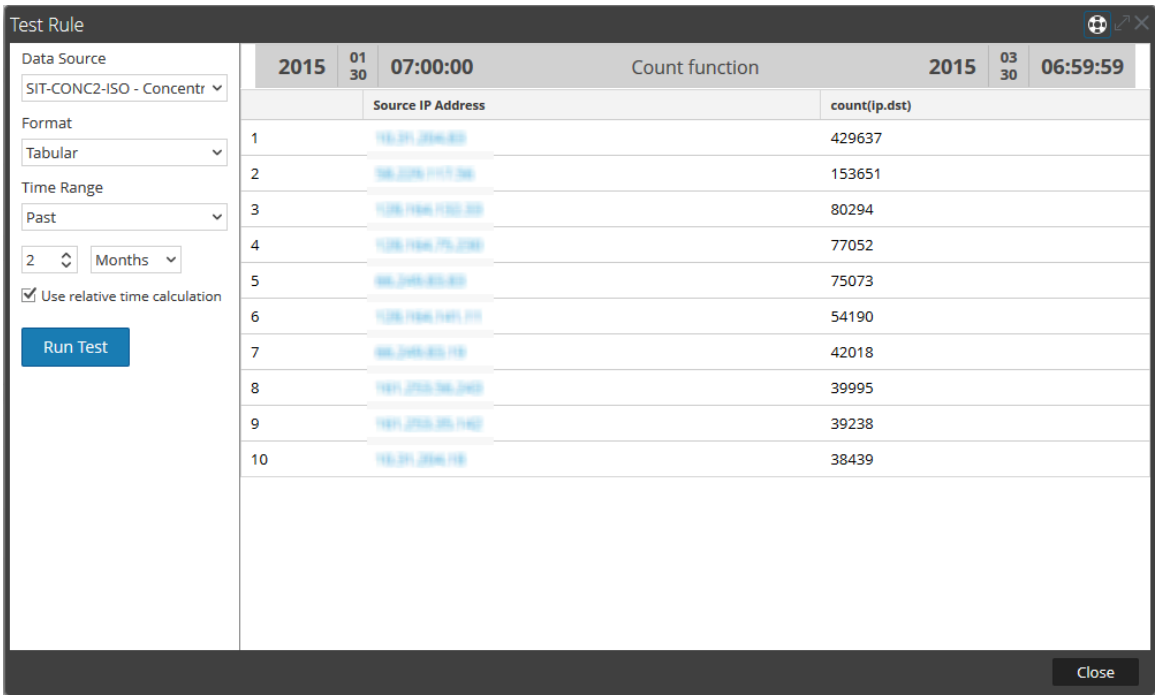
Esta función devuelve la cantidad de valores para una clave de metadatos especificada y excluye los valores nulos, pero incluye los duplicados.

Ejemplo

En la siguiente figura se muestra un ejemplo de consulta de la función count que se usa para la dirección IP de destino y la respectiva dirección IP de origen.



En la siguiente figura se muestra el resultado de la consulta anterior.



Aquí, para cada ip.src (dirección IP de origen) única, la página devuelve la cantidad total o el conteo de valores ip.dst (dirección IP de destino), el cual también incluye los valores duplicados.

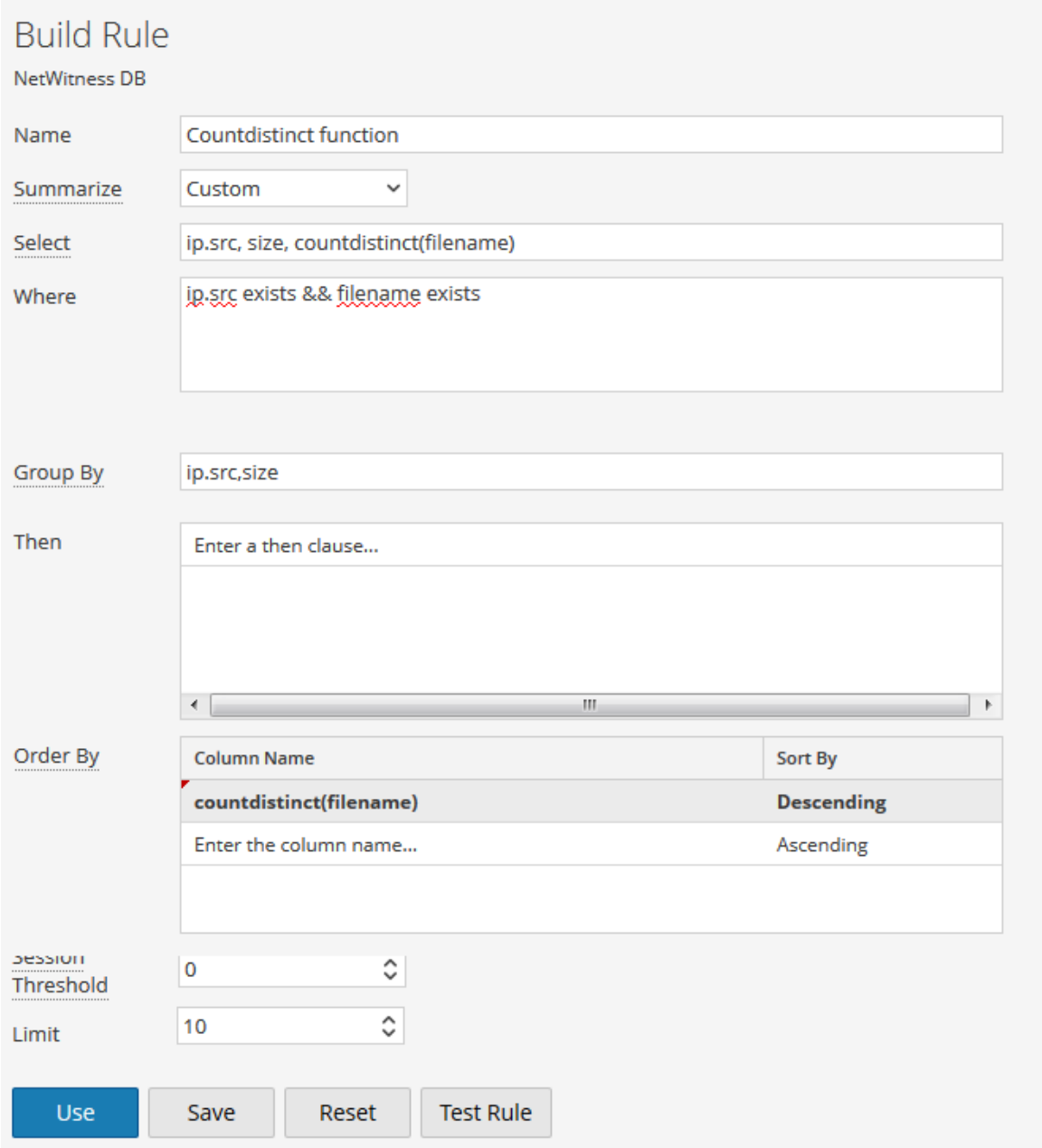
Nota: Si la versión actual de RSA Security Analytics es 10.5 o una más nueva y las versiones de cualquiera de los dispositivos de Security Analytics Core son 10.3 o 10.4, algunas de las funciones de agregado pueden mostrar errores inesperados. Sin embargo, las funciones de agregado como sum() y count() son compatibles con la versión 10.4.

Countdistinct

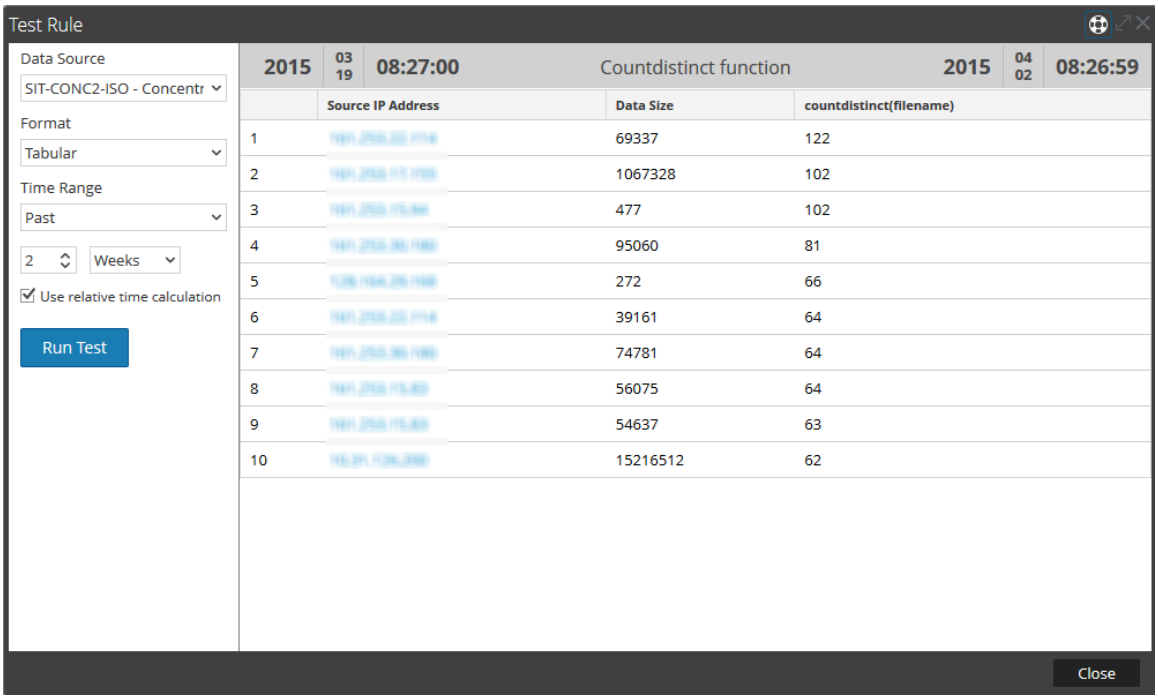
La función countdistinct devuelve el conteo de valores únicos o distintos para la clave de metadatos. Es decir, la función countdistinct se puede usar para recuperar una cantidad de valores distintos para la clave de metadatos especificada.

En la siguiente figura se muestra un ejemplo de consulta en el cual se usa la función countdistinct junto con la dirección IP de origen (ip.src) y el tamaño de los datos (size).

Ejemplo



En la siguiente figura se muestra el resultado de la consulta anterior.



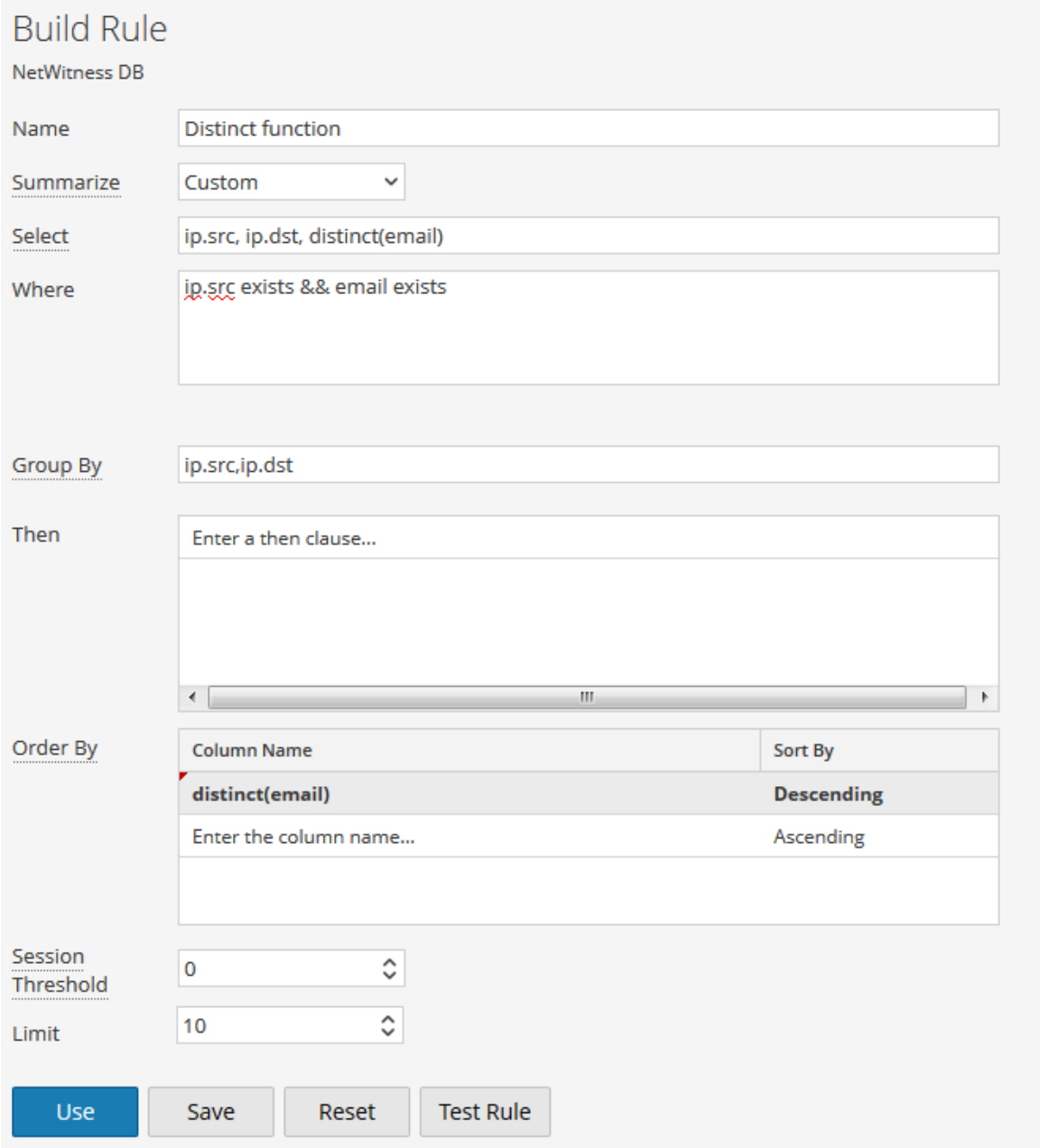
Aquí, la página muestra el tamaño de los datos junto con la cantidad total o el conteo de nombres de archivo distintos desde la respectiva dirección IP de origen. A diferencia de la función count, countdistinct excluye del resultado los valores duplicados.

Distinct

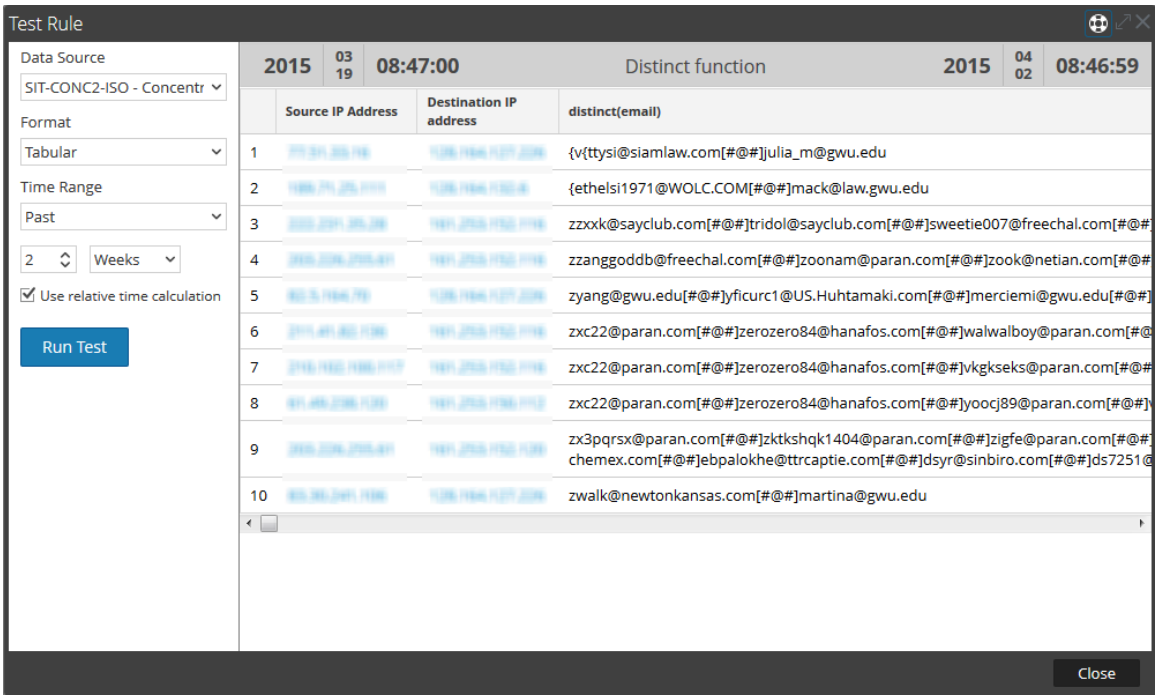
Esta función devuelve todos los valores únicos o distintos de la clave de metadatos.

Ejemplo

En la siguiente figura se muestra un ejemplo de consulta de la función distinct que se usa para recuperar correos electrónicos entre varias direcciones IP de origen y destino (ip.dst).



En la siguiente figura se muestra el resultado de la consulta anterior.



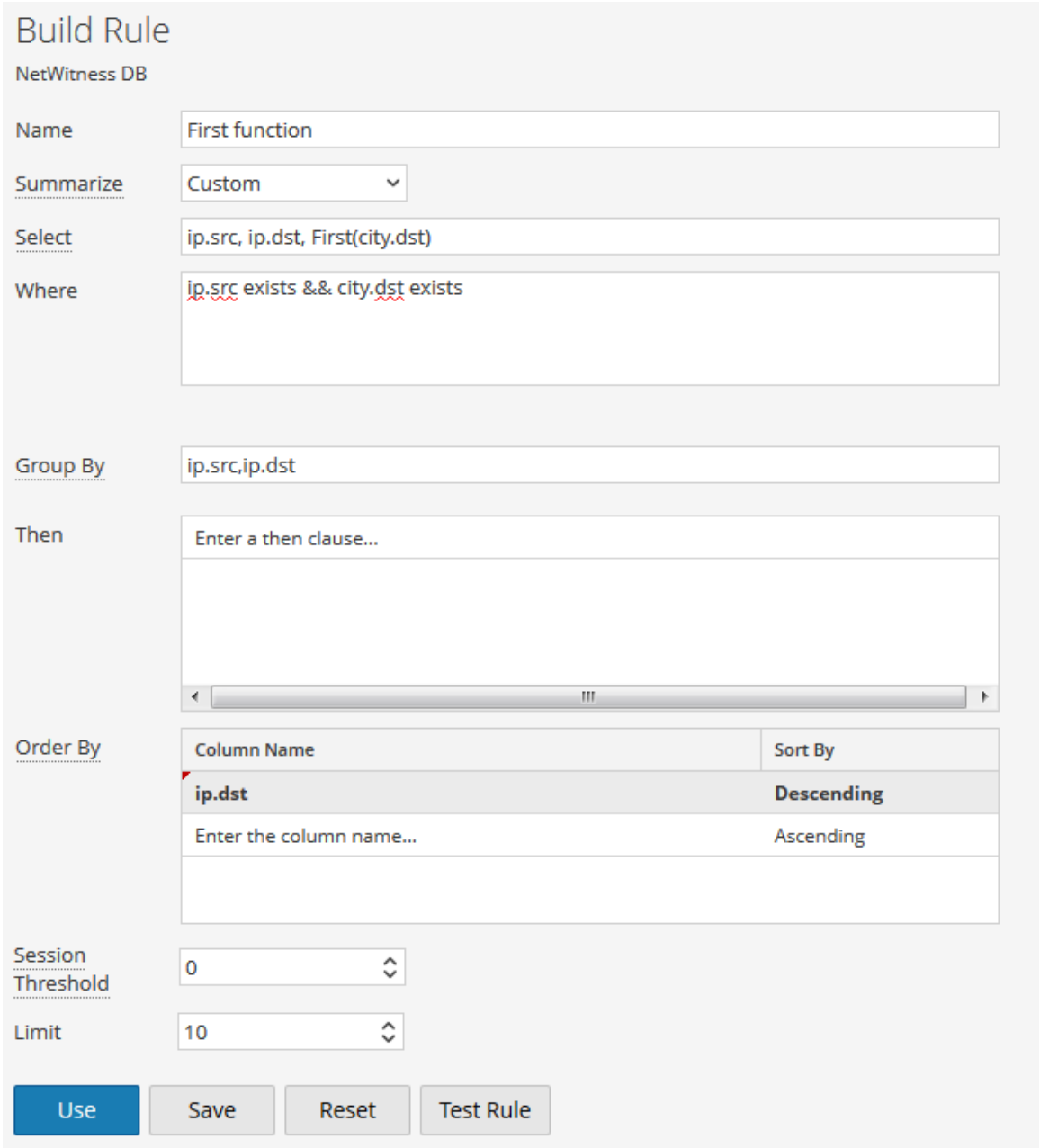
Aquí, la página muestra la lista de correos electrónicos únicos que se intercambiaron entre las respectivas direcciones IP de origen y destino.

Primero

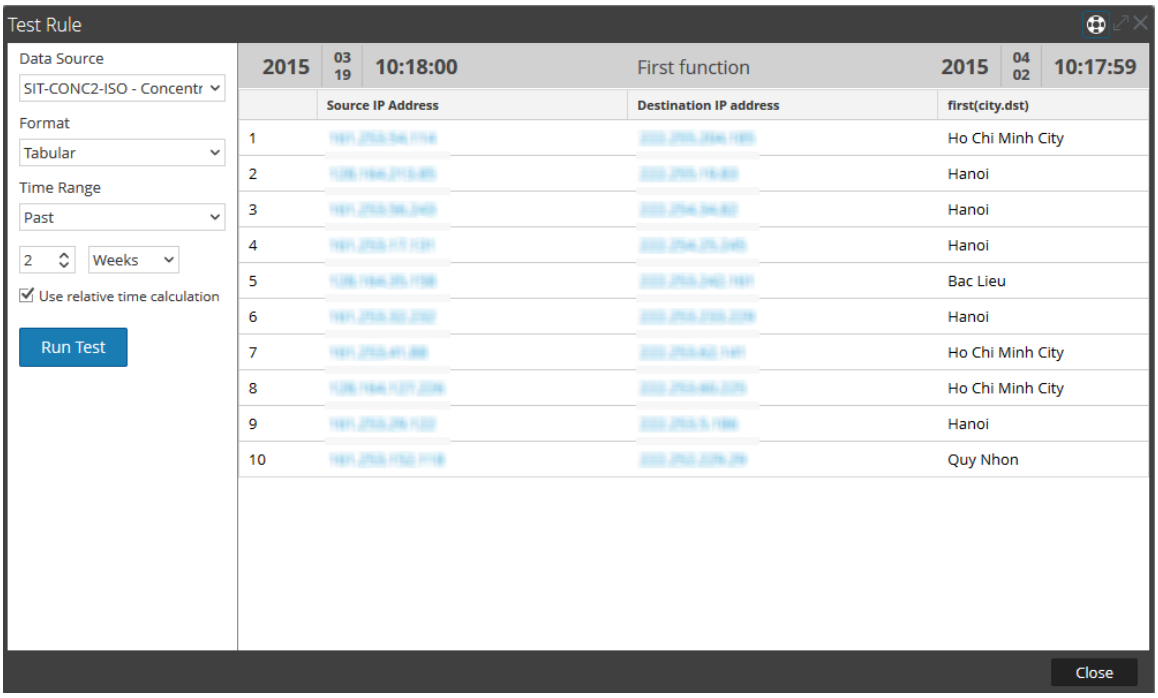
Esta función se usa para recuperar el primer valor de una secuencia ordenada de valores para una clave de metadatos especificada.

Ejemplo

En la siguiente figura se muestra un ejemplo de consulta de la función first que se usa para recuperar el primer nombre de ciudad de destino.



En la siguiente figura se muestra el resultado de la consulta anterior.



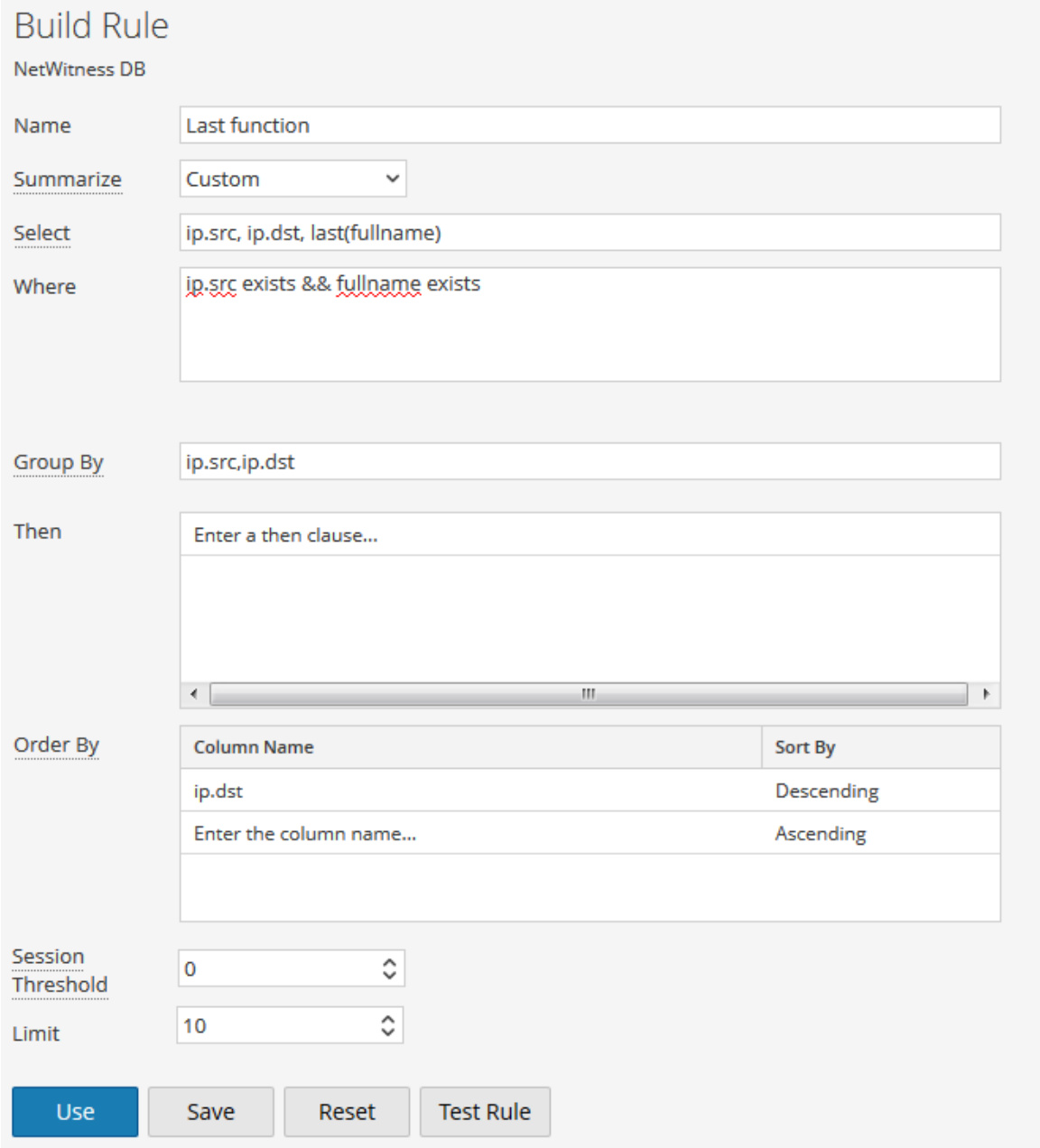
Aquí, la página muestra la primera ciudad de destino para las direcciones IP de origen y destino correspondientes. Puede usar la función first para aislar un valor específico de un resultado de búsqueda.

Última

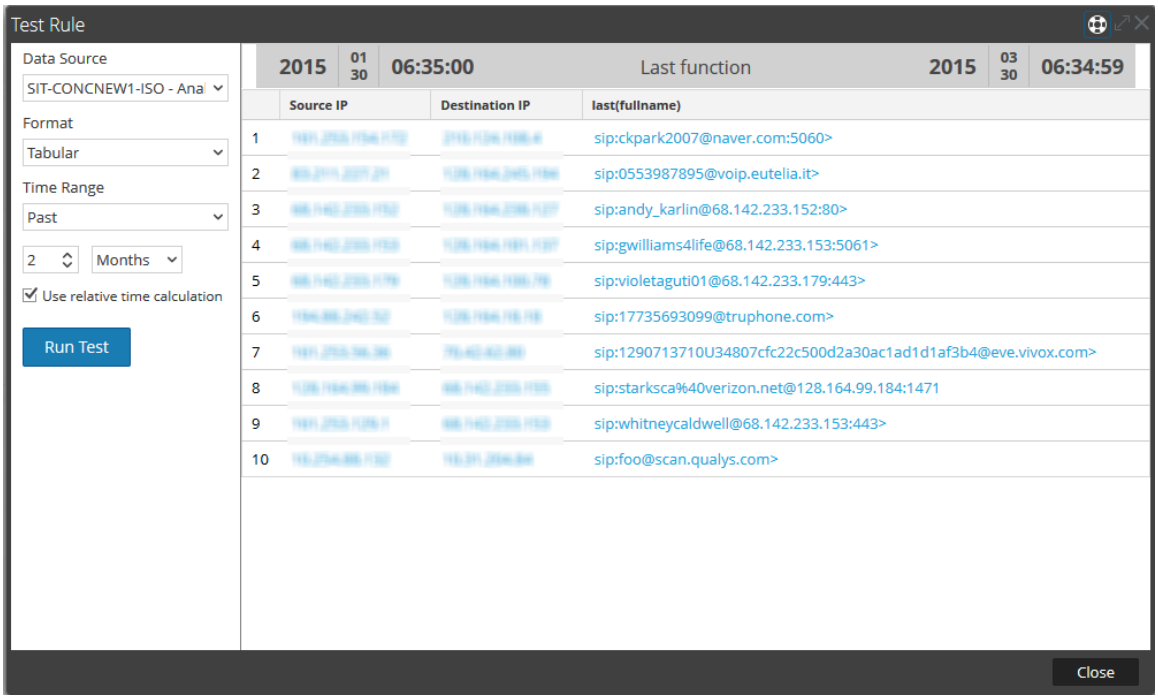
Esta función se usa para recuperar el último valor de una secuencia ordenada de valores para una clave de metadatos especificada.

Ejemplo

En la siguiente figura se muestra un ejemplo de consulta de la función last que se usa para recuperar el nombre de usuario más reciente.



En la siguiente figura se muestra el resultado de la consulta anterior.



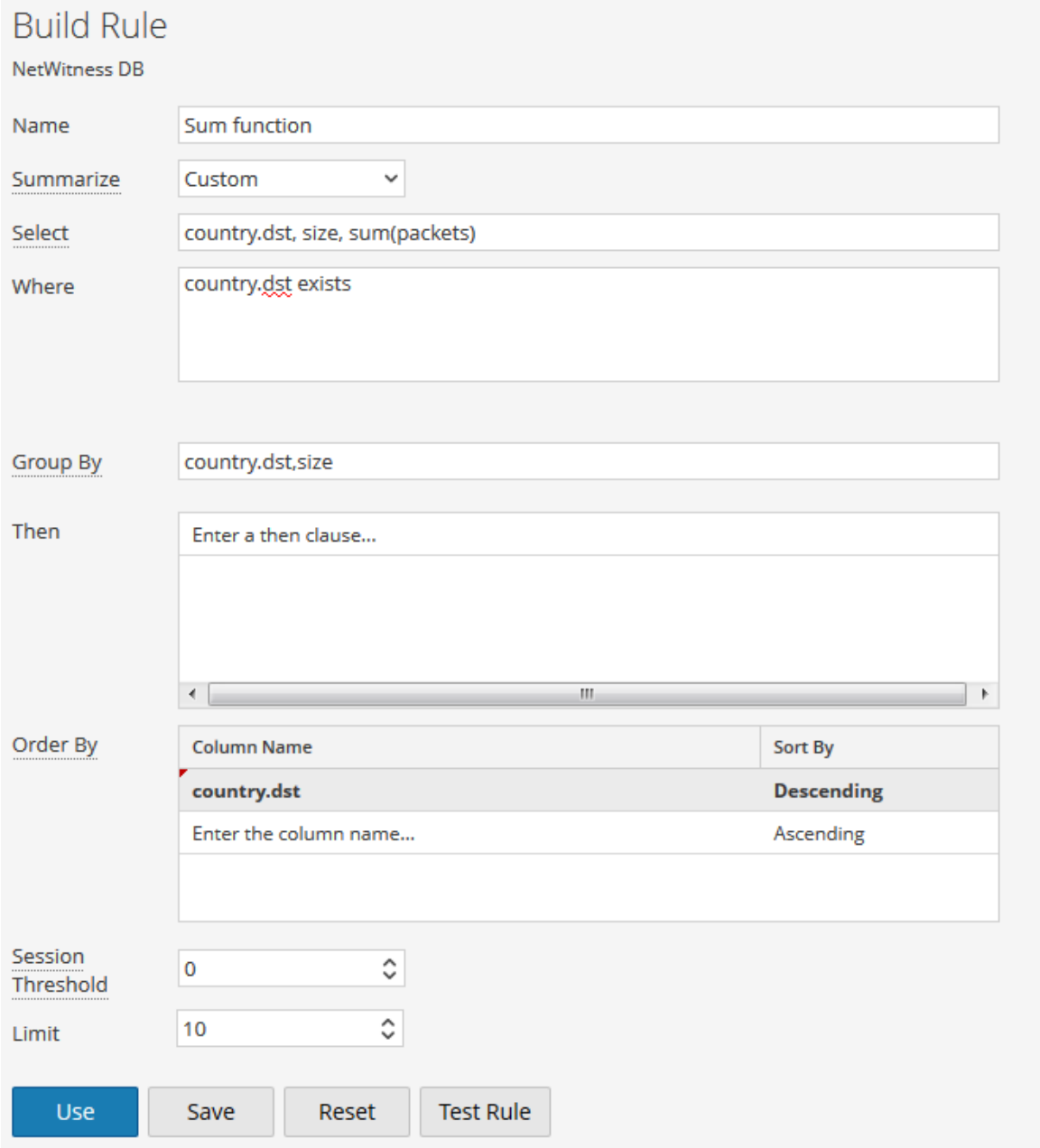
Aquí, la página muestra la lista completa de nombres de usuario más recientes o últimos que se intercambiaron entre las direcciones IP de origen y destino.

Suma

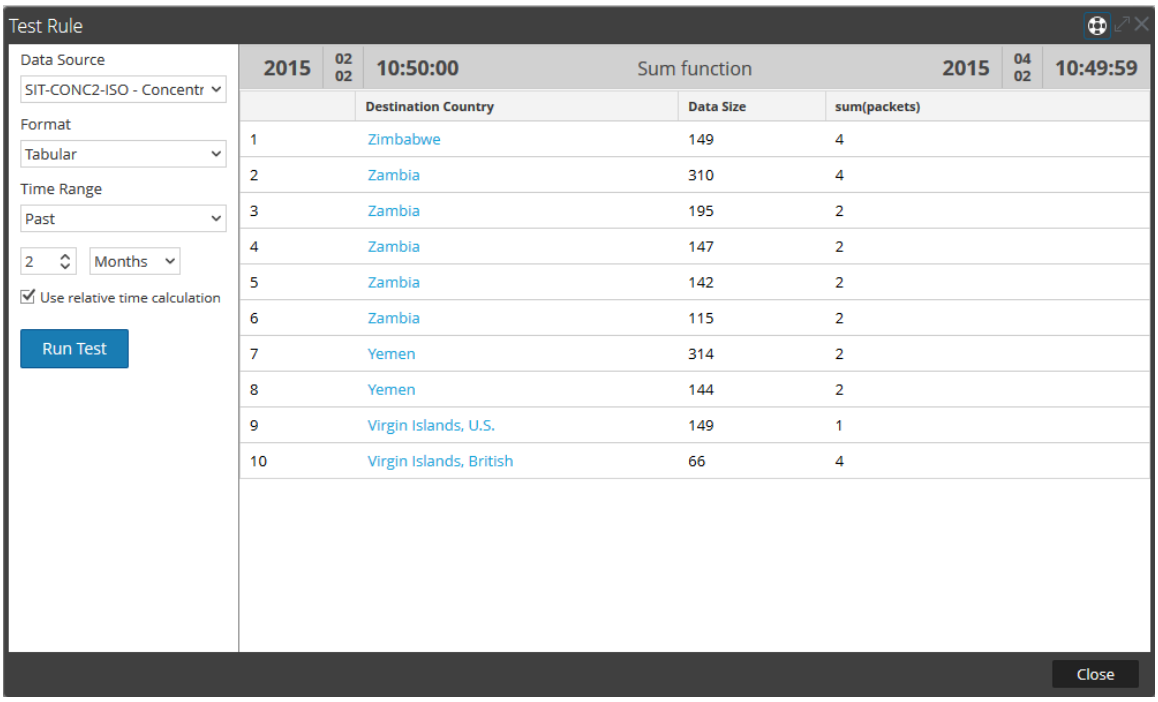
Esta función devuelve el total de los valores no nulos de la clave de metadatos dentro de un grupo.

Ejemplo

En la siguiente figura se muestra una consulta de la función Sum que se usa para paquetes.



En la siguiente figura se muestra el resultado de la consulta anterior.



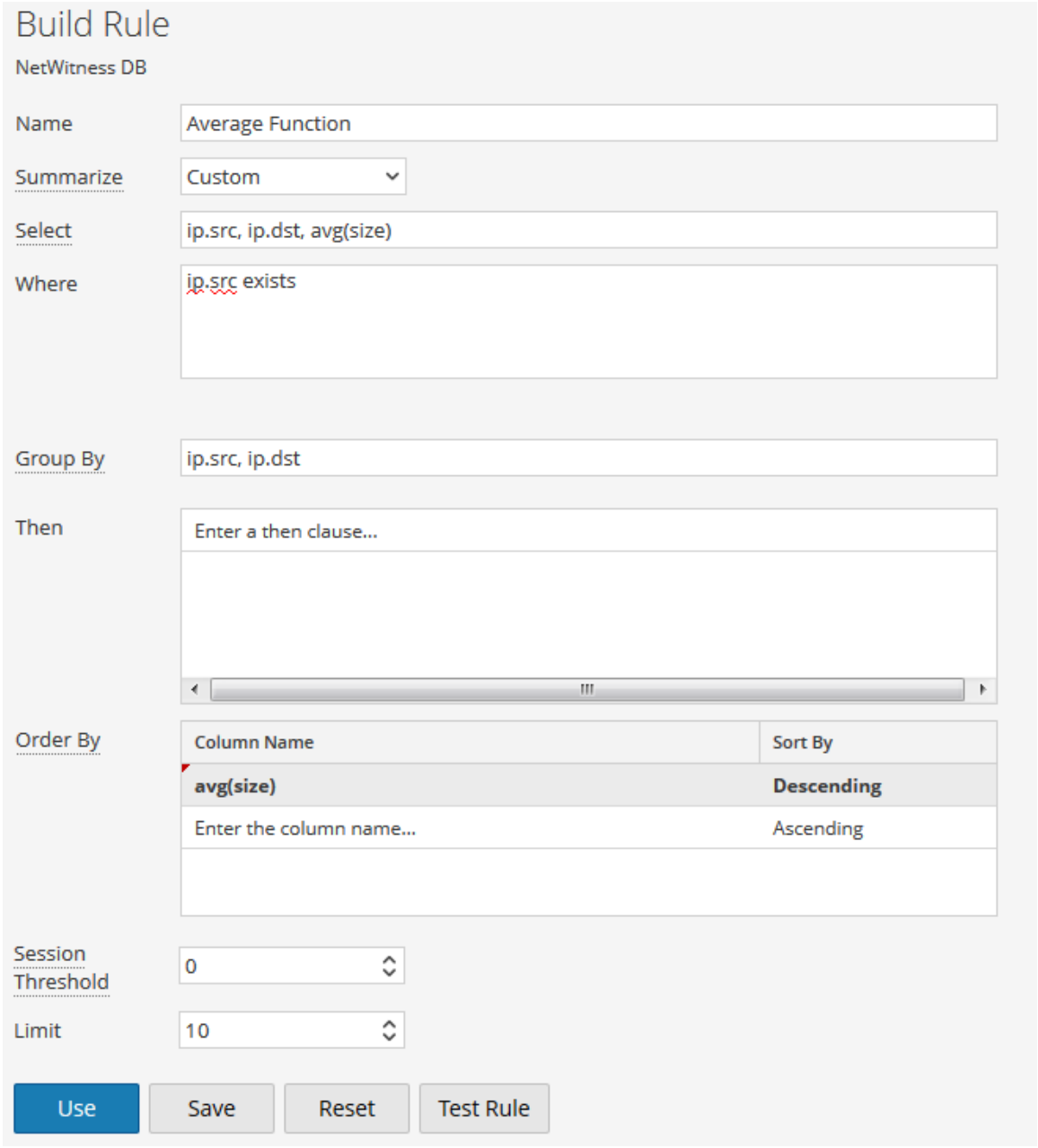
Aquí, la página muestra el total o la suma de los paquetes, junto con el tamaño de los datos para el respectivo país de destino.

Prom.

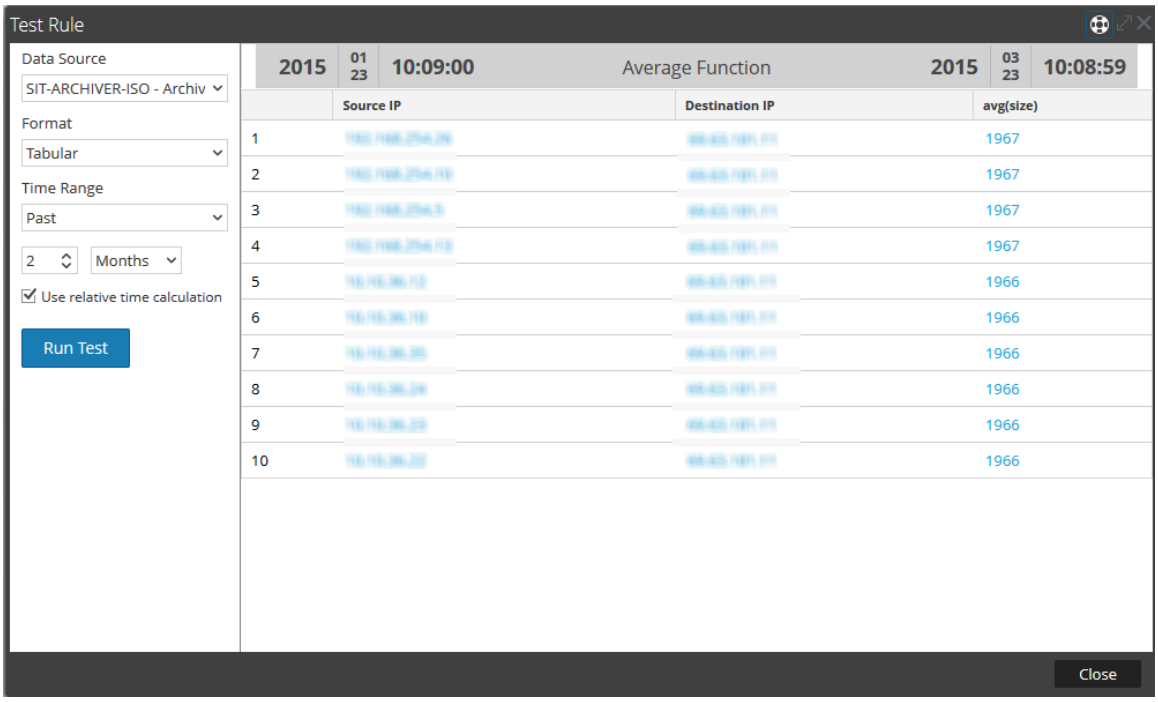
La función average devuelve el promedio de valores no nulos de los metadatos dentro de un grupo.

Ejemplo

En la siguiente figura se muestra un ejemplo de consulta del tamaño promedio de datos transmitidos entre una dirección IP de origen y de destino.



En la siguiente figura se muestra el resultado de la consulta anterior.



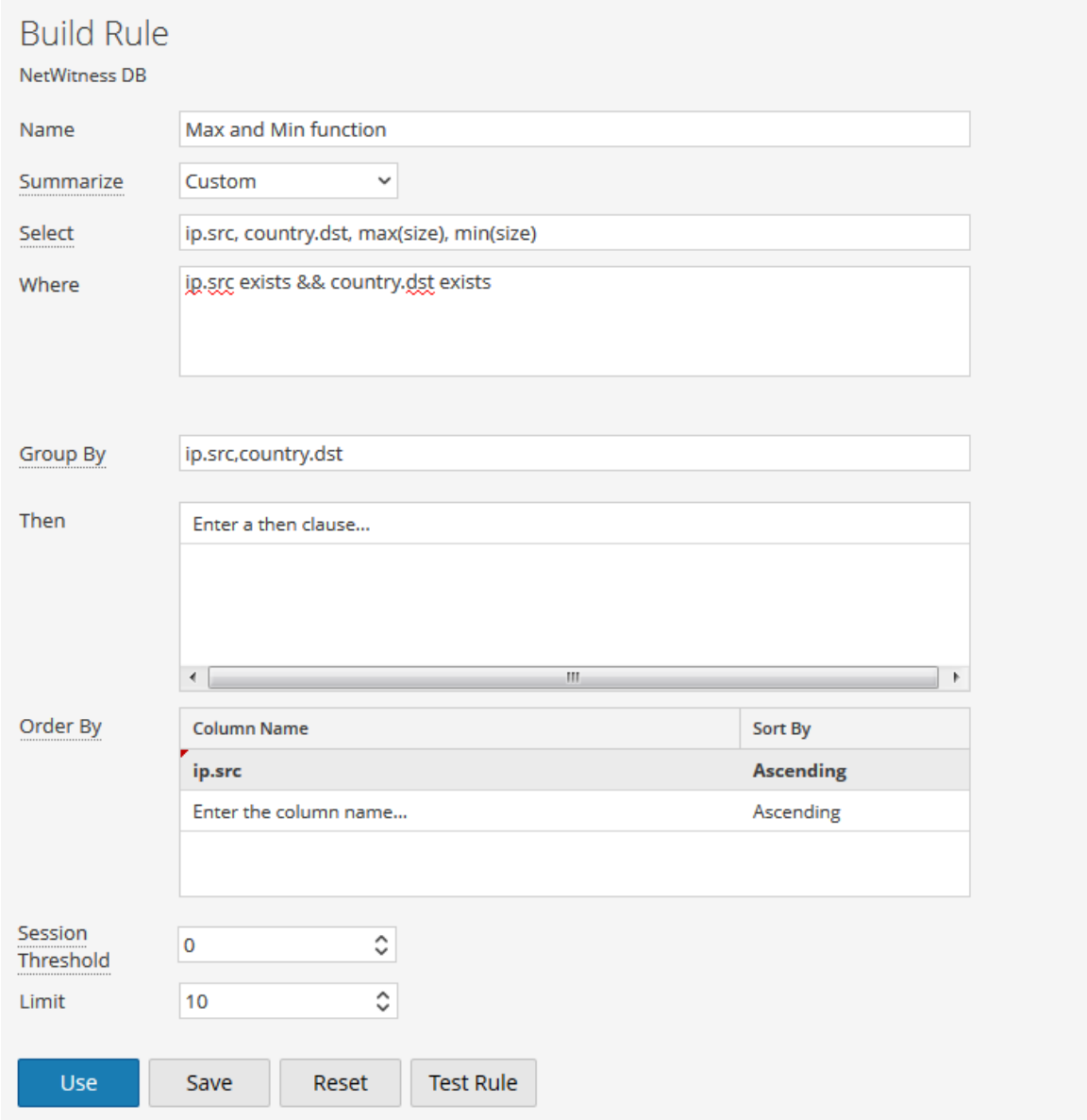
Aquí, la página muestra el tamaño promedio de los datos intercambiados entre una dirección IP de origen y de destino:

Max y Min

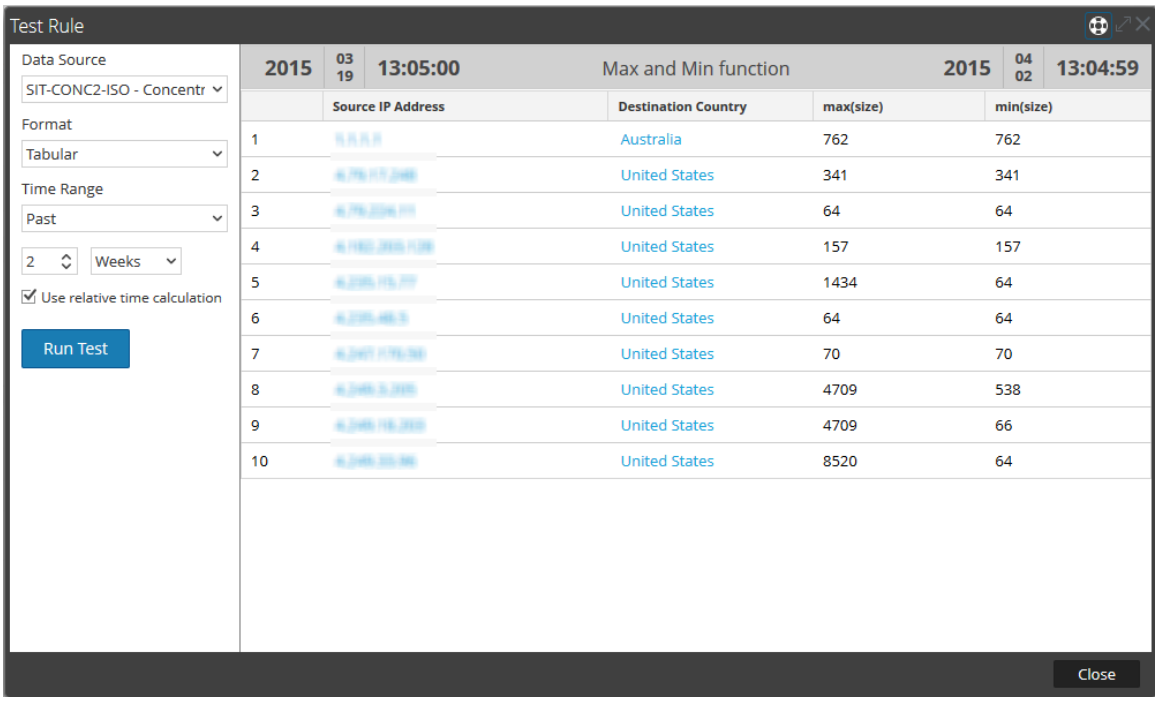
Las funciones Max y Min proporcionan el máximo y el mínimo de determinados valores de metadatos, respectivamente.

En la siguiente figura se muestra un ejemplo de consulta de las funciones max y min para diversos tamaños de datos para una dirección IP de origen y un país de destino.

Ejemplo



En la siguiente figura se muestra el resultado de la consulta anterior.



Aquí, la página muestra las columnas max(size) y min(size), junto con la lista de direcciones IP de origen y de países de destino. La columna max(size) enumera los tamaños máximos de datos que se intercambiaron, mientras que la columna min(size), los tamaños mínimos de datos que se intercambiaron.

Filtrar resultados de metadatos agregados con Max_threshold

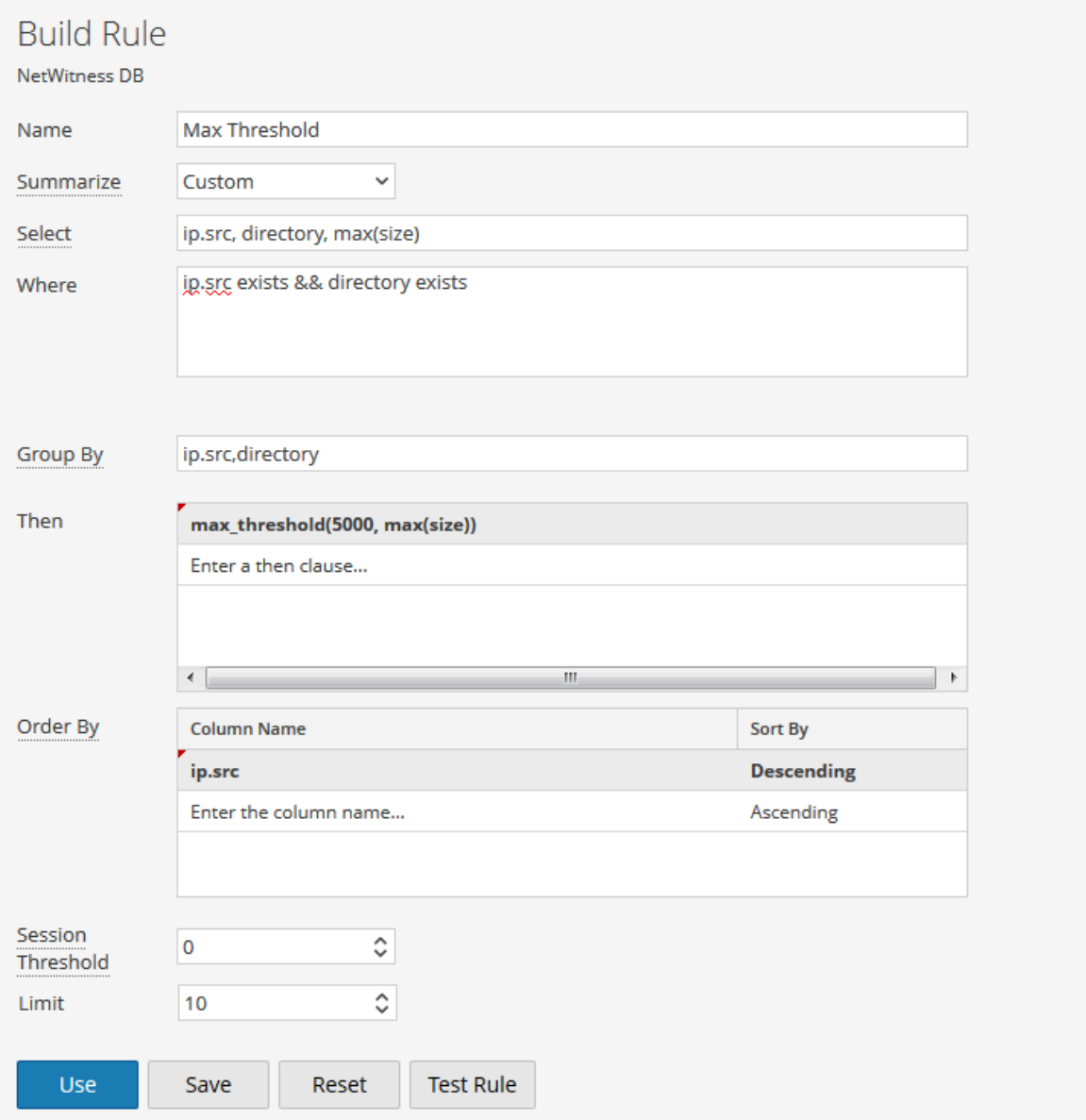
Puede filtrar los resultados de cualquier función mediante el uso de la acción de la regla de umbral.

Ejemplo

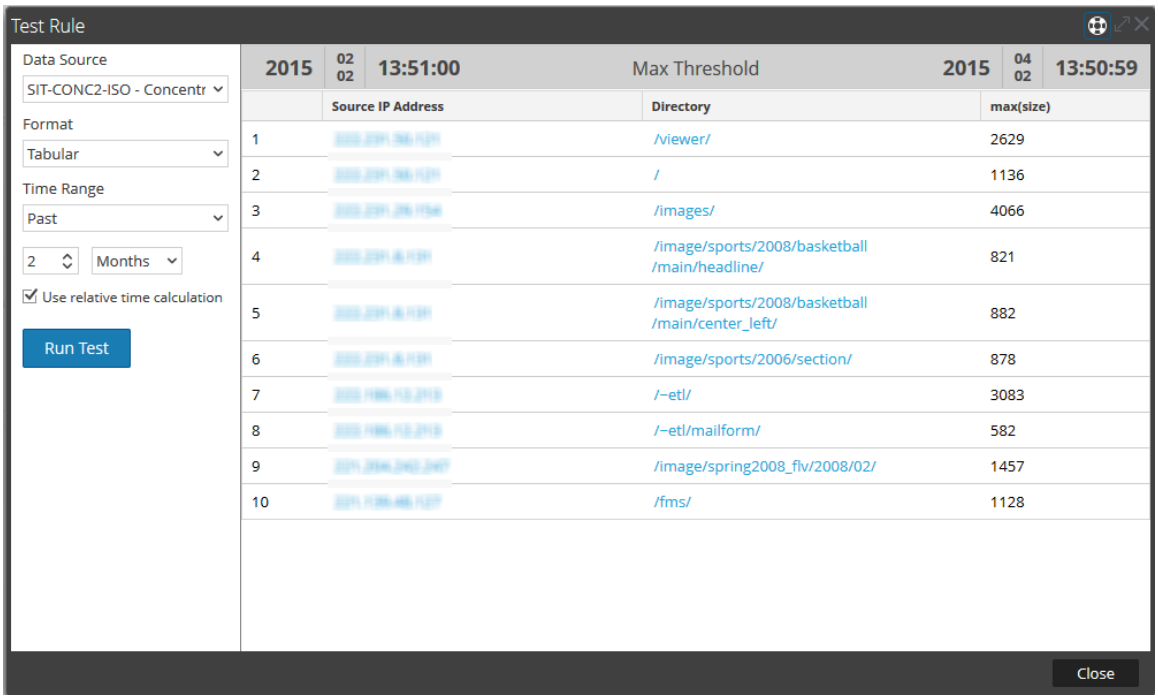
El siguiente es un ejemplo de consulta de max_threshold que se usa junto con la función Max en el campo **Then**:

max_threshold(5000,max(size))

En la siguiente figura se muestra la pantalla Crear regla para la consulta anterior.



Aquí, max_threshold se aplica al tamaño de datos con un límite superior de 5,000. En la siguiente figura se muestra el resultado.



Aquí, la página de resultados muestra la columna max(size) que enumera los tamaños de datos menores de 5,000, ya que este es el umbral máximo en la consulta, junto con la dirección IP de origen correspondiente y el respectivo directorio.

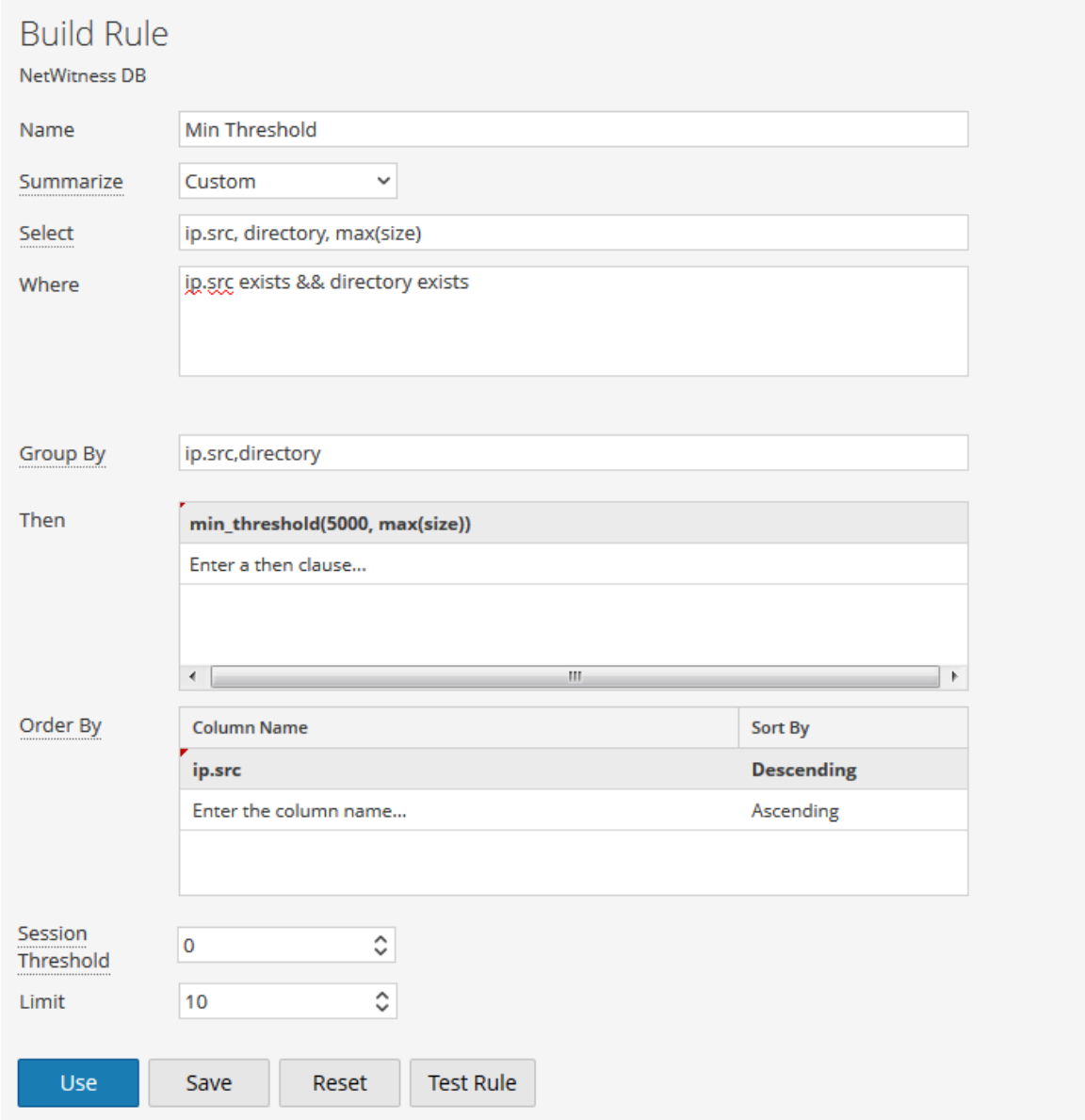
Filtrar resultados de metadatos agregados con Min_threshold

De manera similar, min_threshold se usa para filtrar los resultados de cualquier función. Para explicar esto, se considera un escenario similar al de max_threshold.

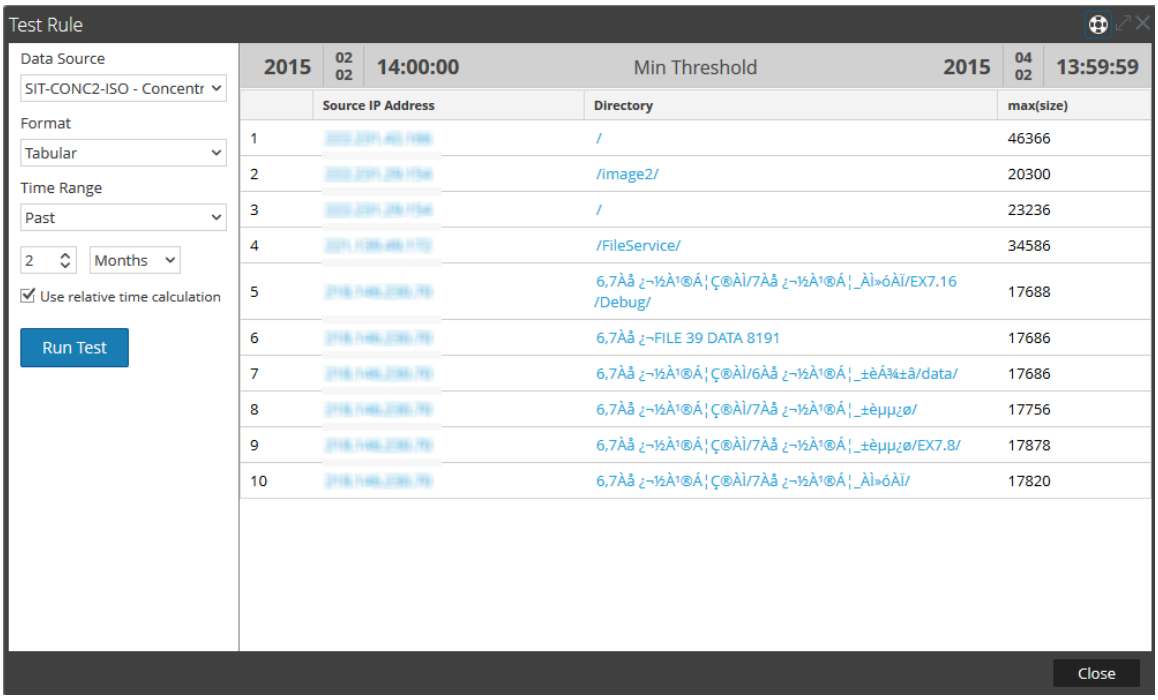
Ejemplo

La consulta de min_threshold que se usa junto con la función Max en el campo **Then** es:
min_threshold(5000,max(size))

En la siguiente figura se muestra la pantalla Crear regla para la consulta anterior.



Aquí, min_threshold se aplica al tamaño de datos con un límite inferior de 5,000. En la siguiente figura se muestra el resultado.



Aquí, la página de resultados muestra la columna max(size) que enumera los tamaños de datos mayores de 5,000, ya que este es el umbral mínimo en la consulta, junto con la dirección IP de origen correspondiente y el respectivo directorio.

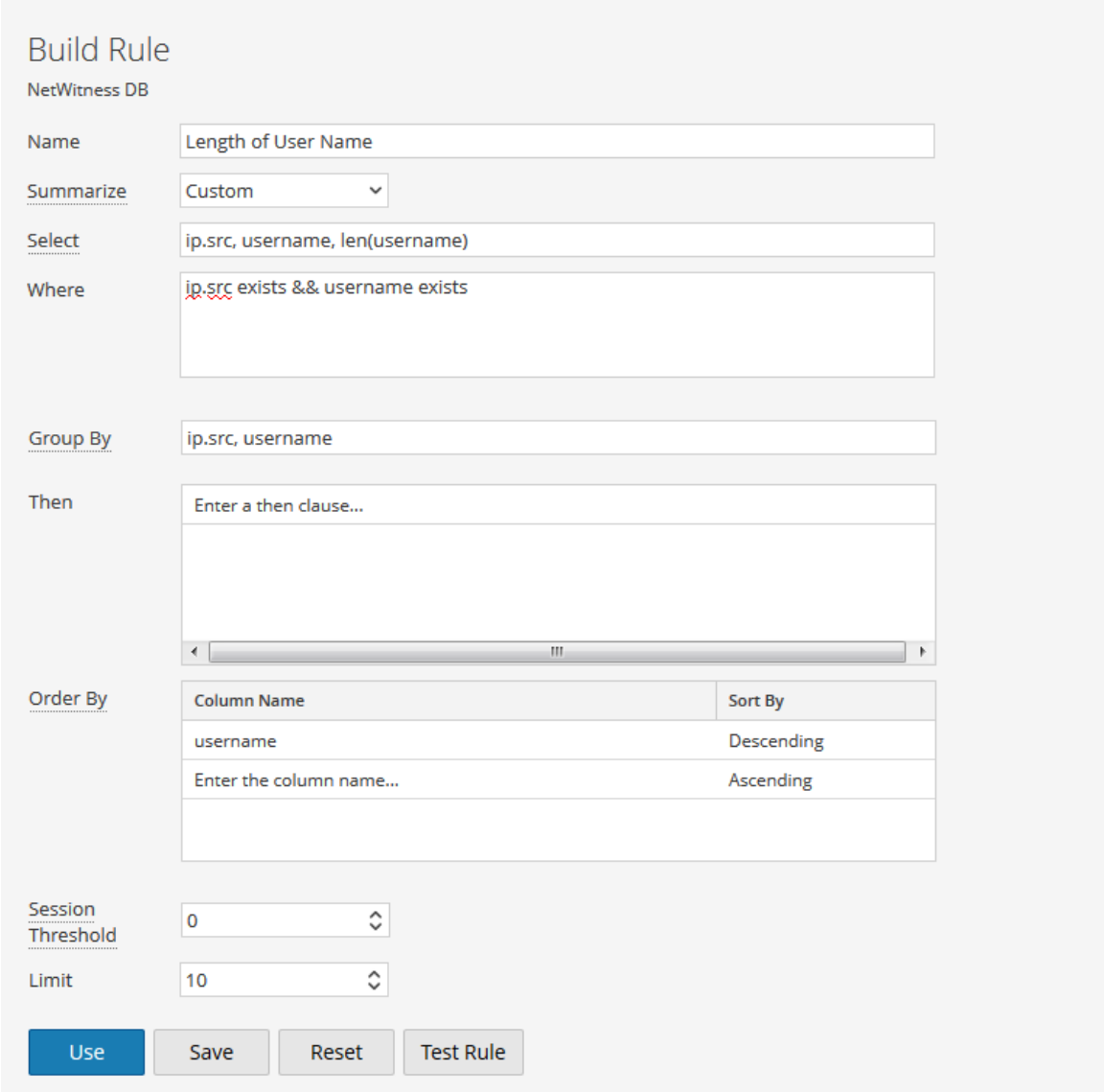
Nota: las acciones de las reglas Max_threshold y Min_threshold son comunes a todas las funciones y se pueden usar junto con otras consultas en el campo **Then** para recuperar la respectiva salida.

Longitud

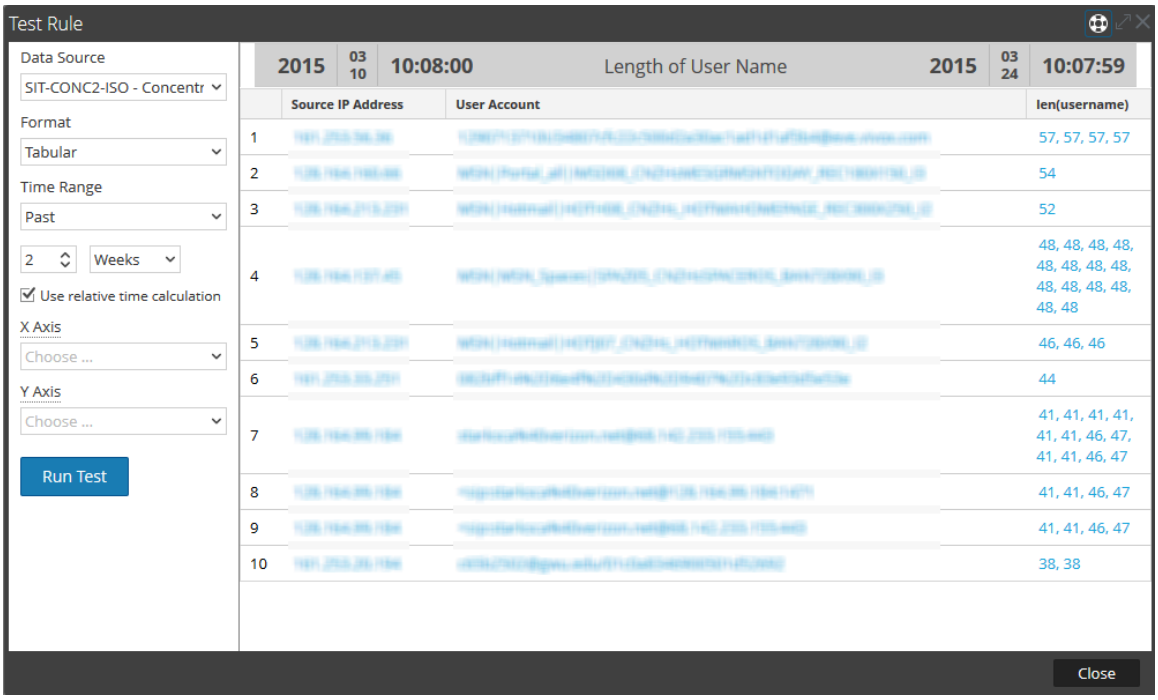
Esta función devuelve la longitud de un valor de metadatos. Es decir, la función Length devuelve la cantidad de bytes que se usan para almacenar el valor real.
Por ejemplo, para el valor “Analítica” se devuelve la longitud 9. De manera similar, para una ip.src IPv4 se devuelve 4 (que representa 4 bytes).

Ejemplo

En la siguiente figura se muestra un ejemplo de consulta de la función length que se usa para nombres de usuario.



En la siguiente figura se muestra el resultado de la consulta anterior.



Aquí, la página muestra la longitud de los nombres de usuario asociados a la cuenta de usuario y su respectiva dirección IP de origen.

Información adicional

Cuando consulta agregados (por ejemplo, sum(size)) con **Group By** en metadatos que tienen múltiples valores en una sesión, la sesión con múltiples valores se considera en el cálculo de agregados para cada valor de esos metadatos.

Ejemplo

Cuando consulta la función de agregado Count con Group By en Alias.host, si la columna tiene múltiples valores en una sesión, la sesión se cuenta para cada aparición, incluidos los valores duplicados.

Considere la siguiente tabla.

SessionID	Alias.host	Ip.src	Tamaño
1	host-a, host-b, host-a	a	10
2	host-b, host-c, host-a, host-c	c	20
3	host-b, host-c, host-d	b	30
4	host-c, host-a	a	40

En la tabla anterior, alias.host para **host-a** y **host-c** tiene valores duplicados para una única sesión. Consideremos la siguiente consulta:

Select : alias.host, count(ip.src), sum(size)
Group By : alias.host

Aquí, **host-a** y **host-c** están presentes en tres sesiones y son duplicados de dos sesiones distintas. Sin embargo, la salida es la que se muestra a continuación.

Alias.host	count(Ip.src)	Sum(size)
host-a	4	80
host-b	3	60
host-c	4	110
host-d	1	30

La tabla de salida muestra que el conteo de **host-a** y **host-c** es 4. Esto se debe a que, para cada valor de alias.host, se considera la sesión completa. De manera similar, para calcular sum (size), las mismas sesiones se consideran para cada valor de alias.host.

Cuadro de diálogo Permisos de regla

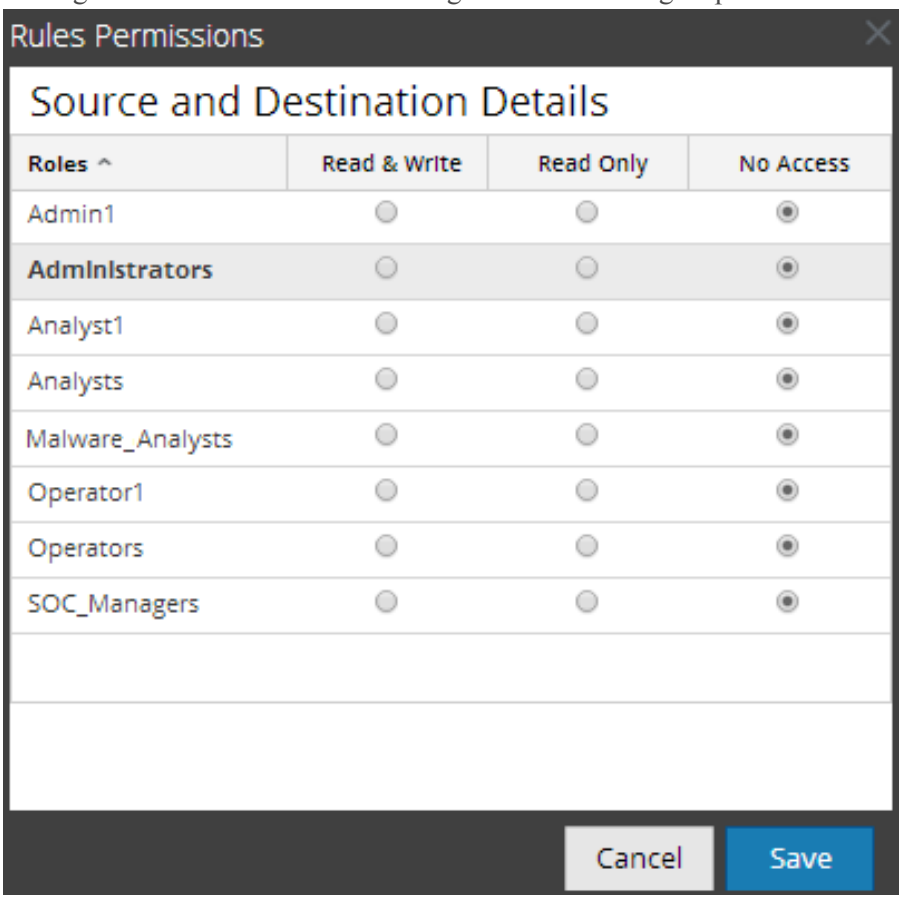
En este tema se describen las funciones del cuadro de diálogo Permisos de reglas. El módulo Reporting proporciona control de acceso en el nivel de regla. Solo un usuario con el conjunto de permisos correcto puede ejecutar las tareas de la regla. Cuando el administrador crea funciones de usuario, debe asegurarse de que las funciones creadas para tareas específicas tengan acceso a todos los permisos más altos en la jerarquía de funciones.

Los procedimientos relacionados con este cuadro de diálogo se describen en Administrar el acceso para una regla o un grupo de reglas

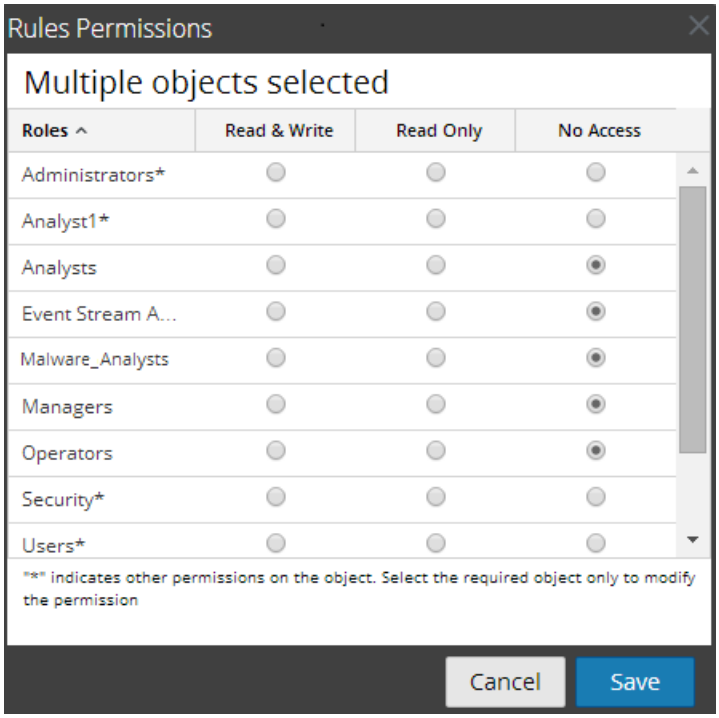
El cuadro de diálogo tiene un aspecto distinto para los grupos de reglas en comparación con las reglas. Para acceder al cuadro de diálogo:

1. En el menú de **Security Analytics**, haga clic en **Administration** > **Informes**.
   Se muestra la pestaña Administrar.
2. En el panel de lista **Reglas**, seleccione una o más reglas o un grupo de reglas.
3. Haga clic en  > **Permisos** en la barra de herramientas.
   Aparece el cuadro de diálogo Permisos de reglas.

Esta figura muestra el cuadro de diálogo Permisos de reglas para una sola regla.



Esta figura muestra el cuadro de diálogo Permisos de reglas cuando se seleccionan múltiples reglas.



Característica	Descripción
Columna Funciones	Enumera las funciones de usuario de Security Analytics, tanto las funciones integradas como las personalizadas. Cada usuario que inicia sesión en Security Analytics tiene funciones de usuario asignadas. Cuando se seleccionan varias reglas, el asterisco junto al nombre de la función, por ejemplo, `Security*`, indica que hay otros permisos disponibles en esa función de usuario. Para cambiar el resto de los permisos, debe seleccionar la función de usuario y cambiar el permiso de acceso.
Columna Lectura y escritura	Cuando se selecciona la casilla de verificación en esta columna, la función de usuario correspondiente tiene permiso para ver, editar, eliminar, importar y exportar reglas en la vista Reglas. El usuario también puede cambiar el permiso en la regla.

Característica	Descripción
Columna Solo lectura	Cuando se selecciona la casilla de verificación en esta columna, la función de usuario correspondiente tiene permiso para ver las reglas del grupo de reglas.
Columna Sin acceso	Cuando se selecciona la casilla de verificación en esta columna, la función de usuario correspondiente no puede ver ni editar las reglas del grupo de reglas. Antes de aplicar permisos de reglas, este es el conjunto de permisos predeterminado para todas las funciones de usuario aunque la casilla de verificación esté deseleccionada.
Casilla de verificación Aplicar estos permisos a subgrupos y reglas de este grupo	Cuando se selecciona, Security Analytics aplica permisos a subgrupos y reglas del grupo.
Opción Cancelar	Cuando se hace clic en Cancelar, se cierra el cuadro de diálogo sin guardar los cambios.
Opción Guardar	Cuando se hace clic en Guardar, se cierra el cuadro de diálogo y se actualizan los permisos de grupo de reglas para las funciones de usuario. Si se especifica, los permisos de acceso se aplican a subgrupos y objetos secundarios de este grupo. Cuando se seleccionan varias reglas, el permiso de acceso se aplica a todas las reglas seleccionadas.

Vista Regla

La vista Regla es la interfaz del usuario para administrar reglas. Los procedimientos asociados se proporcionan en Definir reglas y grupos de reglas, Administrar el acceso para una regla o un grupo de reglas, Crear un gráfico mediante una regla, Crear un informe mediante una reglay Crear una alerta mediante una regla.

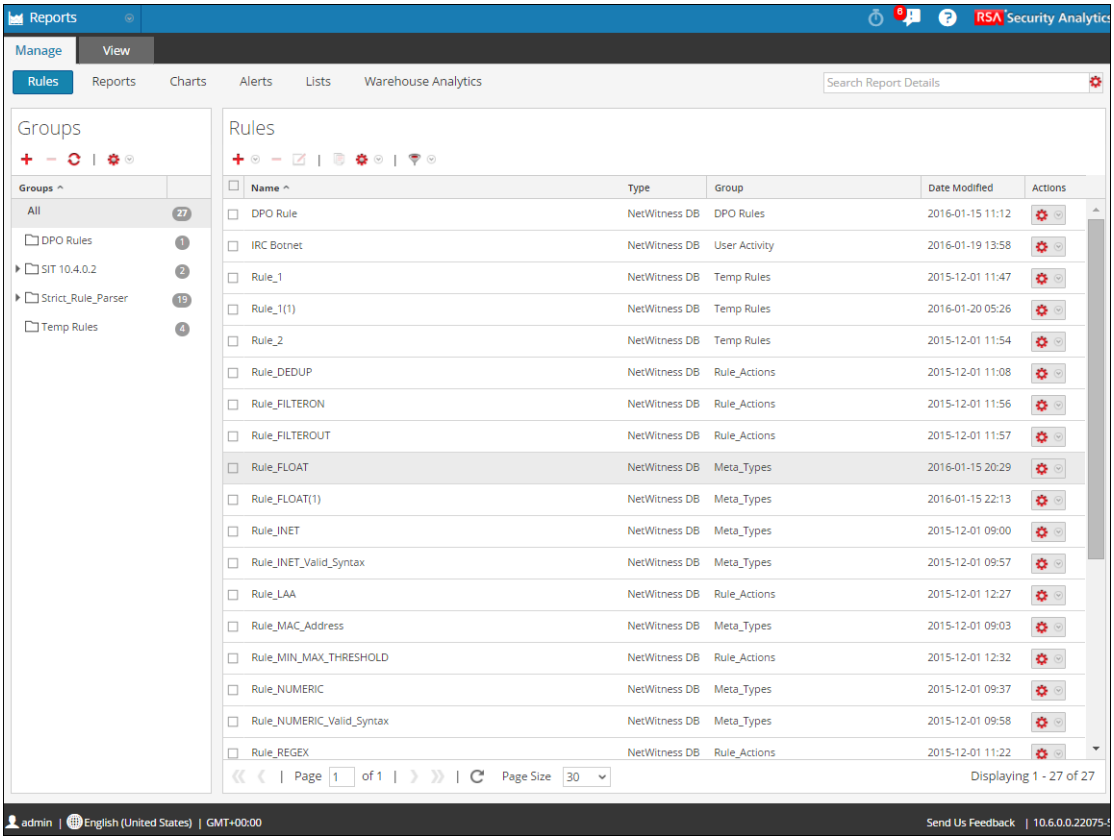
En la vista Regla puede realizar las siguientes acciones:

- Agregar una regla o un grupo de reglas.
- Eliminar reglas y grupos de reglas.
- Establecer permisos de acceso para reglas y grupos de reglas.
- Importar reglas y grupos de reglas.
- Exportar reglas y grupos de reglas.
- Editar una regla.
- Duplicar una regla.
- Crear una alerta.
- Crear un gráfico.
- Crear un informe.
- Ver los dependientes de una regla.
- Actualizar las reglas de un grupo.
- Cambiar el grupo de una regla, para lo cual debe arrastrar y soltar la regla en el nuevo grupo en el panel Grupo de reglas.

Para acceder a la vista Regla:

1. En el menú de Security Analytics, haga clic en **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Rules**.

Se muestra la vista Regla.



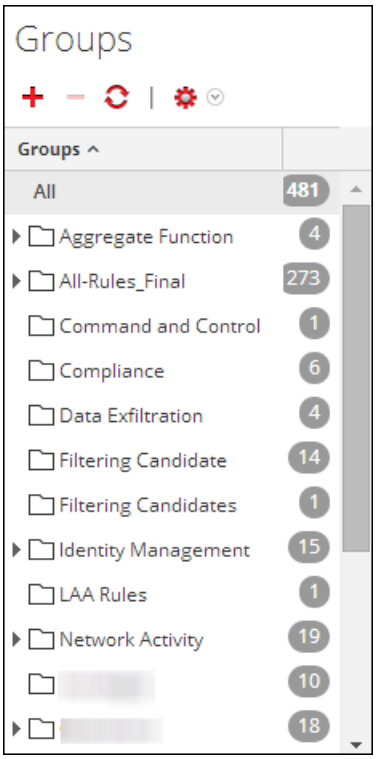
La vista Regla incluye los siguientes paneles:

- Grupos de reglas
- Lista de reglas
- Barra de herramientas Regla

Panel Grupos de reglas

El panel Grupos de reglas permite organizar las reglas en grupos mediante las opciones de la barra de herramientas. Puede crear grupos y subgrupos y agregar reglas en ellos. También puede agrupar y transferir las reglas entre los distintos grupos.

En la siguiente figura se muestran los grupos del panel Grupos de reglas:



En la siguiente tabla se describen las funciones del panel Grupos de reglas.

Característica	Descripción
+	Esta opción le permite agregar un nuevo grupo de reglas al módulo Reporting.
−	Esta opción le permite eliminar uno o más grupos de reglas.
↻	Esta opción actualiza la lista de grupos de reglas.
⚙	El menú Acciones tiene las siguientes opciones: Importar, exportar y permisos.
Todas	Muestra una lista de grupos de reglas.

Barra de herramientas Regla

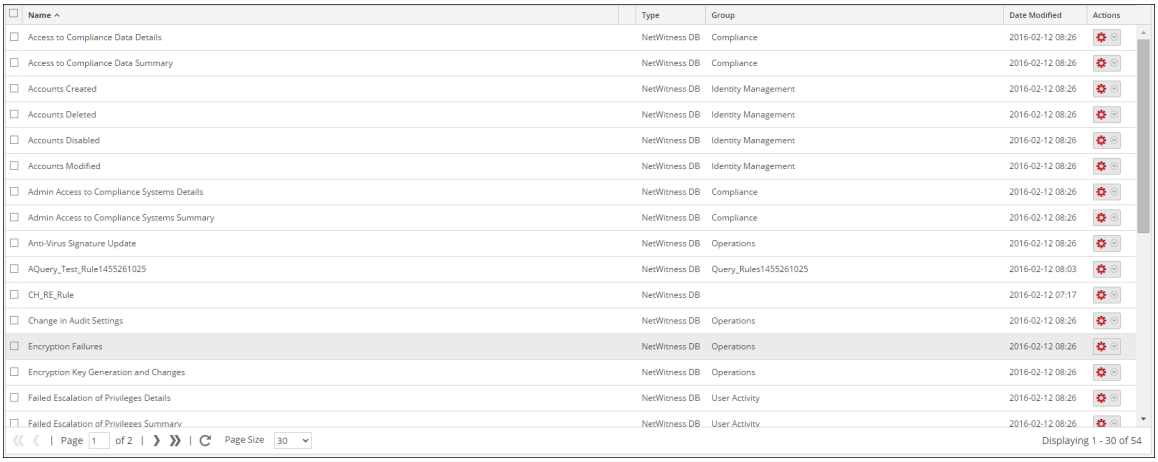
La barra de herramientas Regla permite agregar, eliminar, editar y duplicar una regla. La siguiente figura muestra la barra de herramientas.

En la siguiente tabla se describen las funciones de la barra de herramientas Regla.

Característica	Descripción
	Esta opción le permite agregar una nueva regla al módulo Reporting.
	Esta opción le permite eliminar una o más reglas seleccionadas.
	Esta opción le permite editar una regla.
	Esta opción le permite duplicar una regla.
	El menú Acciones tiene las siguientes opciones: Usar, Importar, Exportar y Permisos.
	Esta opción le permite seleccionar el tipo de regla.

Panel Lista de reglas

En la siguiente figura se muestra la lista de reglas del panel Lista de reglas.



En la siguiente tabla se describen las funciones del panel Lista de reglas.

Característica	Descripción
Nombre	Muestra el nombre de la regla que se creará o editará. **Nota:** En el campo **Nombre**, el ícono para expandir el tamaño de la columna no se muestra al final del campo de la columna. Debe mover el mouse un poco hacia la izquierda para ver el ícono que permite ampliar la columna.

Característica	Descripción
Tipo	Muestra el tipo de base de datos compatible para la regla que creó.
Grupo	Muestra los valores que se agrupan.
Fecha de modificación	Muestra la fecha en que se modificó la regla por última vez.
Acciones	Muestra el menú Acciones con las siguientes opciones: Crear alerta, crear gráfico, crear informe, eliminar, editar, exportar y dependientes.

Especificación de orígenes de eventos de IPDB

En este tema se describen los orígenes de eventos de IPDB que puede especificar. Puede especificar orígenes de eventos de IPDB mediante comodines o si especifica la dirección completa del origen de eventos. En la siguiente tabla se indican las especificaciones de los orígenes de eventos de IPDB compatibles.

Origen de eventos	Descripción
::*:*:*	Todos los dominios, sitios, nodos, tipos de dispositivo (tipos de orígenes de eventos) y direcciones IP de origen de eventos. Security Analytics es compatible con un único comodín de sitio para dominio y sitio.
domain:site:*:*:*	Todos los nodos, los tipos de dispositivos y las direcciones IP de origen de eventos del sitio especificado.
domain:site:node:*:*	Todos los tipos de dispositivos y las direcciones IP de origen de eventos del nodo especificado.

Origen de eventos	Descripción
domain:site:node:devicetype:*	Todas las direcciones IP de origen de eventos del dominio, el sitio, el nodo y el tipo de dispositivo especificados.
domain:site:node:devicetype:event-source-address1,domain:site:node:devicetype:event-source-address2,...-domain:site:node:devicetype:event-source-addressN.	Lista de orígenes de eventos separada por comas.

Modos de definición de reglas de la base de datos de Warehouse

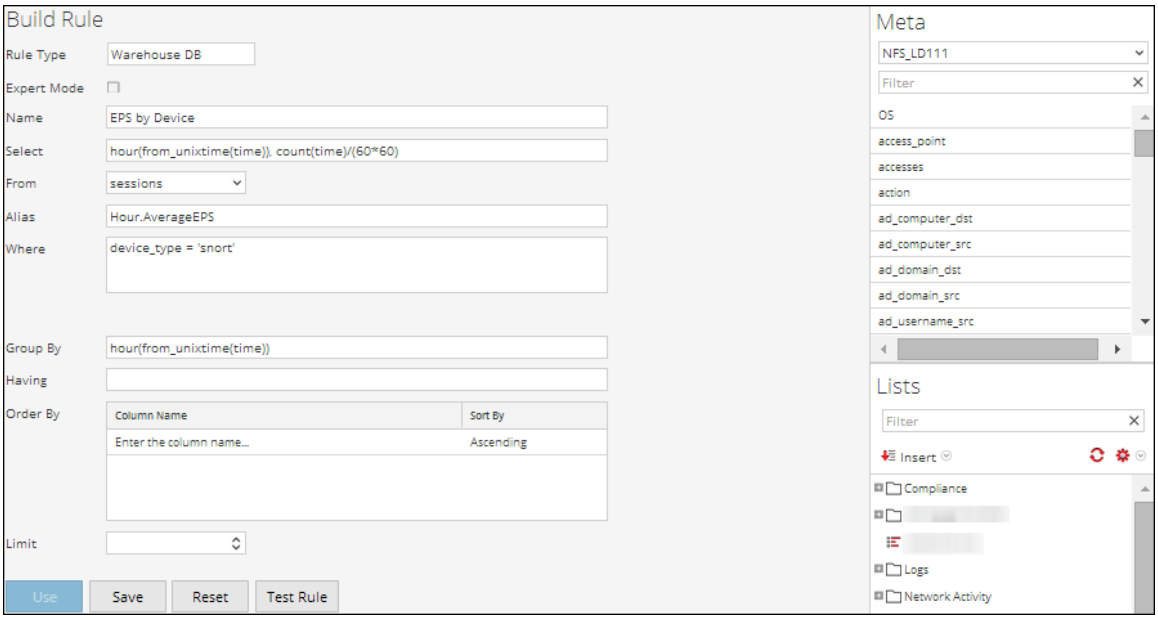
En este tema, se describen los modos de definición de reglas de la base de datos de Warehouse. Puede generar informes del origen de datos de Warehouse, para lo cual debe crear reglas para consultar el origen de datos. Las reglas se pueden definir de dos modos:

- Modo Predeterminado
- Modo experto

Modo Predeterminado

En el modo predeterminado, puede crear reglas que contengan SQL sencillos como consultas de HIVE que contengan cláusulas como Select, Where, Group By y Having. De manera predeterminada, puede crear reglas para realizar consultas a las sesiones o registros crudos. Para obtener más información acerca de la sintaxis de consulta simple y ejemplos, consulte Informe Todas las categorías de eventos.

La siguiente figura es un ejemplo de la **vista Crear regla** que se muestra cuando selecciona **Base de datos de Warehouse** para **Tipo de regla** sin el modo experto seleccionado.

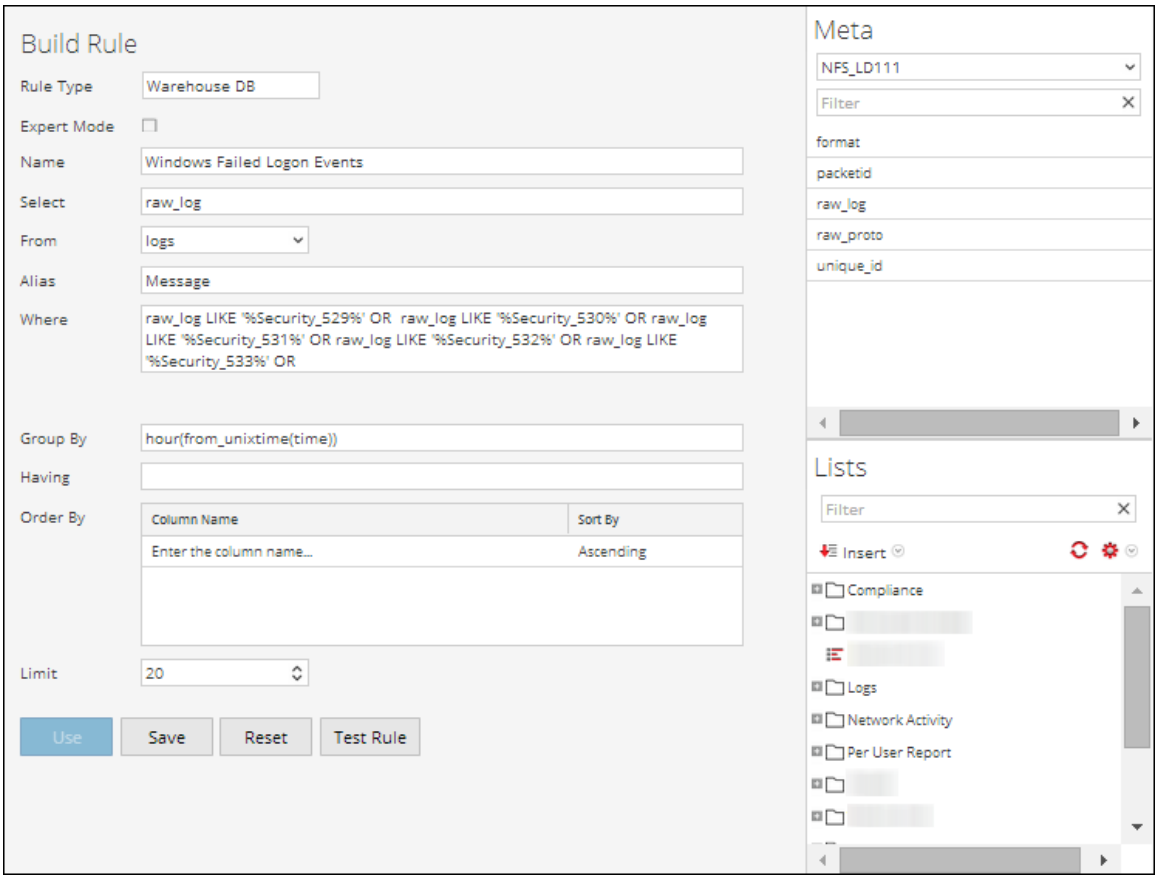


Realizar consultas a los registros crudos

Se usa el formato de registro crudo en la cláusula Select o Where para consultar por registros crudos.

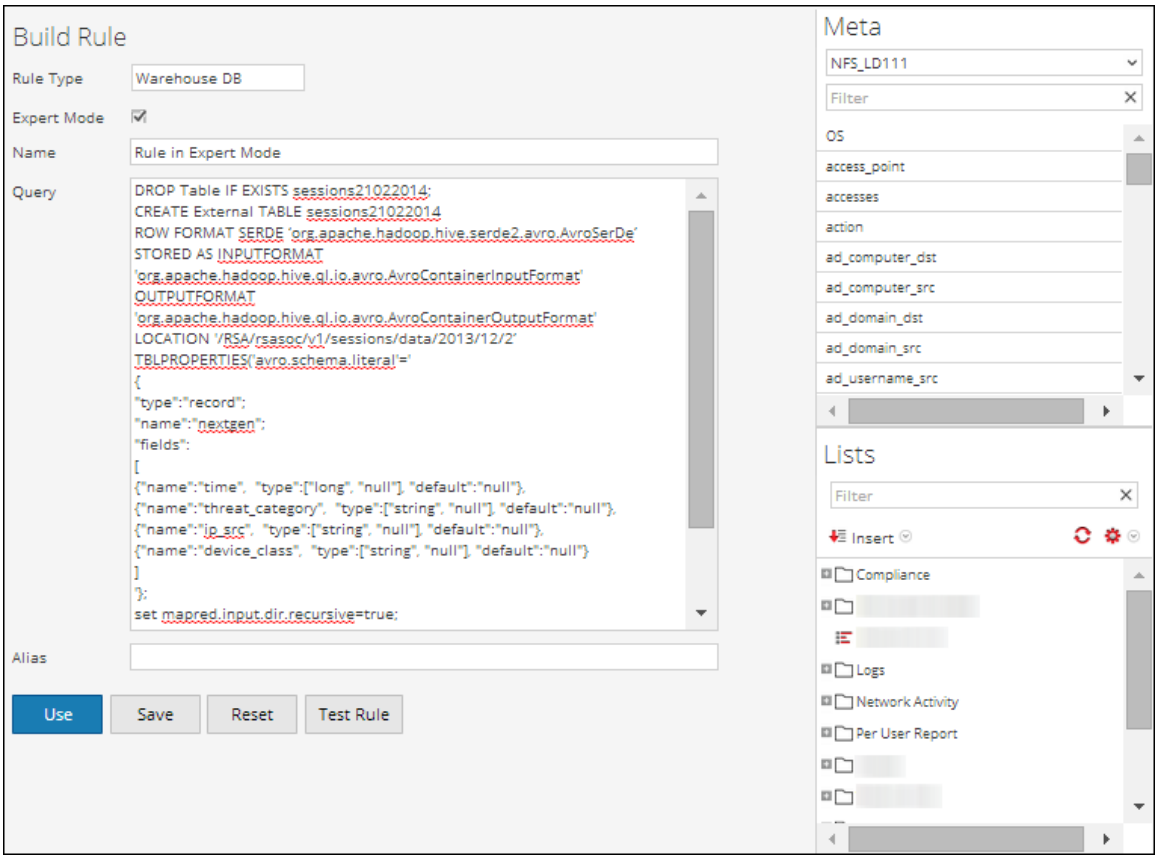
Nota: El rango de tiempo que puede especificar en la consulta es un día (24 horas). Si especificó un rango de tiempo inferior a un día en la consulta, el conjunto de resultados tendrá datos de al menos un día (24 horas).

La siguiente figura es un ejemplo de la **vista Crear regla** que se muestra cuando selecciona **Base de datos de Warehouse** para **Tipo de regla** y crea una regla para realizar consultas a los registros crudos:



Modo experto

La siguiente figura es un ejemplo de la **vista Crear regla** que se muestra cuando selecciona **Base de datos de Warehouse** para **Tipo de regla** con el modo experto seleccionado.



Si desea generar un informe con un rango de tiempo específico, debe definir manualmente el rango de tiempo en la consulta utilizando las siguientes dos variables:

- ${report_starttime}: la hora de inicio del rango en segundos.
- ${report_endtime}: la hora de finalización del rango en segundos.

Por ejemplo, **SELECT col1, col2 FROM custom_table WHERE timecol >= ${report_starttime} AND timecol <= ${report_endtime};**

Nota: De forma predeterminada, Reporting Engine considera `${keyword}` como una variable. Si desea especificar las variables HIVE, debe mencionar la sintaxis completa de una variable. Por ejemplo, `${hiveconf:hive.exec.scratchdir}`.

Temas

- Sintaxis general de una regla avanzada
- Informe Todas las categorías de eventos