Geek2Net

IMPORTANTE

Caso Implementación Colombia Compra Eficiente

Netskope: **2**
- Licencias de SWG. 2
- Configuración inicial del tenant. 3
  - Crear administrador delegado 3
  - Crear roles para administradores restringidos 4
- Netskope Client 5
- Configuración de políticas. 5
- Configuración de políticas base de DLP. 8
- Licencia de NPA (Acceso remoto) 11
- VPN 12

Nemasis **14**
- Características del Servidor: 14
- Instalación de Nemesis 14
- Configuraciòn módulo de escaneo. 27
  - Task. 27
  - Basic: 29
  - Targets and Alerts 30
  - Scan Target: 31

IMPORTANTE

Historial de Modificaciones			
Fecha	**Versión**	**Creado por**	**Descripción de la modificación**
15-12-22	1	Carlos Triana	Creación del documento
15-12-22	1.1	Winston Gaviria	Ajustes menores.

IMPORTANTE

Introducción:

El presente documento tiene como finalidad mostrar evidencias y descripción de las actividades que se realizaron durante la implementación del proyecto.
Se implementó por un lado la herramienta Netskope que pretende ampliar la cobertura de seguridad que tiene la entidad a través del control de acceso remoto de cero confianza, para todos los usuarios que estén fuera de la organización y necesiten consumir servicios internos, de tal manera que se pueda garantizar la seguridad de las conexiones y mitigar las amenazas relacionadas con ataques a través de VPNs, identidad de los usuarios, entre otros.
Netskope también tiene módulos de protección para el control de la navegación a través de aplicaciones, permite evidenciar que aplicaciones son sancionadas y cuáles no, y tomar decisiones corporativas sobre el uso versus el riesgo que pueden representar las mismas para la información de la entidad. Se complementa con características de DLP que permiten controlar la información que los usuarios pueden enviar fuera de la organización hacia páginas de terceros, personales, o que simplemente no tengan relación con la entidad.
Por otro lado, Nemasis es una herramienta orientada al análisis de vulnerabilidades sin límites de activos, de tal manera que hace un match perfecto con los procesos internos de gestión de vulnerabilidades que podrán ser ejecutados sin limitaciones durante la vigencia de la licencia.

Netskope:

Licencias de SWG.

Next Gen SWG: provee capacidades para prevenir malware, detectar amenazas avanzadas, filtrar sitios web por categoría, proteger datos, controlar aplicación y servicios en la nube para cualquier usuario, ubicación o dispositivo. Proxy en línea de un solo paso incomparable por su capacidad para decodificar el tráfico web y en la nube incluida la instancia y actividad.

Características:

- Tráfico web y visibilidad de aplicaciones, incluidos datos, actividad y contexto
- Rendimiento de la nube para inspeccionar con la escala de la nube para cualquier usuario, dispositivo o ubicación

IMPORTANTE

- Prevención de pérdida de datos para aplicaciones administradas y no administradas y tráfico web
- Acceso a la red de confianza cero para el acceso remoto a aplicaciones privadas tanto en la nube pública como en los centros de datos
- Malware y defensas contra amenazas avanzadas, sandboxing y más de 40 fuentes de inteligencia contra amenazas
- Consola única y controles de políticas unificados

Principales casos de uso

- Monitoreo y visibilidad

    - Observar el comportamiento de los usuarios en Internet
    - CASB monitorear aplicaciones y actividades de SaaS
    - Nivel de riesgo para aplicaciones SaaS

- Malware y detección avanzada de amenazas

    - Analice el tráfico de Internet bidireccionalmente
    - Análisis de la UEBA de la actividad de la cuenta en la nube en busca de
    - AV comprometidos o internos, IPS/exploits, análisis de secuencias de comandos, heurística previa a la ejecución, sandboxing en la nube

- Conectar oficinas y trabajadores móviles

    - La rápida adopción de aplicaciones SaaS está impulsando las oficinas remotas directamente a Internet
    - La pila de seguridad basada en la nube protege a los trabajadores remotos y móviles

Configuración inicial del tenant.

Crear administrador delegado

1. Vaya a Configuración > Administración > Administradores .

IMPORTANTE

2. Haga clic en Nuevo administrador .
3. Ingrese una dirección de correo electrónico (nombre de usuario) y, para la contraseña, elija generar una contraseña automáticamente o crear una. Si crea una contraseña, tenga en cuenta los requisitos de contraseña:
    - 8+ caracteres
    - Una combinación de mayúsculas y minúsculas, números y símbolos

4. Seleccione el botón de radio para saber cómo proporcionar la contraseña para el nuevo administrador. Anote el nombre de usuario y la contraseña si opta por proporcionar la contraseña manualmente. Tenga en cuenta las restricciones de contraseña para el usuario administrador. Si utiliza la selección predeterminada para generar una nueva contraseña, se le pedirá al administrador que cambie la contraseña al iniciar sesión por primera vez. Puede eliminar el usuario administrador en cualquier momento.

    Seleccione el rol para asignar al nuevo administrador. Sus opciones incluyen:

    - Administrador de inquilinos: administrador de nivel superior que tiene todos los privilegios.
    - Administrador delegado: todos los privilegios, excepto la gestión de otros administradores.
    - Administrador restringido: tiene acceso de solo lectura a todas las funciones.
    - Analista de inteligencia en la nube: sólo tiene acceso a informes y análisis.
    - Analista de riesgos de aplicaciones: puede ejecutar informes y análisis y leer el CCI.
    - Administrador de aplicaciones empresariales: puede administrar la aplicación CCI.
    - Administrador de directorio: puede administrar usuarios.
    - Administrador de seguridad: puede administrar la configuración.
    - Administrador de operaciones de InfoSec: puede administrar políticas.
    - Oficial de Cumplimiento: Puede remediar incidentes de DLP.
    - Analista de seguridad: puede analizar malware y amenazas.

5. Haga clic en Crear para notificar al nuevo administrador.

Crear roles para administradores restringidos

IMPORTANTE

1. Vaya a Configuración > Administración > Funciones .
2. Haga clic en Crear nuevo .
3. Se debe proporcionar un nombre de función y una descripción si lo desea. El tipo de función se establece en Solo lectura de forma predeterminada
4. Especifique la lista de usuarios y/o grupos a los que tendrá acceso el administrador.
5. Permitir el acceso al contenido del archivo, esto permite a los administradores descargar, obtener una vista previa y ver archivos desde Protección y análisis forense habilitados para API.
6. Opcionalmente, puede elegir la opción de ofuscar
7. Se debe seleccionar el ámbito , Todos los eventos o seleccione eventos específicos.
8. Se da click en Crear.

Más información

Netskope Client

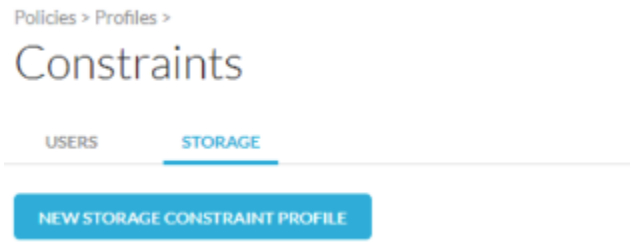
Se puede implementar como:

- Aplicación instalable: en los dispositivos que ejecutan los sistemas operativos Windows, macOS y Android, el Cliente se instala como una aplicación liviana y no intrusiva que dirige el tráfico desde el dispositivo del usuario a la nube de Netskope. Puede descargar el cliente desde la página Descargar scripts y clientes de Netskope.
- Perfil de configuración : en los dispositivos que ejecutan el sistema operativo iOS, el cliente se implementa como un perfil de configuración de VPN bajo demanda o por aplicación.

Configuración de políticas.

1. Navegue a Policies > Contrain.
2. Seleccione la pestaña Storage.

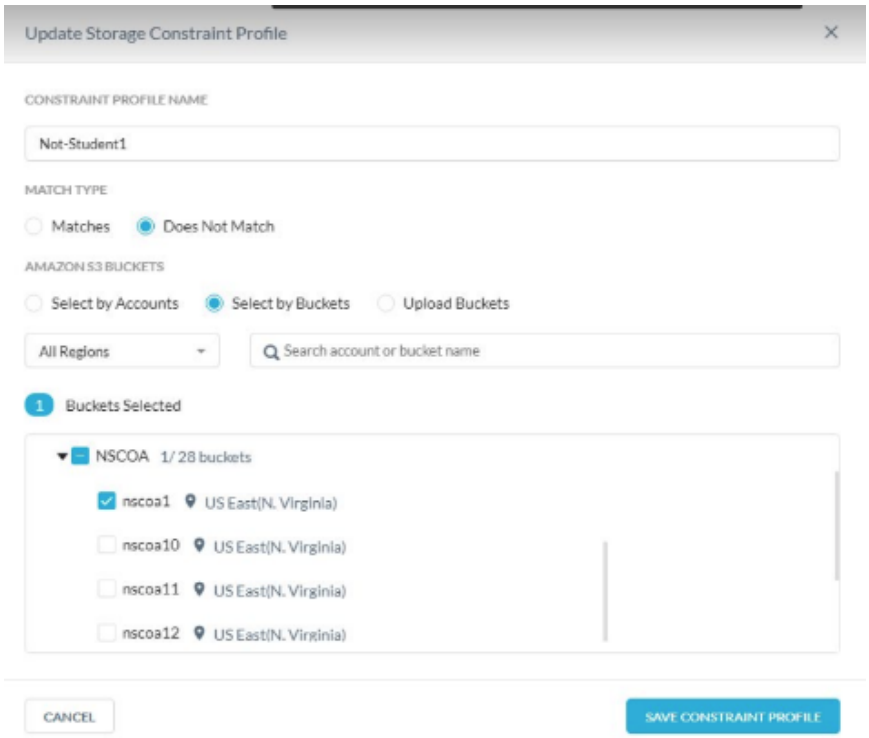
IMPORTANTE



3. Cree un nuevo perfil de restricción de almacenamiento.
4. Nombre el perfil (NOMBRE).
5. Seleccione el botón de opción **Does Not Match**.
6. Desde Amazon S3 Buckets, haga clic en **Select by Buckets**.
7. Seleccione la cuenta o todas las cuentas según corresponda.

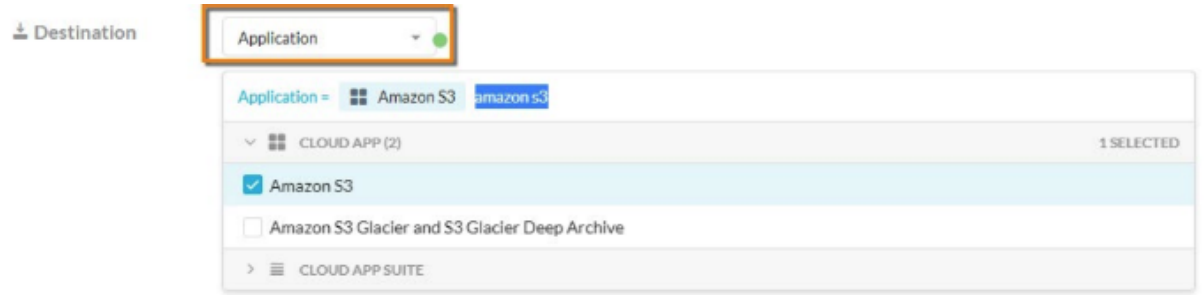
Ejemplo:

IMPORTANTE



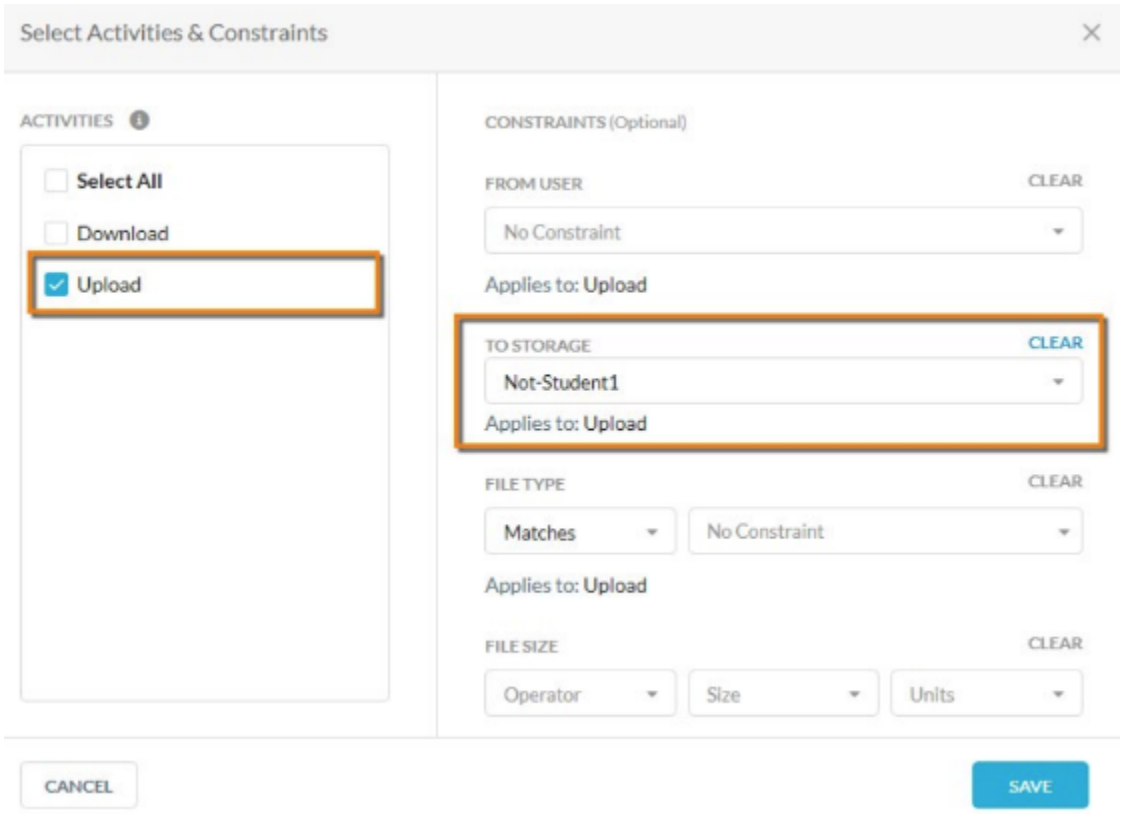
Haga clic en Guardar perfil de restricción para guardar los cambios. Luego, haga clic en Aplicar cambios. Una confirmación se mostrará el mensaje. Haga clic en Aplicar para confirmar.

9. Navegue a Policies > Real-time Protection.
10. Haga clic en New Policy > Cloud App Access.
11. En la sección Fuente, seleccione (el usuario) de la lista de Usuarios.
12. En la sección Destino, seleccione Aplicación y luego busque Amazon S3.
13. Seleccione Amazon S3.



IMPORTANTE

En la sección de Activities & Constraints hace click editar. Luego, Seleccionar Upload y en el campo de Storage elegir el usuario.



15. Click Save.
16. En la sección the Profile & Action, seleccionar the Block action and select the Block S3 template.
17. En la sección de políticas, agregar el nombre de la política.
18. Click Save. En la ventana mover política, conserve la selección predeterminada de Hacia arriba y haga clic en Guardar nuevamente. Luego, haga clic en Aplicar cambios y haga clic en Aplicar para confirmar.

IMPORTANTE

Configuración de políticas base de DLP.

Netskope Data Loss Prevention (DLP) protege los datos confidenciales en la nube con exactitud y precisión mediante la inspección de todos los servicios en la nube autorizados y no autorizados. Cuando los usuarios violan una política de DLP, Netskope registra el incidente. Si tiene Endpoint DLP , los usuarios que violan sus políticas de control de contenido también desencadenan un incidente de DLP.

Visualización de incidentes de DLP
Para ver los incidentes de DLP en su organización, vaya a Incidentes > DLP .

En la página de DLP, puede:

1. Actualice los resultados del incidente de DLP.

2. Filtre los incidentes de DLP por un marco de tiempo específico. Puede usar un marco de tiempo predefinido o elegir Rango de fechas para usar los menús de calendario y tiempo para personalizar el suyo propio.

3. Busque y filtre los incidentes de DLP por una consulta. Haga clic en + Agregar filtro para agregar otros filtros para restringir los resultados de su búsqueda. Por ejemplo, puede elegir Bloquear para la última acción y seleccionar una aplicación para ver solo los incidentes de DLP que coincidan con este criterio. También puede hacer clicEl icono del modo de consulta de Netskope.para cambiar al modo de búsqueda de consulta avanzada. Hacer clicEl icono Guardar filtro.para guardar la combinación de filtros para futuras búsquedas.

   Nota: Si tiene Endpoint DLP , puede filtrar incidentes por Política de control de contenido de Endpoint .

4. Vea las 5 aplicaciones principales, las exposiciones y las 5 políticas principales con infracciones.

5. Ver una lista de incidentes de DLP. Para cada incidente, puede ver la siguiente información predeterminada:

IMPORTANTE

- Objeto : el nombre del archivo o del objeto que desencadenó la infracción. Haga clic para abrir una página con más detalles donde puede cambiar el estado, asignar incidentes, cambiar la gravedad y tomar medidas.
- Aplicación : la aplicación que desencadenó la infracción.
- Sitio : el sitio web que desencadenó la infracción.
- Exposición : el nivel de exposición del archivo.
    - Público - Indexado
    - Público - No listado
    - Público
    - Privado
    - Compartido externamente
    - Compartido internamente
    - Empresa compartida
    - Geográfico cruzado
- # Violations : El número total de violaciones con archivo. El conteo se refiere al número agregado de registros detectados en todas las políticas del incidente.
- Última acción : la acción que se realizó, como permitir, bloquear, alertar, etc.
- Estado : Muestra el estado del evento. Hay tres estados:
    - Nuevo
    - En progreso
    - Resuelto
- Asignatario : La persona asignada para monitorear el incidente.
- Gravedad : el nivel de gravedad del objeto o archivo. Hay cuatro niveles:
    - Bajo
    - Medio
    - Alto
    - Crítico

      Además, si seleccionó Contar solo registros únicos en Umbral de gravedad para una regla de DLP , la gravedad muestra el recuento como Recuento: <Número de infracciones> único . Si anula la selección de Contar solo registros únicos , el conteo de gravedad se muestra como Contar: <Número de infracciones> .

- Id. de objeto : el Id. del objeto o archivo.

IMPORTANTE

- Marca de tiempo : la fecha y la hora en que ocurrió la infracción.
- Instancia : la instancia de la aplicación que desencadenó la infracción.
- ID de instancia : el ID de la instancia de la aplicación.
- Última modificación por : el usuario que realizó los últimos cambios en el archivo cuando Netskope lo procesó.
- Propietario del objeto : el propietario original del objeto o archivo.
- Ruta del archivo : la ruta completa del archivo en el dispositivo.
- Política de DLP : la política de DLP que desencadenó la infracción.
- Perfil de DLP : el perfil de DLP asociado con la política y la infracción de DLP.
- Regla de DLP : las reglas de DLP asociadas con la política y la infracción de DLP.

6. Seleccione uno o más objetos para actualizar Marcar estado como y Gravedad , así como Asignar a alguien para monitorear el incidente.

7. Ordena la tabla de la siguiente manera:
   - Objeto
   - Solicitud
   - Sitio
   - Exposición
   - Estado
   - Cesionario
   - Gravedad
   - Instancia
   - Última modificación por
   - Propietario del objeto
   - Marca de tiempo

8. Seleccione uno o más objetos para actualizar el estado. También puedes:
   - Crear estado personalizado : cree un nombre para un estado personalizado.
   - Administrar estados personalizados : vea, edite o elimine cualquier estado personalizado.

9. Seleccione uno o más objetos para editar el nivel de gravedad.

IMPORTANTE

10. Seleccione uno o más objetos para elegir una dirección de correo electrónico de un administrador para monitorear el incidente.

11. Exporte todos los incidentes de DLP (hasta 500 000 filas) a un archivo CSV como resumen o incluyendo todos los detalles.

12. Hacer clic en el ícono de Configuración. Para personalizar las columnas de la tabla o restaurar las predeterminadas.

13. Vea hasta 100 incidentes de DLP por página.

14. Ver varias páginas de la tabla.

Más información

Licencia de NPA (Acceso remoto)

Netskope Private Access (NPA) conecta a los usuarios en cualquier lugar con los recursos privados alojados en las instalaciones o en la nube, lo que garantiza la conectividad rápida y directa de las aplicaciones y una experiencia superior para los usuarios.

Con la arquitectura de acceso privado, los recursos privados permanecen ocultos y protegidos de descubrimientos y ataques. Los usuarios autentificados obtienen un acceso directo y seguro a las aplicaciones autorizadas con un cifrado de tráfico de extremo a extremo.

Maneja Trust Network Access (ZTNA), un enfoque más nuevo, cierra el abismo aparente sin crear compensaciones. ZTNA también fomenta la colaboración entre los equipos de infraestructura de TI, redes y seguridad, un paso que impulsa aún más la transformación digital con el objetivo de mejorar la agilidad empresarial, la resiliencia, la productividad y la
en última instancia, mejorar la competitividad de una empresa.

Los productos ZTNA son pilares importantes de una arquitectura de borde de servicio de acceso seguro (SASE), para que se espera que más del 60% de las empresas cuenten con un plan en los próximos años. Pero implementar ZTNA puede ser una tarea importante. Los equipos de TI que todavía están lidiando con la pandemia pueden resistir tal cambio transformacional, temiendo el resultado o lo que podría significar para su seguridad laboral.

IMPORTANTE

Para los tomadores de decisiones, las elecciones correctas en tres áreas pueden ayudar a superar la resistencia potencial y generar aceptación en toda la empresa:

- Otorgue a cada parte interesada un asiento en la mesa y asegúrese de que se satisfagan las necesidades de TI, de seguridad y del negocio.
- Comience con un solo caso de uso o concéntrese en un grupo de usuarios.
- Elija el producto ZTNA correcto.

Las buenas decisiones en estas áreas permitirán toda la iniciativa y, por lo tanto, la transformación más grande turnos que involucren SASE—para proceder mucho más suavemente

VPN

Las aplicaciones VPN de terceros requieren excepciones de configuración de dirección para garantizar que la aplicación VPN respectiva pueda llegar a su puerta de enlace. Para obtener más información sobre cómo crear excepciones de VPN, consulte Configuración de excepciones para aplicaciones de VPN .

Configuración de excepciones para aplicaciones VPN

Los clientes de Netskope instalados en dispositivos (mac y Windows) que ejecutan aplicaciones VPN en modo de túnel completo pueden experimentar conflictos con aplicaciones VPN de terceros. Esto suele suceder cuando cualquiera de las aplicaciones intenta interceptar el tráfico destinado a sus respectivos destinos.

Este artículo enumera las excepciones que se deben agregar a las configuraciones de dirección para evitar todo el tráfico de VPN a la puerta de enlace de VPN respectiva. Los cambios de configuración incluyen lo siguiente:

- Creación de una política de ubicación de red
- Adición de excepciones de ubicación de destino a la configuración de dirección

IMPORTANTE

Administración:

ENABLED	ADMIN	TYPE	ROLE	LAST LOGIN
	carlos.triana@geek2net.com	Local Account	Tenant Admin	-
	david.marin@geek2net.com	Local Account	Tenant Admin	-
	hriveros@netskope.com	Local Account	Tenant Admin	-
	htamayo@netskope.com	Local Account	Tenant Admin	December 10 2022 07:25 AM
	natalia.romero@geek2net.com	Local Account	Tenant Admin	December 16 2022 02:23 PM
	pov-automation@netskope.com	Local Account	Tenant Admin	December 10 2022 01:20 AM
	wilson.coronado@colombiacompra....	Local Account	Tenant Admin	December 14 2022 03:59 PM
	winston.gaviria@geek2net.com	Local Account	Tenant Admin	December 16 2022 04:19 PM

Reenvío de tráfico:

NPA	Last edited Dec 16, 2022 by winston.gaviria@geek2net.com	Navegacion Netskope Cloud Apps Only, All Private Apps	...
Default tenant config	Last edited Dec 15, 2022 by winston.gaviria@geek2net.com	All Users All Web Traffic	...

IMPORTANTE

Publishers:

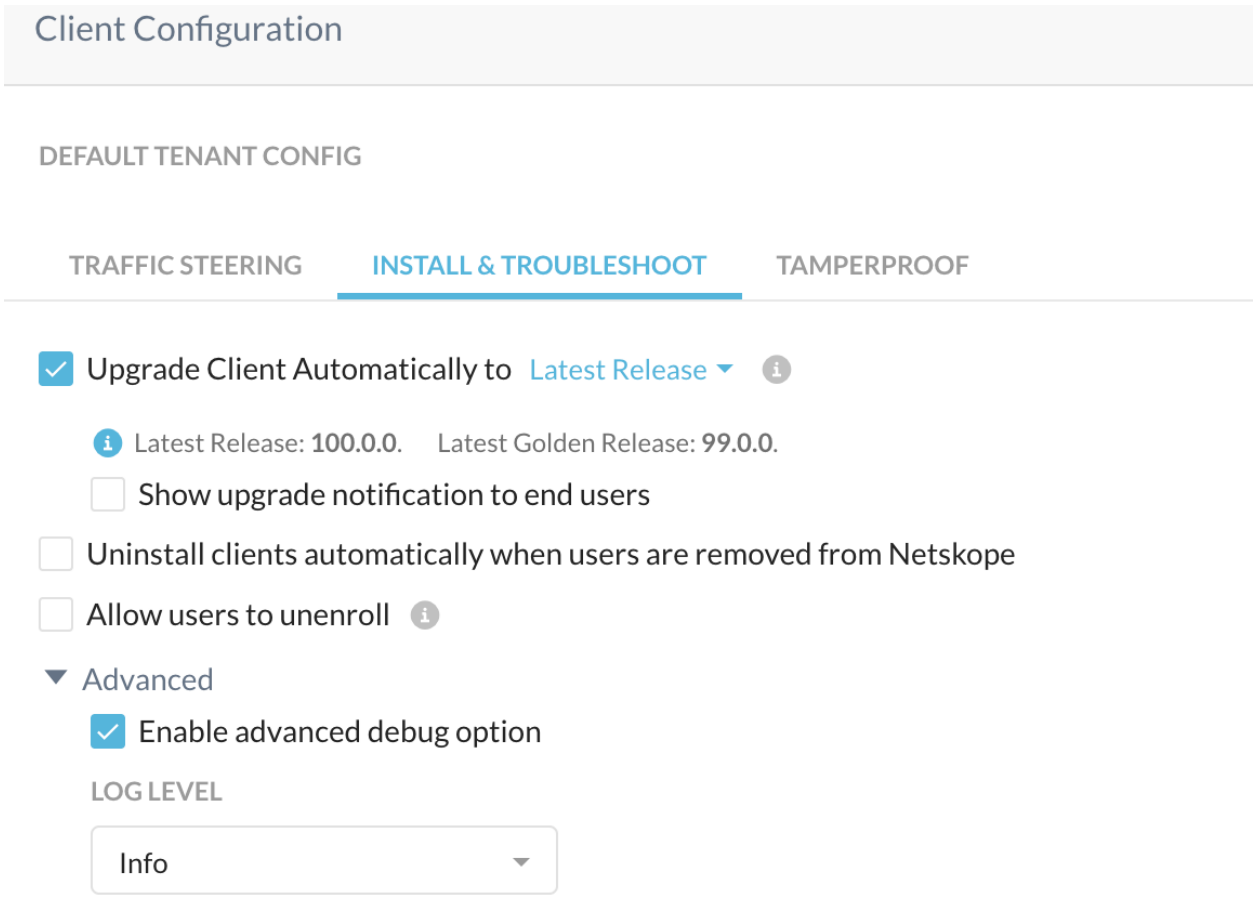
Publishers
3 CREATED

Sort by: Select

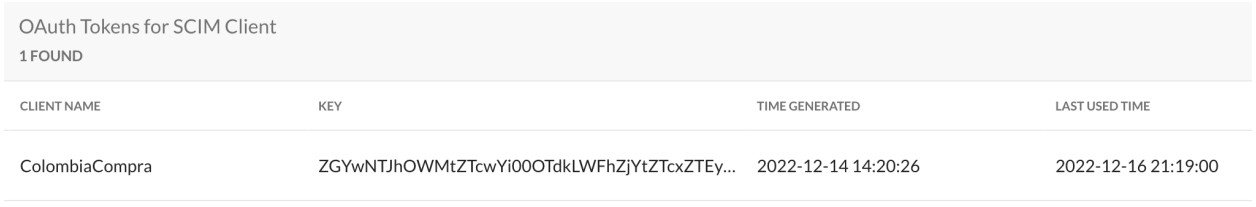
PUBLISHER	STATUS	VERSION	UPDATE PROFILE
CCE-AZURE	Connected	99.0.0.7505	default
CCE-Datacenter	Connected	99.0.0.7505	default
CCE-ORACLE	Connected	99.0.0.7505	default

IMPORTANTE

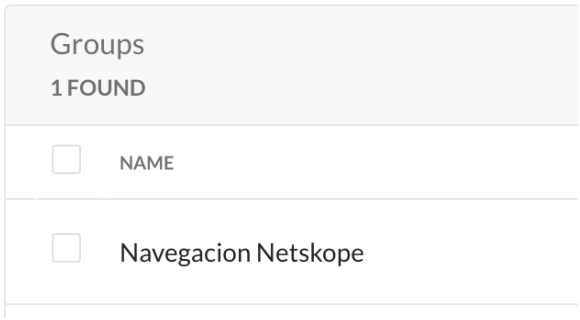
Configuración global de agentes:



Integración con Azure:



IMPORTANTE



Nemasis

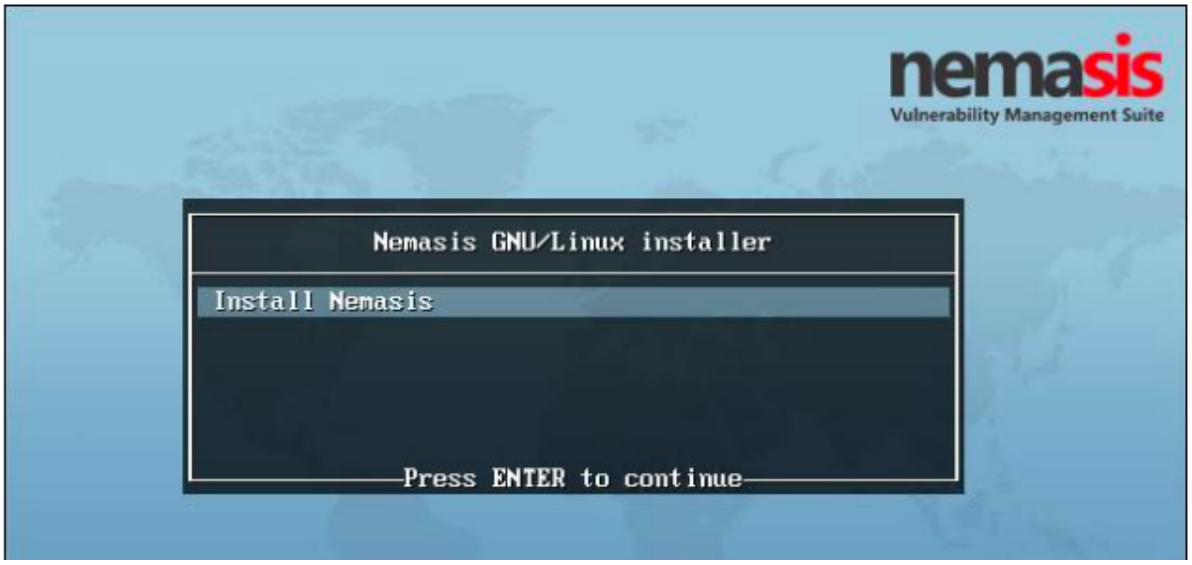
Características del Servidor:

Se puede implementar en ambientes virtuales como vmware, virtualbox o Microsoft Hyper-V. Las características del servidor son de tener 4 cpu, 16GB de RAM y 100 GB de disco HDD

Instalación de Nemesis

Para iniciar el proceso de instalación se debe tener una imagen .iso la cual se debe ejecutar para empezar la instalación de Nemesis.

IMPORTANTE



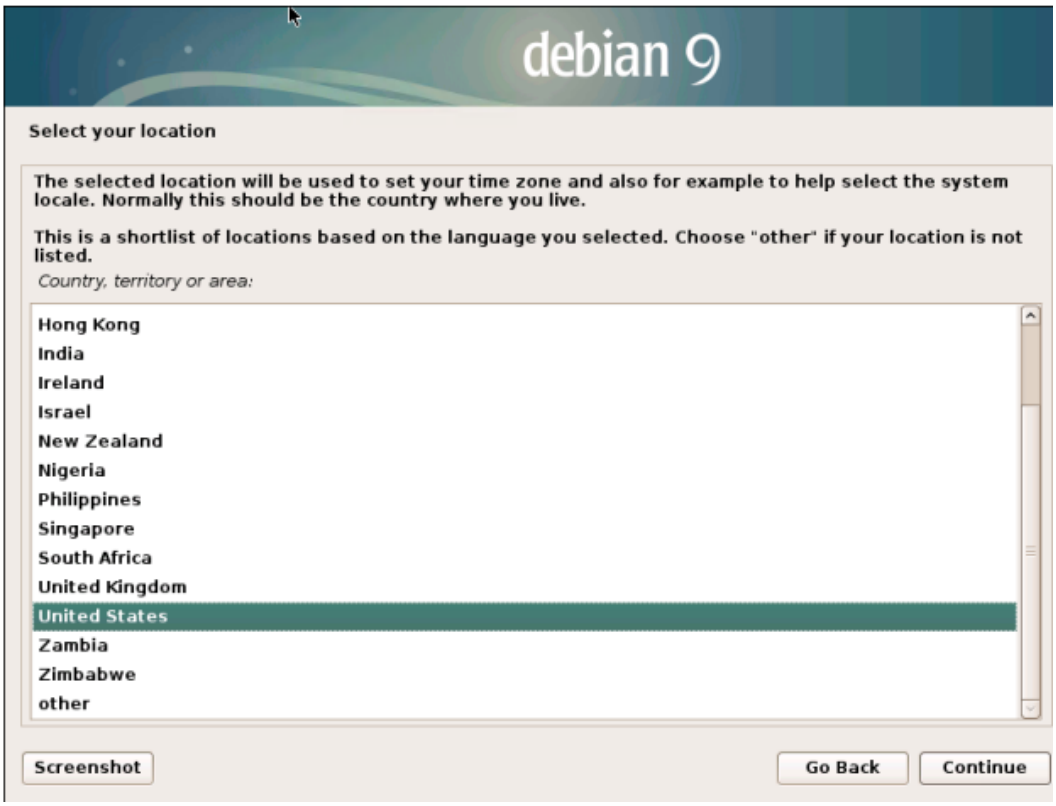
Seleccionar el idioma de instalaciòn

IMPORTANTE



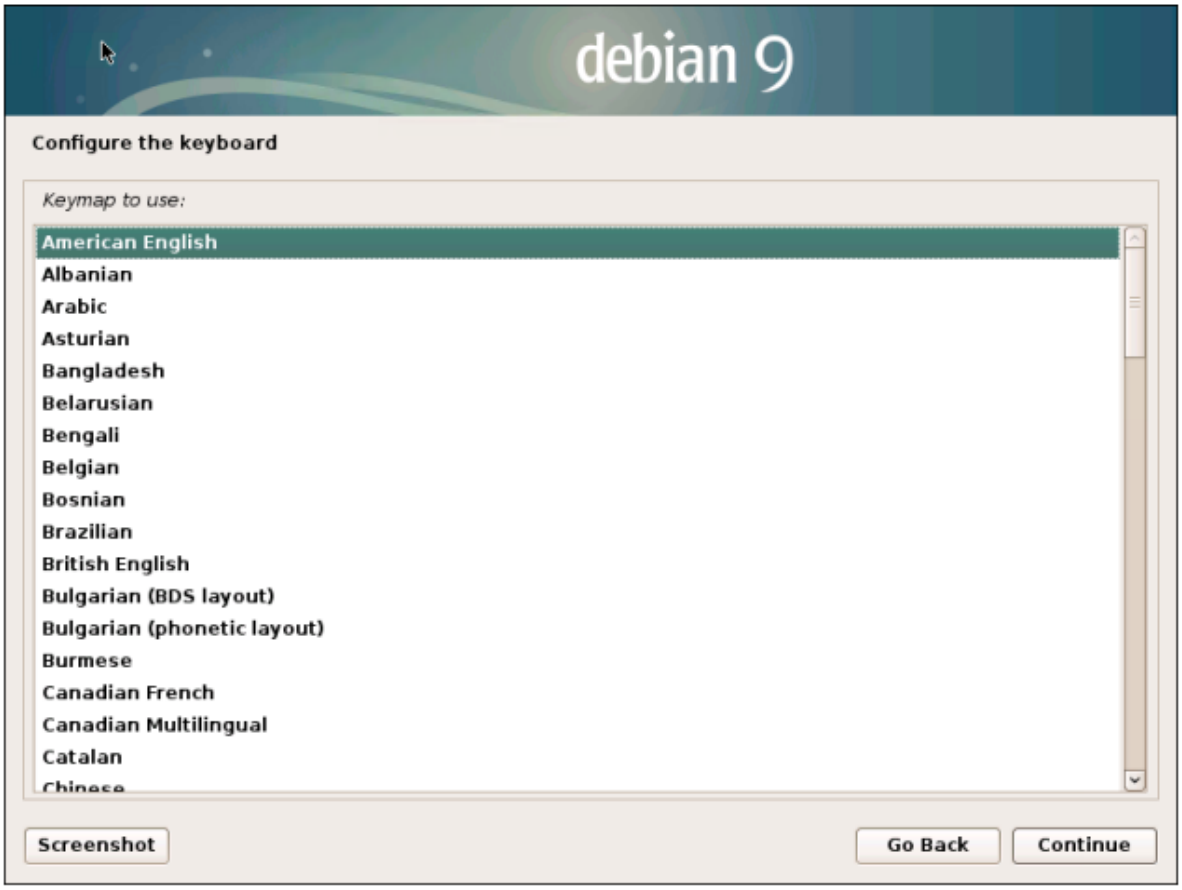
Seleccionar el país de ubicación

IMPORTANTE



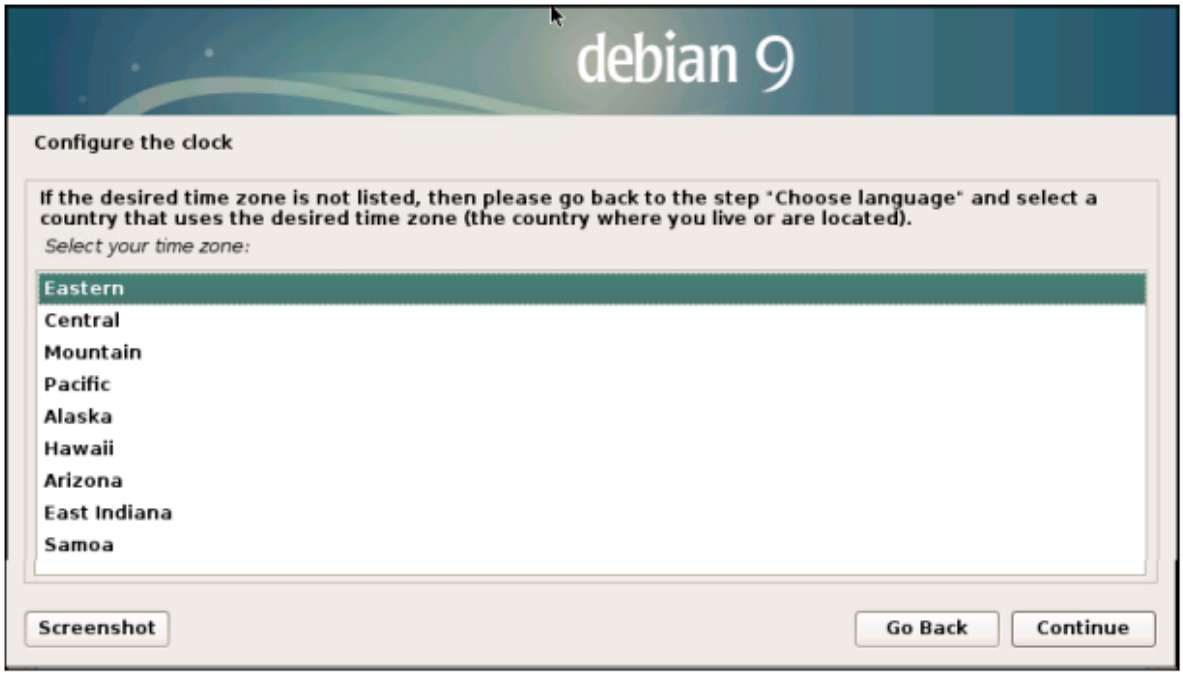
Seleccionar la configuración del teclado

IMPORTANTE



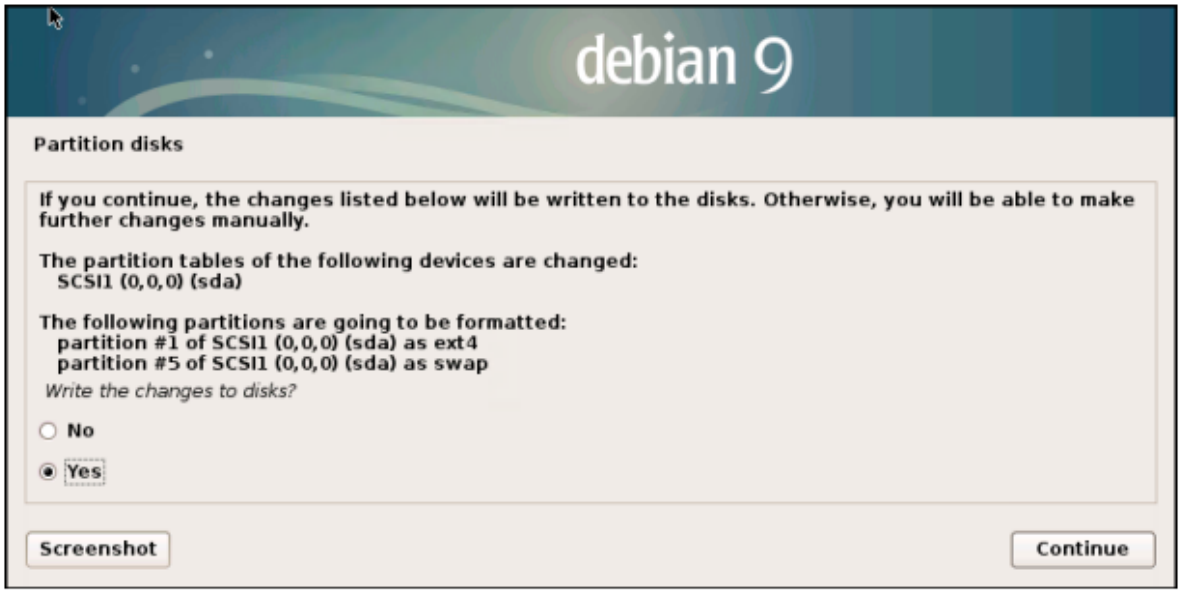
Configurar el reloj del sistema

IMPORTANTE



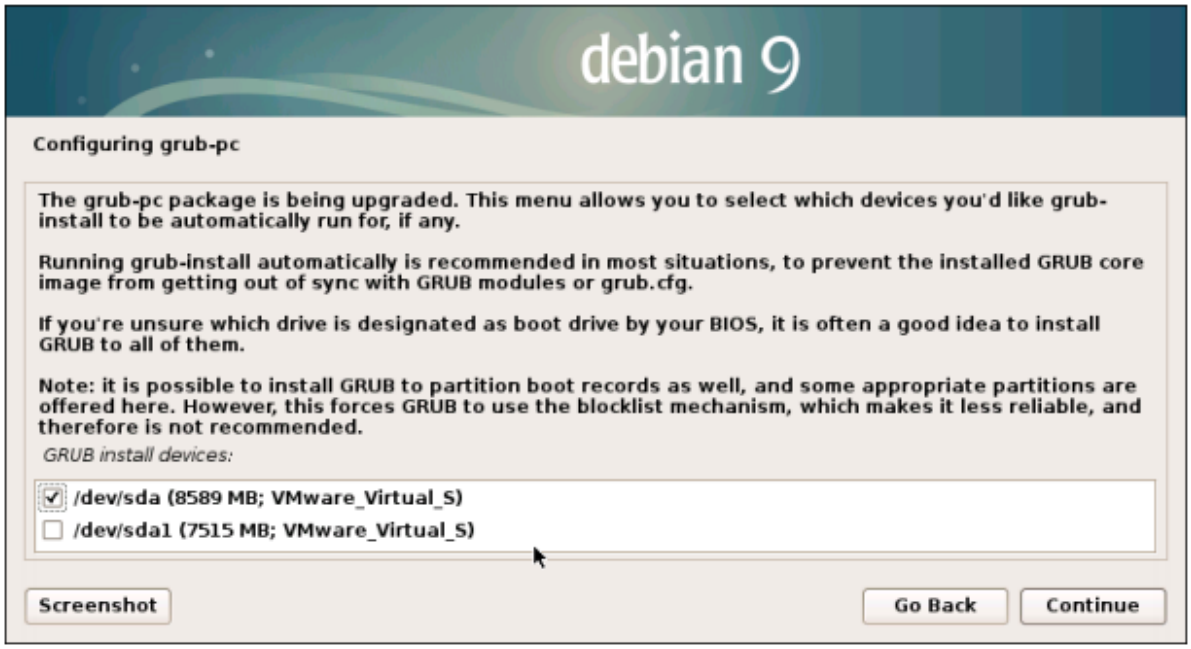
El sistema configura las particiones del disco, hacer clic en yes y dar continue

IMPORTANTE



Iniciará la instalación del paquete del GRUP PC. Se debe seleccionar una unidad y dar clic en continuar

IMPORTANTE



Después de haber desplegado el proceso de instalación, el sistema preguntará si se desea escanear otro CD o DVD, se debe dar clic en No y dar en continuar

IMPORTANTE



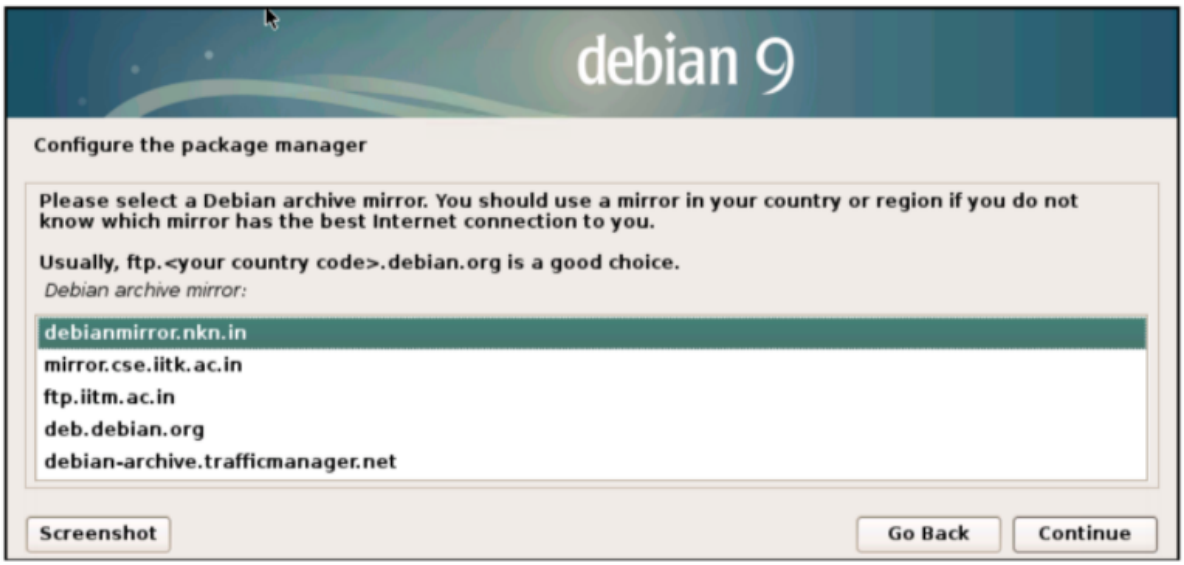
Seleccionar el país para configurar el paquete de gestión de Nemesis

IMPORTANTE

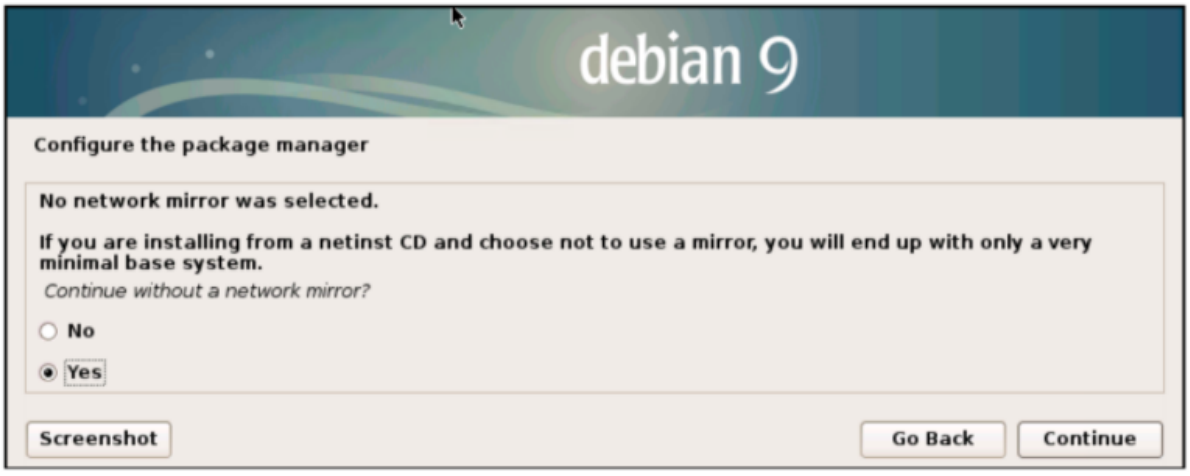


Seleccionar el archivo debian correspondiente y dar clic en continuar

IMPORTANTE

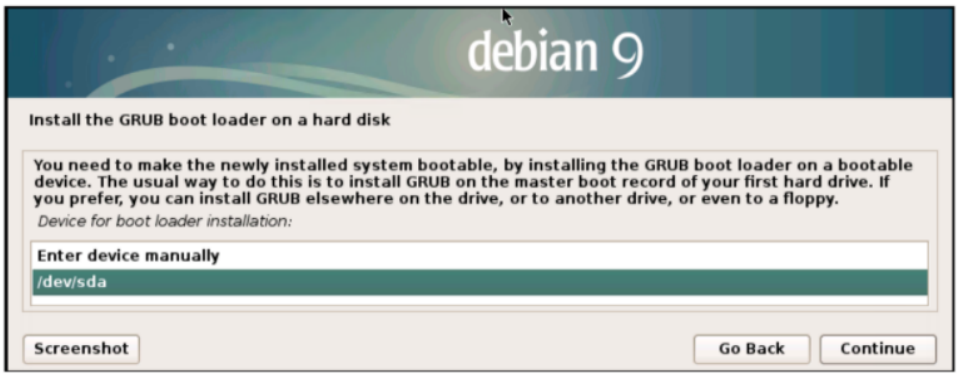


Dar clic en Yes para configurar el administrador de paquetes



Instalar el boot del grupo pc para que cargue en el disco duro. se debe seleccionar la opción por defecto y dar clic en continuar.

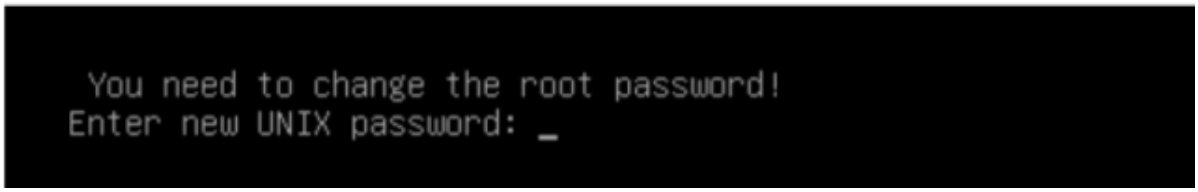
IMPORTANTE



Después de terminar el proceso de instalación, Nemesis iniciara el cargue de su sistema operativo

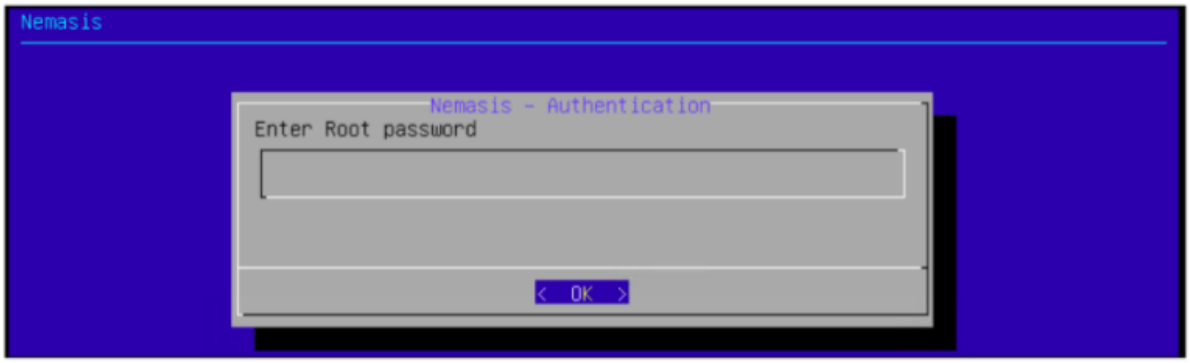


Para completar la instalación, se solicitará una nueva contraseña para el usuario root

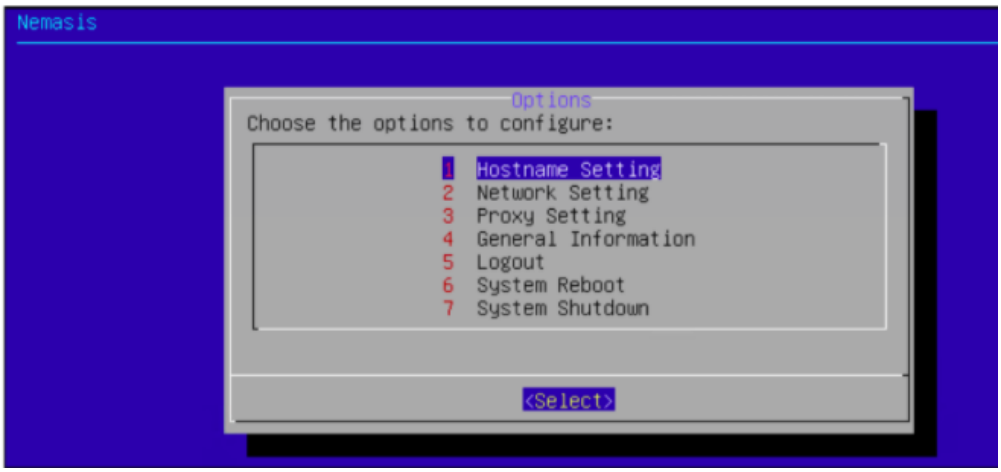


Posteriormente para ingresar al sistema escriba la contraseña anteriormente configurada

IMPORTANTE



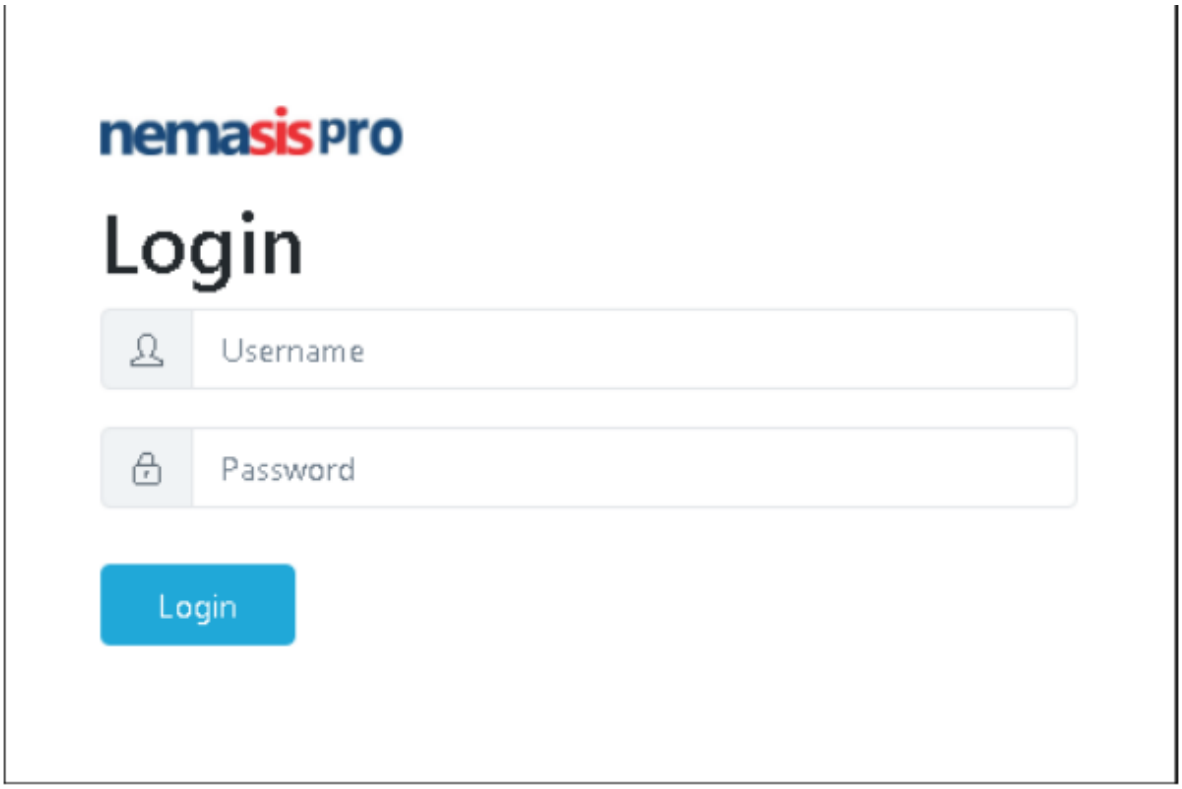
Se despliega un menú de opciones para configurar el sistema como se muestra a continuación



Posteriormente a la instalación, se puede ingresar a la herramienta de seguridad por medio de los navegadores de internet, como Google Chrome, Mozilla, Microsoft Edge e Internet Explorer versiòn11.

Se debe ingresar la url con la IP que se configuró en la herramienta por el puerto 10042. de la forma *https://<IP Address de Nemesis>:10042.* Con las credenciales por defecto **user:** admin y **password:** admin

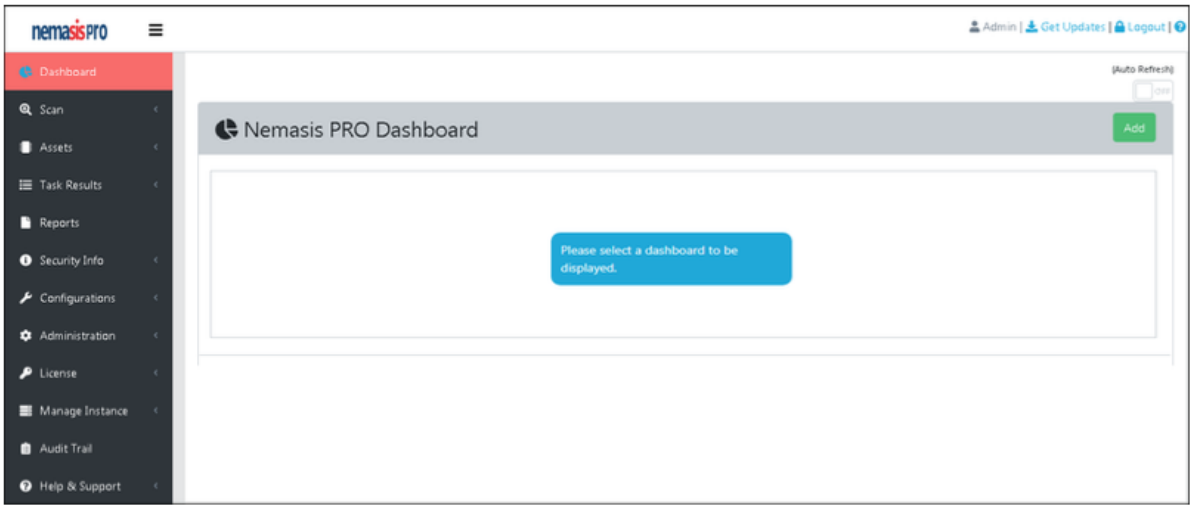
IMPORTANTE



La consola mostrará al lado izquierdo los siguientes módulos que tiene para administrar la red de la compañía.

- Dashboard
- Scan
- Assets
- Task Results
- Reports
- Security info
- Configuration
- Administration
- License
- Manage Instance
- Audit Trial
- Help & support

IMPORTANTE



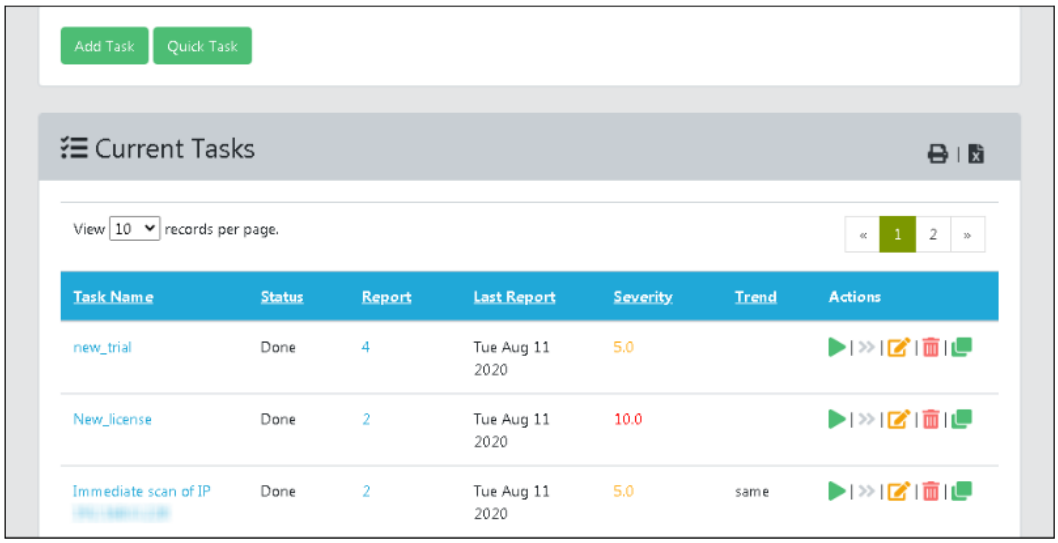
Configuraciòn módulo de escaneo.

En el módulo escaneo existen 3 opciones para realizar el escaneo de la red, *Task, Quick Task, Advanced Quick Task.*

Task.

En este submódulo se puede observar las tareas configuradas, el estado del escaneo cuando se esté realizando, los reportes y la severidad de la tarea.

IMPORTANTE

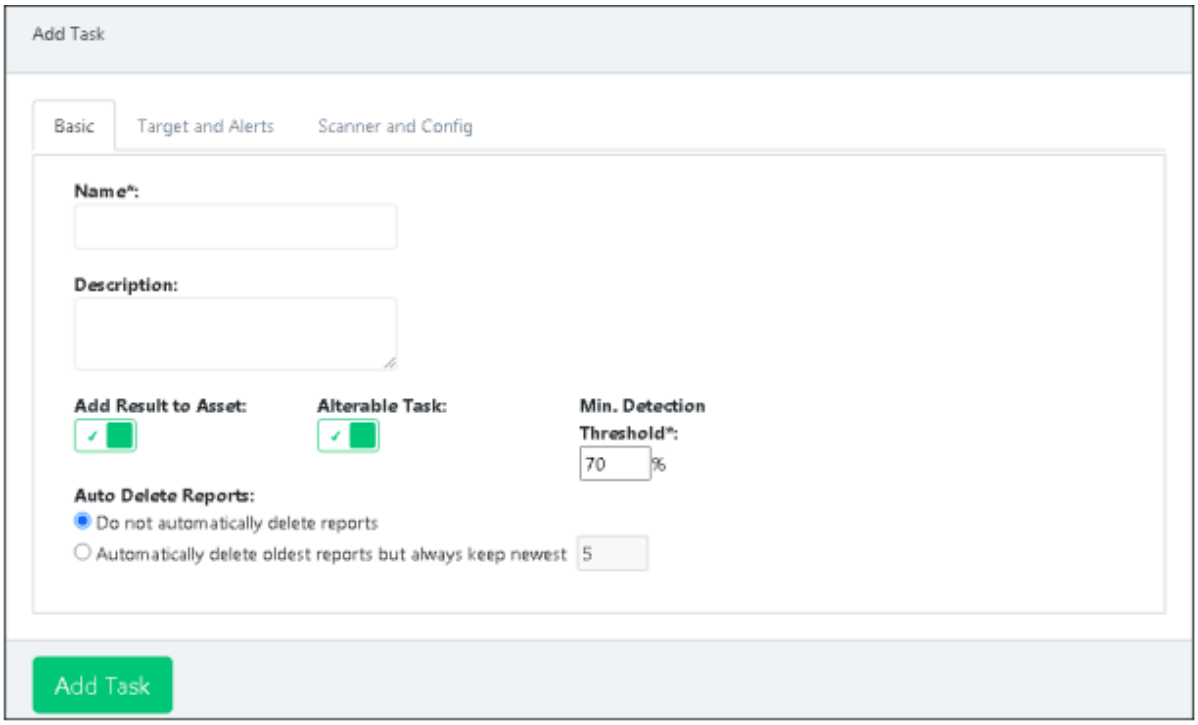


La severidad está categorizada por niveles de bajo, medio y alto. Por defecto los rangos de la severidad son para bajo de 1 a 4, medio de 4.1 a 7 y alto de 7.1 a 10.

La columna ***Trend*** muestra y compara los resultados del último escaneo realizado con respecto al actual. Si en el resultado se encontraron menos alertas, esta columna mostrará *down*, si se encontraron más alertas, mostrará *UP*, y si se mantiene el mismo número de alertas, mostrará *same.*

Para añadir una tarea nueva, se da clic sobre el botón Add task y aparecen tres diferentes opciones de configuración, *Basic, Target and Alerts y scanner configuration.*

IMPORTANTE



Basic:

En esta ventana se puede configurar el nombre de la tarea, una descripción y habilitar el campo Add Result to Asset para que se adicione el resultado de esta tarea al módulo activo, por defecto aparece habilitada.

Alterable Task , Esta opción permite modificar una tarea aun cuando el reporte se encuentre generado, si se modifica dichas tareas no habrá coincidencias entre los últimos informes generados.

El campo *Min Detection Threshold,* establece el porcentaje de la calidad, para que los resultados se adicionen al database de activos.

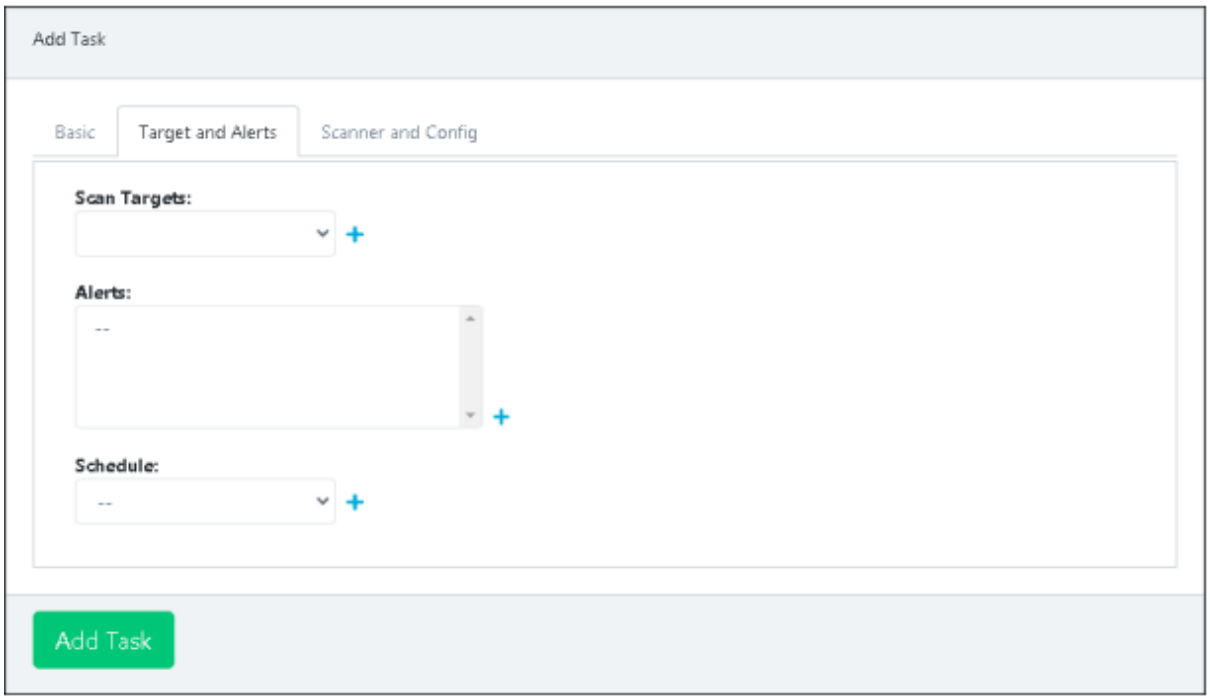
La opción de *Auto Delete reports,* permite eliminar los reportes de manera automática o de manera manual. Si se elige la opción de eliminar los reportes de manera automática, se debe

IMPORTANTE

especificar el número de reportes que se desea almacenar, después de superar esa cantidad de reportes, la herramienta elimina desde el más antiguo al más reciente. Por defecto aparece seleccionada la opción de no eliminar los reportes de manera automática.

Targets and Alerts

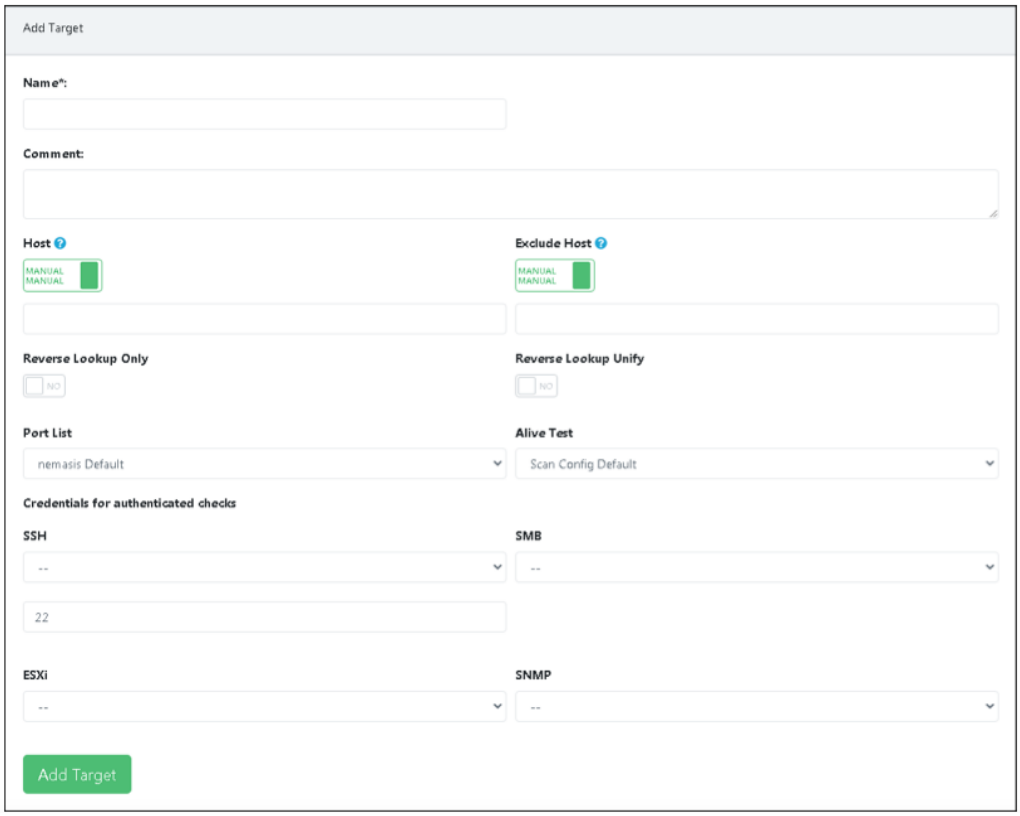
En esta pestaña se puede elegir o adicionar los destinos que se quiera escanear de la lista configurada en la herramienta, así mismo como las alertas y el horario que se desea realizar.



IMPORTANTE

Scan Target:

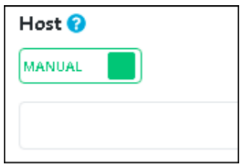
Es una lista que se puede escoger para elegir el destino que se desea configurar. Esta lista puede ser de un host o varios host. Para adicionar un nuevo destino se debe configurar los siguientes parámetros:

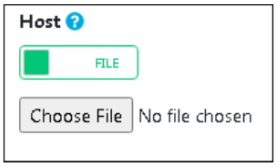


Nombre: Nombre del destino
Comentario: Descripción del destino
Host: Se define la IP o una lista de IP que se pueden importar. Para escribir la IP se puede realizar en los formatos tradicionales x.x.x.x
por rango, por ejemplo, 192.168.128.30-40
por mascara de red 192.168.30.0/24

IMPORTANTE

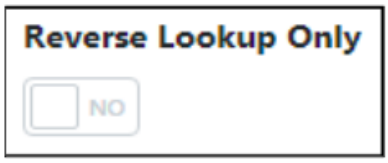
Para cargar un archivo debe ser csv o txt. En este caso se debe dar clic en el botón de host y validar que cambie de manual a file para seleccionar el archivo que se quiere subir

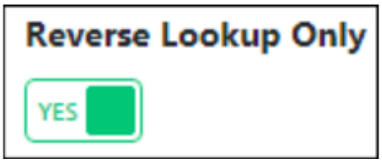




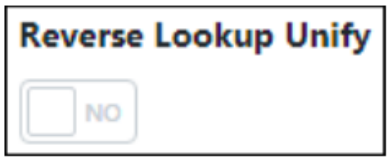
Excluir host: Define las IP que se desean excluir del archivo. Si se tiene un archivo con las IP a excluir se debe dar clic en el botón de exclude host para elegir el archivo que se quiere subir.

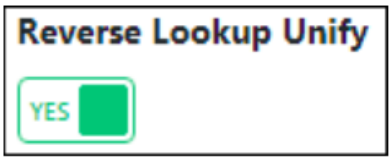
Reverse Lookup Only: Esta opción permite escanear las IP que resuelven por un DNS. Por defecto esta opción no está habilitada en la herramienta.





Reverse Lookup Unify: Si un nombre de DNS resuelve varias IP, la herramienta puede escanear una sola vez por nombre. Por defecto esta opción no está habilitada en la herramienta.





Lista de puertos: Selecciona la lista de puertos permitidas para el escaneo de los diferentes dispositivos de la red,

Alive Test: En esta opción se configura el método para probar si el destino es alcanzado por la herramienta para realizar el escaneo. Se puede configurar con cualquiera de las siguientes opciones:

IMPORTANTE

ICMP Ping
TCP-ACK Service Ping
TCP-SYN Service Ping
ARP Ping
ICMP & TCP-ACK Service Ping
ICMP & ARP Ping

TCP-ACK Service & ARP Ping
ICMP, TCP-ACK Service & ARP Ping
Consider Alive
Scan Config Default

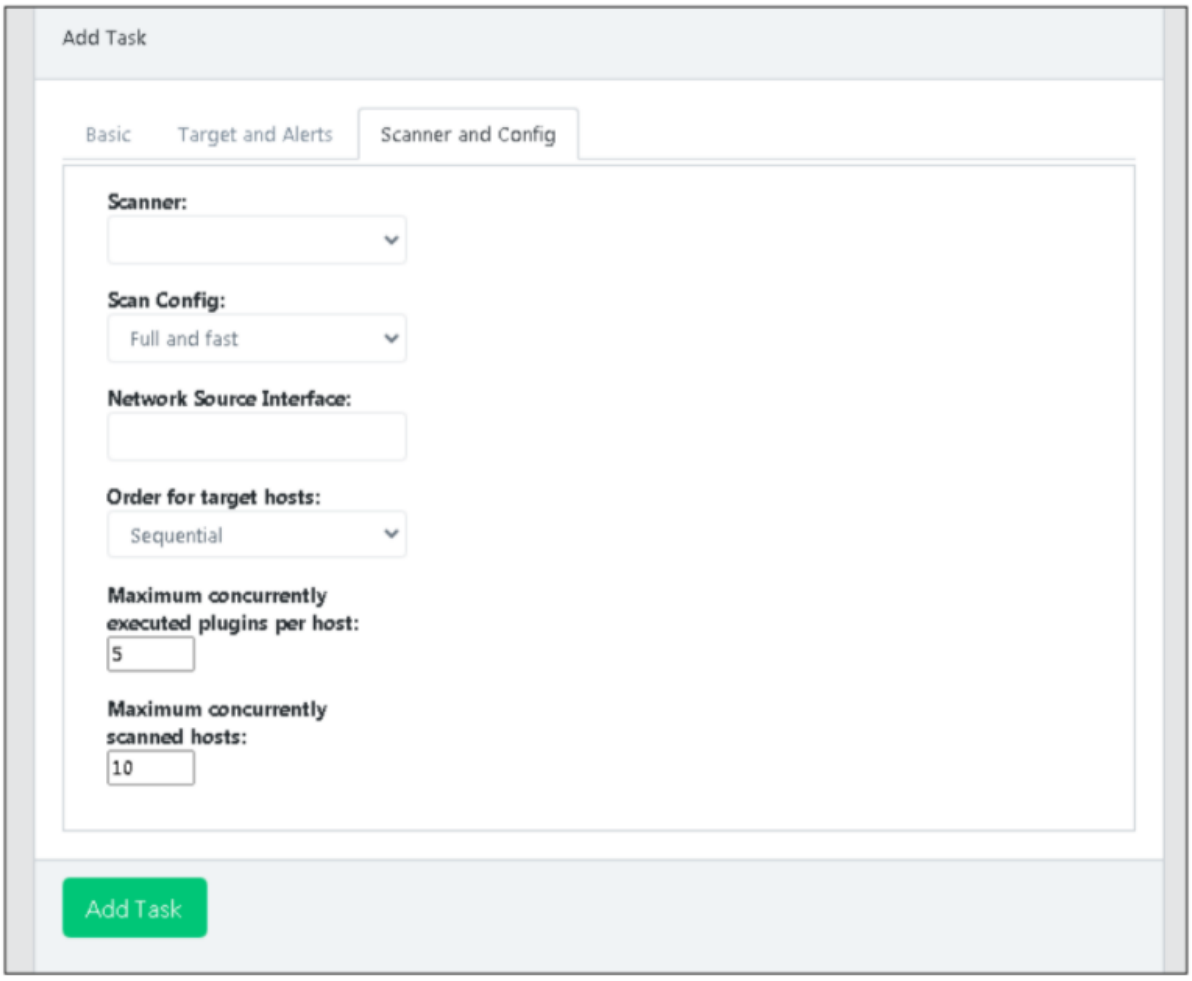
Credenciales para autenticación

Selecciona la manera de ingresar al dispositivo de destino, se tiene varias opciones según el sistema operativo del dispositivo.

Scanner and Config

En esta pestaña se puede configurar los parámetros de configuración para escanear la red, se puede elegir el modo de escaneo, se debe escribir la interfaz origen de la herramienta que se desea escanear, el orden de los host, se puede elegir entre secuencial, aleatorio o invertido.

IMPORTANTE



Las opciones de *Maximum concurrently executed plugins per host / Maximum concurrently scanned hosts,* permite elegir el número máximo de complementos y el número máximo de host que se pueden realizar por cada escaneo.

IMPORTANTE