Ponga en marcha Cloud Data Sense

Cloud Data Sense

NetApp
March 08, 2023

Tabla de Contenido

Ponga en marcha Cloud Data Sense

Ponga en marcha Cloud Data en el cloud

Complete unos pasos para poner en marcha Cloud Data en el cloud. La instancia de detección de datos se pondrá en marcha en la misma red de proveedores de cloud que BlueXP Connector.

Tenga en cuenta que también puede "Instale Data Sense en un host Linux que tenga acceso a Internet". Este tipo de instalación puede ser una buena opción si prefiere analizar sistemas ONTAP en las instalaciones mediante una instancia de Data Sense que también está ubicada en las instalaciones — pero esto no es un requisito. El software funciona exactamente de la misma manera, independientemente del método de instalación que elija.

Inicio rápido

Empiece rápidamente siguiendo estos pasos o desplácese hacia abajo hasta las secciones restantes para obtener todos los detalles.

Cree un conector

Si aún no tiene un conector, cree un conector ahora. Consulte "Creación de un conector en AWS", "Creación de un conector en Azure", o. "Creación de un conector en GCP".

También puede hacerlo "Ponga en marcha el conector en las instalaciones" En un host Linux en su red o en la nube.

Revise los requisitos previos

Asegúrese de que el entorno pueda cumplir con los requisitos previos. Esto incluye acceso saliente a Internet para la instancia, conectividad entre el conector y Cloud Data SENSE a través del puerto 443, entre otros. Vea la lista completa.

La configuración predeterminada requiere 16 vCPU para la instancia de Cloud Data Sense. Consulte "más detalles acerca del tipo de instancia".

Ponga en marcha Cloud Data Sense

Inicie el asistente de instalación para implementar la instancia de Cloud Data Sense en el cloud.

Suscríbase al servicio Cloud Data Sense

Los primeros 1 TB de datos que analiza Cloud Data Sense en BlueXP son gratuitos durante 30 días. Debe haber una suscripción a BlueXP a través de su plataforma de proveedores de cloud o una licencia BYOL de NetApp para continuar analizando los datos después de ese punto.

Cree un conector

Si aún no tiene un conector, cree un conector en su proveedor de cloud. Consulte "Creación de un conector en AWS" o. "Creación de un conector en Azure", o. "Creación de un conector en GCP". En la mayoría de los casos, es probable que tenga un conector configurado antes de intentar activar Cloud Data Sense porque la mayoría "Las funciones de BlueXP requieren un conector", pero hay casos en los que necesitará configurar uno ahora.

Existen algunas situaciones en las que debe utilizar un conector implementado en un proveedor de cloud específico:

- Cuando se escanear datos en Cloud Volumes ONTAP en AWS, Amazon FSX para ONTAP o en bloques AWS S3, se utiliza un conector en AWS.
- Al analizar datos en Cloud Volumes ONTAP en Azure o en Azure NetApp Files, utiliza un conector en Azure.
  - Para Azure NetApp Files, debe implementarse en la misma región que los volúmenes que desea analizar.
- Al analizar datos en Cloud Volumes ONTAP en GCP, se utiliza un conector en GCP.

Los sistemas ONTAP en las instalaciones, recursos compartidos de archivos que no son de NetApp, almacenamiento de objetos genéricos de S3, bases de datos, carpetas de OneDrive, cuentas de SharePoint y cuentas de Google Drive se pueden analizar al utilizar cualquiera de estos conectores de cloud.

Tenga en cuenta que también puede "Ponga en marcha el conector en las instalaciones" En un host Linux en su red o en la nube. Algunos usuarios que planean instalar Data Sense on-prem también pueden optar por instalar el conector on-prem.

Como puede ver, puede que haya algunas situaciones en las que necesite utilizar "Múltiples conectores".

Apoyo del Gobierno en las regiones

Cloud Data Sense es compatible cuando el conector se ha puesto en marcha en una región gubernamental (AWS GovCloud, Azure Gov o Azure DoD). Cuando se implementa de esta manera, Data Sense tiene las siguientes restricciones:

- Las cuentas de OneDrive, cuentas de SharePoint y cuentas de Google Drive no se pueden analizar.
- La funcionalidad de etiqueta de Microsoft Azure Information Protection (AIP) no se puede integrar.

Revise los requisitos previos

Revise los siguientes requisitos previos para asegurarse de que dispone de una configuración compatible antes de implementar Cloud Data Sense en el cloud.

Habilite el acceso a Internet de salida desde Cloud Data Sense

Cloud Data Sense requiere acceso saliente a Internet. Si la red virtual o física utiliza un servidor proxy para el acceso a Internet, asegúrese de que la instancia de detección de datos tiene acceso saliente a Internet para contactar con los siguientes puntos finales. Al implementar Data Sense en la nube, se encuentra en la misma subred que el conector.

Revise la siguiente tabla según cuál sea su caso, ya se esté poniendo en marcha Cloud Data Sense en AWS, Azure o GCP.

extremos necesarios para implementaciones de AWS:

Puntos finales	Específico
https://api.bluexp.netapp.com	Comunicación con el servicio BlueXP, que incluye cuentas de NetApp.
https://netapp-cloud-account.auth0.com https://auth0.com	Comunicación con el sitio Web de BlueXP para la autenticación centralizada del usuario.
https://cloud-compliance-support-netapp.s3.us-west-2.amazonaws.com https://hub.docker.com https://auth.docker.io https://registry-1.docker.io https://index.docker.io/ https://dseasb33srnrn.cloudfront.net/ https://production.cloudflare.docker.com/	Proporciona acceso a imágenes, manifiestos y plantillas de software.
https://kinesis.us-east-1.amazonaws.com	Permite a NetApp transmitir datos desde registros de auditoría.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://user-feedback-store-prod.s3.us-west-2.amazonaws.com https://customer-data-production.s3.us-west-2.amazonaws.com	Permite que Cloud Data Sense acceda y descargue manifiestos y plantillas, así como para enviar registros y métricas.

Extremos necesarios para implementaciones de Azure y GCP:

Puntos finales	Específico
https://api.bluexp.netapp.com	Comunicación con el servicio BlueXP, que incluye cuentas de NetApp.
https://netapp-cloud-account.auth0.com https://auth0.com	Comunicación con el sitio Web de BlueXP para la autenticación centralizada del usuario.
https://support.compliance.api.bluexp.netapp.com/ https://hub.docker.com https://auth.docker.io https://registry-1.docker.io https://index.docker.io/ https://dseasb33srnrn.cloudfront.net/ https://production.cloudflare.docker.com/	Proporciona acceso a imágenes de software, manifiestos, plantillas y para enviar registros y métricas.
https://support.compliance.api.bluexp.netapp.com/	Permite a NetApp transmitir datos desde registros de auditoría.

Asegúrese de que BlueXP tiene los permisos necesarios

Asegúrese de que BlueXP tiene permisos para implementar recursos y crear grupos de seguridad para la instancia de Cloud Data Sense. Puede encontrar los últimos permisos de BlueXP en "Las políticas proporcionadas por NetApp".

Compruebe sus límites de vCPU

Compruebe que el límite de vCPU de su proveedor de cloud permita poner en marcha una instancia con 16 núcleos. Deberá verificar el límite de vCPU para la familia de instancias correspondiente en la región donde se está ejecutando BlueXP. "Consulte los tipos de instancia necesarios".

Consulte los siguientes enlaces para obtener más información sobre los límites de vCPU:

- "Documentación de AWS: Cuotas de servicio de Amazon EC2"
- "Documentación de Azure: Cuotas de vCPU de máquina virtual"
- "Documentación de Google Cloud: Cuotas de recursos"

  Tenga en cuenta que puede implementar la detección de datos en un sistema con menos CPU y menos RAM, pero existen limitaciones al utilizar estos sistemas. Consulte "Con un tipo de instancia más pequeño" para obtener más detalles.

Asegúrese de que BlueXP Connector puede acceder a Cloud Data Sense

Asegure la conectividad entre el conector y la instancia de Cloud Data Sense. El grupo de seguridad del conector debe permitir el tráfico entrante y saliente a través del puerto 443 hacia y desde la instancia de detección de datos. Esta conexión permite la implementación de la instancia de Data Sense y permite ver información en las fichas cumplimiento y Gobierno. Cloud Data Sense es compatible en regiones gubernamentales de AWS y Azure.

Se requieren reglas adicionales de grupos de seguridad entrantes y salientes para las implementaciones de AWS GovCloud. Consulte "Reglas para el conector en AWS" para obtener más detalles.

Se requieren reglas adicionales de grupos de seguridad entrantes y salientes para implementaciones gubernamentales de Azure y Azure. Consulte "Reglas para Connector en Azure" para obtener más detalles.

Asegúrese de que puede mantener en funcionamiento Cloud Data Sense

La instancia de Cloud Data Sense tiene que seguir para poder analizar sus datos de forma continua.

Garantice la conectividad del navegador web con Cloud Data Sense

Después de habilitar Cloud Data Sense, asegúrese de que los usuarios acceden a la interfaz BlueXP desde un host que tiene una conexión a la instancia de detección de datos.

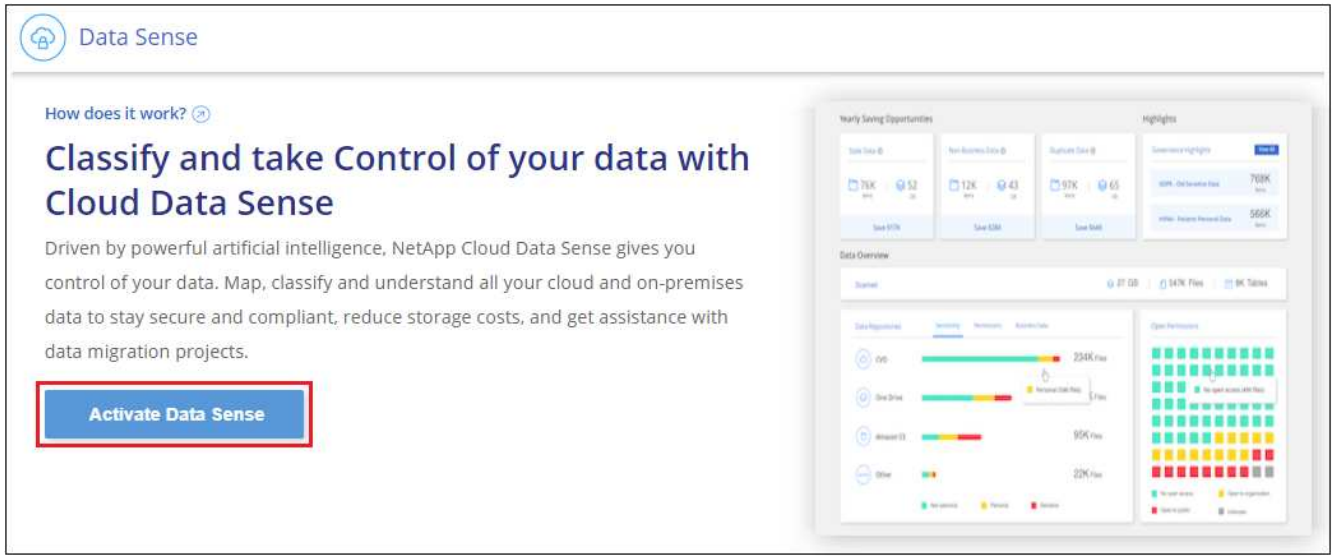
La instancia de detección de datos utiliza una dirección IP privada para garantizar que los datos indexados no sean accesibles a Internet. Como resultado, el navegador web que utiliza para acceder a BlueXP debe tener una conexión a esa dirección IP privada. Esa conexión puede provenir de una conexión directa a su proveedor de cloud (por ejemplo, una VPN) o de un host que esté dentro de la misma red que la instancia de Data Sense.

Ponga en marcha el sentido de los datos en el cloud

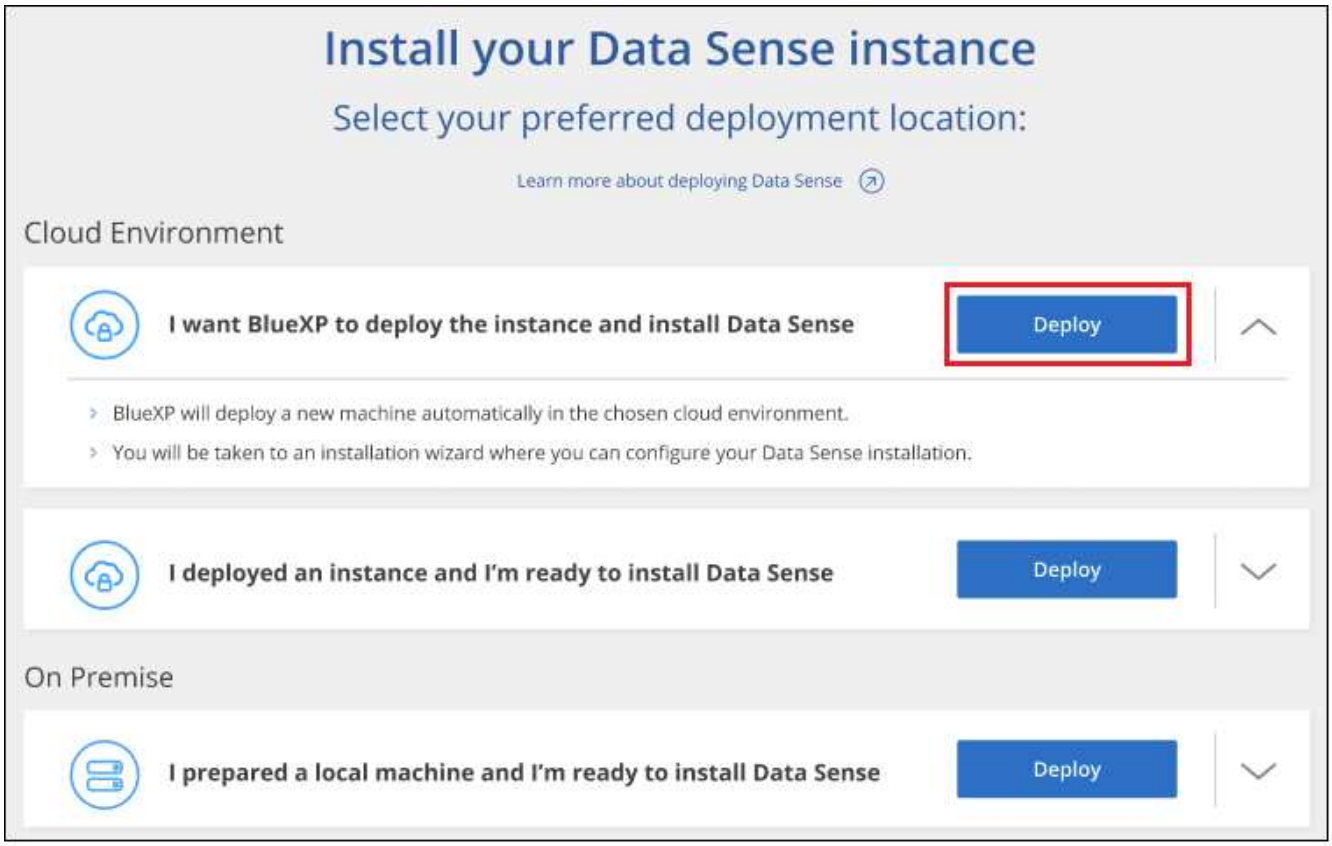
Siga estos pasos para poner en marcha una instancia de Cloud Data Sense en el cloud.

Pasos

1. En el menú de navegación izquierdo de BlueXP, haga clic en **Gobierno > Clasificación**.
2. Haga clic en **Activar detección de datos**.



3. Haga clic en **desplegar** para iniciar el asistente de implementación de la nube.



4. El asistente muestra el progreso a medida que avanza por los pasos de implementación. Se detendrá y pedirá información si se presenta algún problema.

5. Cuando se despliegue la instancia, haga clic en **continuar con la configuración** para ir a la página *Configuration*.

Resultado

BlueXP pone en marcha la instancia de Cloud Data Sense en su proveedor de cloud.

Las actualizaciones al conector BlueXP y al software de detección de datos se automatizan siempre que las instancias tengan conexión a Internet.

El futuro

En la página Configuración puede seleccionar los orígenes de datos que desea analizar.

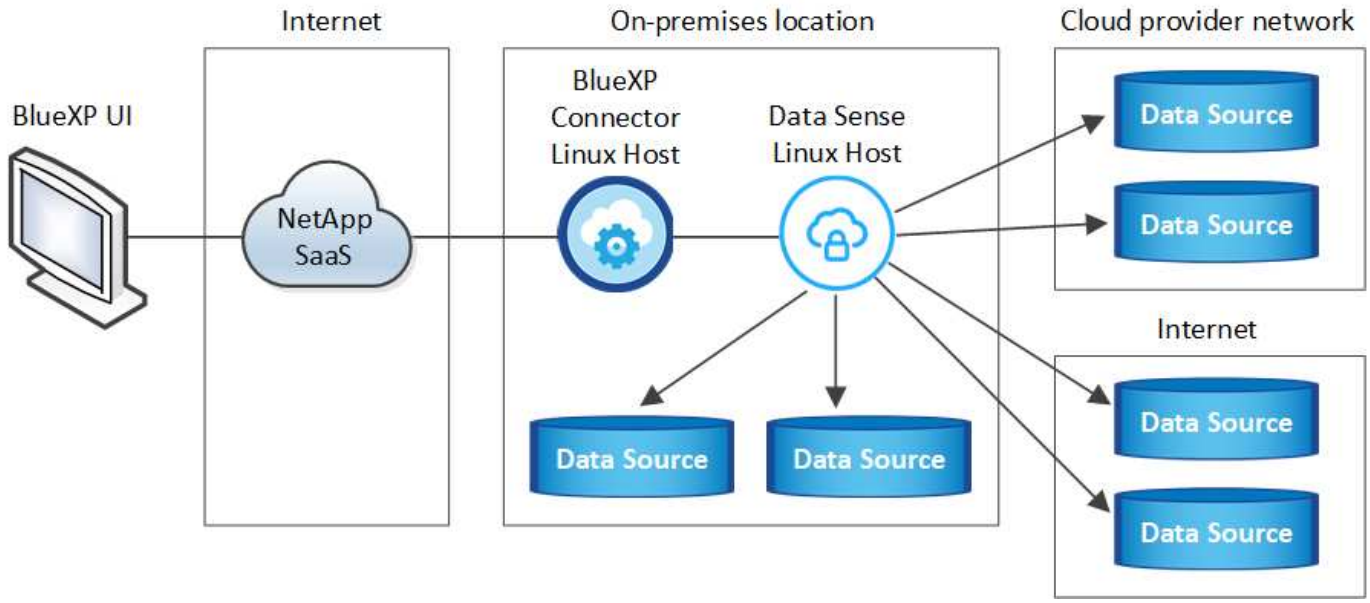
También puede hacerlo "Configure la licencia de Cloud Data Sense" en este momento. No se le cobrará hasta que finalice su prueba gratuita de 30 días.

Ponga en marcha Cloud Data Sense en un host que tiene acceso a Internet

Complete unos pasos para implementar Cloud Data Sense en un host Linux de su red, o en un host Linux en la nube, que tenga acceso a Internet.

La instalación en las instalaciones puede ser una buena opción si prefiere analizar sistemas ONTAP en las instalaciones mediante una instancia de detección de datos que también está ubicada en las instalaciones, pero esto no es un requisito. El software funciona exactamente de la misma manera, independientemente del método de instalación que elija.

La instalación típica en las instalaciones tiene los siguientes componentes y conexiones.



En configuraciones de gran tamaño en las que va a escanear petabytes de datos, puede incluir varios hosts para proporcionar una capacidad de procesamiento adicional. Cuando se utilizan varios sistemas host, el sistema principal se denomina *Manager node* y los sistemas adicionales que proporcionan potencia de procesamiento adicional se denominan *Scanner Nodes*.

Tenga en cuenta que también puede "Ponga en marcha la detección de datos en un sitio en las instalaciones que no tenga acceso a Internet" para ubicaciones completamente seguras.

Inicio rápido

Empiece rápidamente siguiendo estos pasos o desplácese hacia abajo hasta las secciones restantes para obtener todos los detalles.

1 Cree un conector

Si aún no tiene un conector, "Ponga en marcha el conector en las instalaciones" En un host Linux de su red o en un host Linux del cloud.

También puede crear un conector con su proveedor de cloud. Consulte "Creación de un conector en AWS", "Creación de un conector en Azure", o. "Creación de un conector en GCP".

2 Revise los requisitos previos

Asegúrese de que el entorno pueda cumplir con los requisitos previos. Esto incluye acceso saliente a Internet para la instancia, conectividad entre el conector y Cloud Data SENSE a través del puerto 443, entre otros. Vea la lista completa.

También necesita un sistema Linux que cumpla con el siga los requisitos.

3 Descargue e implemente Cloud Data Sense

Descargue el software Cloud Data Sense del sitio de soporte de NetApp y copie el archivo del instalador en el host Linux que tiene pensado utilizar. A continuación, inicie el asistente de instalación y siga las instrucciones

para implementar la instancia de detección de datos.

4 **Suscríbase al servicio Cloud Data Sense**

Los primeros 1 TB de datos que analiza Cloud Data Sense en BlueXP son gratuitos durante 30 días. Debe suscribirse a su mercado de proveedores de cloud o una licencia de BYOL de NetApp para continuar analizando los datos después de ese punto.

Cree un conector

Se necesita un conector BlueXP para poder instalar y utilizar Data Sense. En la mayoría de los casos, es probable que tenga un conector configurado antes de intentar activar Cloud Data Sense porque la mayoría "Las funciones de BlueXP requieren un conector", pero hay casos en los que necesitará configurar uno ahora.

Para crear una en su entorno de proveedor de cloud, consulte "Creación de un conector en AWS", "Creación de un conector en Azure", o. "Creación de un conector en GCP".

Existen algunas situaciones en las que debe utilizar un conector implementado en un proveedor de cloud específico:

- Cuando se escanear datos en Cloud Volumes ONTAP en AWS, Amazon FSX para ONTAP o en bloques AWS S3, se utiliza un conector en AWS.
- Al analizar datos en Cloud Volumes ONTAP en Azure o en Azure NetApp Files, utiliza un conector en Azure.

  Para Azure NetApp Files, debe implementarse en la misma región que los volúmenes que desea analizar.

- Al analizar datos en Cloud Volumes ONTAP en GCP, se utiliza un conector en GCP.

Los sistemas ONTAP en las instalaciones, recursos compartidos de archivos que no son de NetApp, almacenamiento de objetos genérico de S3, bases de datos, carpetas de OneDrive, cuentas de SharePoint y cuentas de Google Drive se pueden analizar con cualquiera de estos conectores de cloud.

Tenga en cuenta que también puede "Ponga en marcha el conector en las instalaciones" En un host Linux en su red o en la nube. Algunos usuarios que planean instalar Data Sense on-prem también pueden optar por instalar el conector on-prem.

Como puede ver, puede que haya algunas situaciones en las que necesite utilizar "Múltiples conectores".

Necesitará la dirección IP o el nombre de host del sistema conector al instalar Data Sense. Tendrá esta información si instaló el conector en sus instalaciones. Si el conector está implementado en la nube, puede encontrar esta información desde la consola BlueXP: Haga clic en el icono Ayuda, seleccione **Soporte** y haga clic en **conector BlueXP**.

Prepare el sistema host Linux

El software de detección de datos debe ejecutarse en un host que cumpla con requisitos específicos del sistema operativo, requisitos de RAM, requisitos de software, etc. El host Linux puede estar en su red o en la nube. No se admite la detección de datos en un host que se comparte con otras aplicaciones; el host debe ser un host dedicado.

Asegúrese de que puede mantener en funcionamiento Cloud Data Sense. El equipo Cloud Data Sense tiene que seguir para analizar sus datos de forma continua.

- **CPU**: 16 núcleos
- **RAM**: 64 GB (la memoria de intercambio debe estar desactivada en el host)
- **Disco**: SSD con 500 GIB disponibles en /, o.
  - 100 GIB disponibles en /opt
  - 400 GIB disponibles en /var
  - 5 GIB en /tmp

  Tenga en cuenta que puede implementar la detección de datos en un sistema con menos CPU y menos RAM, pero existen limitaciones al utilizar estos sistemas. Consulte "Con un tipo de instancia más pequeño" para obtener más detalles.
- **Tipo de instancia de AWS EC2**: Tipo de instancia que cumple los requisitos de CPU y RAM anteriores. Lo recomendamos "m5.4xgrande".
- **Tamaño de máquina virtual de Azure**: Tipo de instancia que cumple los requisitos de CPU y RAM anteriores. Lo recomendamos "Standard_D16s_v3".
- **Tipo de máquina GCP**: Tipo de instancia que cumple los requisitos de CPU y RAM anteriores. Lo recomendamos "n2-estándar-16".
- **Sistema operativo**: Red Hat Enterprise Linux o CentOS versiones 8.0 a 8.7
  - CentOS Stream 8 también es compatible
  - Se pueden utilizar las versiones 7.8 o 7.9, pero la versión de kernel de Linux debe ser 4.0 o posterior
  - El sistema operativo debe ser capaz de instalar el motor del docker
- **Red Hat Subscription Management**: Un sistema Red Hat Enterprise Linux debe estar registrado con Red Hat Subscription Management. Si no está registrado, el sistema no puede acceder a los repositorios para actualizar el software de terceros necesario durante la instalación.
- **Software adicional**: Debe instalar el siguiente software en el host antes de instalar Data Sense:
  - Docker Engine versión 19.3.1 o posterior. "Ver las instrucciones de instalación".
  - Python 3 versión 3.6 o posterior. "Ver las instrucciones de instalación".
- * Consideraciones de Firewalld*: Si usted está planeando utilizar `firewalld`, Le recomendamos que lo habilite antes de instalar Data Sense. Ejecute los siguientes comandos para configurar `firewalld` Para que sea compatible con Data Sense:

```
firewall-cmd --permanent --add-service=http
firewall-cmd --permanent --add-service=https
firewall-cmd --permanent --add-port=80/tcp
firewall-cmd --permanent --add-port=8080/tcp
firewall-cmd --permanent --add-port=443/tcp
firewall-cmd --reload
```

Si tiene pensado utilizar hosts de detección de datos adicionales como nodos de escáner, agregue estas reglas al sistema principal en este momento:

```
firewall-cmd --permanent --add-port=2377/tcp
firewall-cmd --permanent --add-port=7946/udp
firewall-cmd --permanent --add-port=7946/tcp
firewall-cmd --permanent --add-port=4789/udp
```

Si activa `firewalld` Después de instalar Data Sense, debe reiniciar docker.

La dirección IP del sistema host Data Sense no se puede cambiar tras la instalación.

Habilite el acceso a Internet de salida desde Cloud Data Sense

Cloud Data Sense requiere acceso saliente a Internet. Si la red virtual o física utiliza un servidor proxy para el acceso a Internet, asegúrese de que la instancia de detección de datos tiene acceso saliente a Internet para contactar con los siguientes puntos finales.

Puntos finales	Específico
https://api.bluexp.netapp.com	Comunicación con el servicio BlueXP, que incluye cuentas de NetApp.
https://netapp-cloud-account.auth0.com https://auth0.com	Comunicación con el sitio Web de BlueXP para la autenticación centralizada del usuario.
https://support.compliance.api.bluexp.netapp.com/ https://hub.docker.com https://auth.docker.io https://registry-1.docker.io https://index.docker.io/ https://dseasb33srnrn.cloudfront.net/ https://production.cloudflare.docker.com/	Proporciona acceso a imágenes de software, manifiestos, plantillas y para enviar registros y métricas.
https://support.compliance.api.bluexp.netapp.com/	Permite a NetApp transmitir datos desde registros de auditoría.
https://github.com/docker https://download.docker.com http://mirror.centos.org http://mirrorlist.centos.org http://mirror.centos.org/centos/7/extras/x86_64/Packages/container-selinux-2.107-3.el7.noarch.rpm	Proporciona paquetes de requisitos previos para la instalación.

Verifique que todos los puertos necesarios estén habilitados

Debe asegurarse de que todos los puertos necesarios estén abiertos para la comunicación entre el conector, detección de datos, Active Directory y sus orígenes de datos.

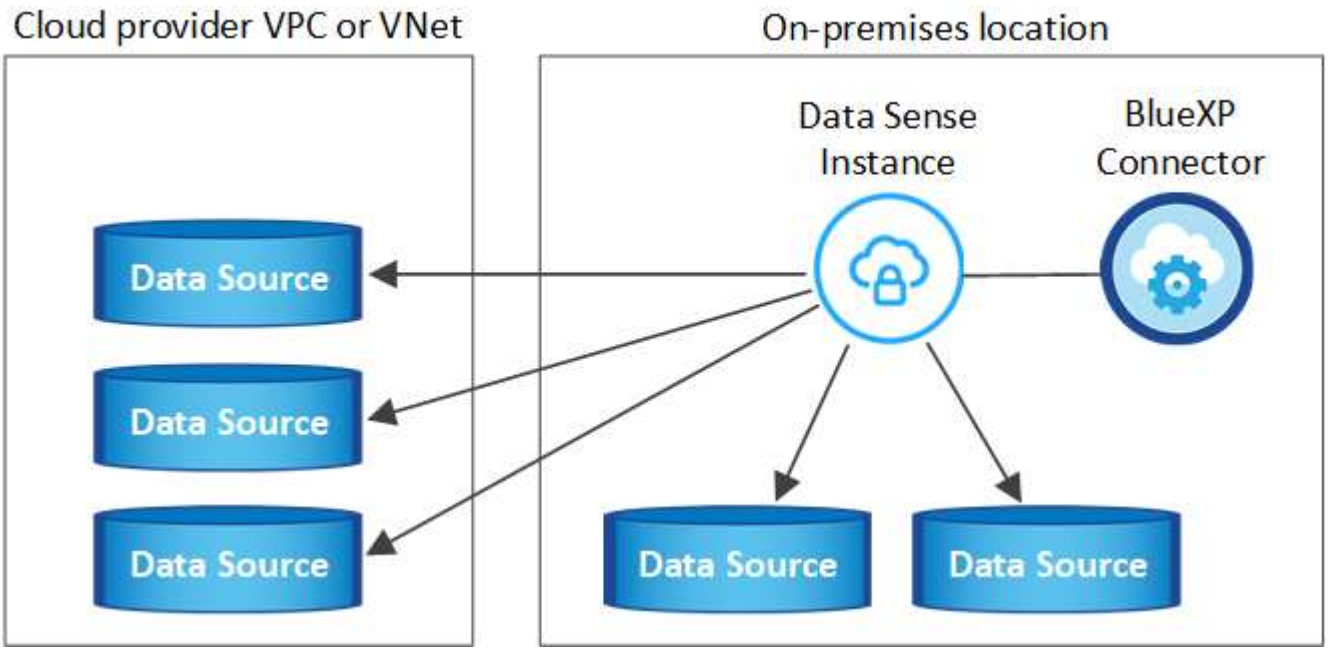
Tipo de conexión	Puertos	Descripción
Conector <> detección de datos	8080 (TCP), 443 (TCP) y 80	El firewall o las reglas de enrutamiento del conector deben permitir el tráfico entrante y saliente a través del puerto 443 hacia y desde la instancia de detección de datos. Asegúrese de que el puerto 8080 está abierto para que pueda ver el progreso de la instalación en BlueXP.
Conector <> clúster ONTAP (NAS)	443 (TCP)	BlueXP detecta los clústeres de ONTAP mediante HTTPS. Si utiliza directivas de firewall personalizadas, deben cumplir los siguientes requisitos: • El host del conector debe permitir el acceso HTTPS de salida a través del puerto 443. Si el conector está en la nube, todas las comunicaciones salientes se permiten mediante el firewall predefinido o las reglas de enrutamiento. • El clúster ONTAP debe permitir el acceso HTTPS de entrada a través del puerto 443. La política de firewall "mgmt" predeterminada permite el acceso HTTPS entrante desde todas las direcciones IP. Si ha modificado esta directiva predeterminada o si ha creado su propia directiva de firewall, debe asociar el protocolo HTTPS con esa directiva y habilitar el acceso desde el host de Connector.
Detección de los datos <> clúster de ONTAP	• Para NFS: 111 (TCP\UDP) y 2049 (TCP\UDP) • Para CIFS: 139 (TCP\UDP) y 445 (TCP\UDP)	Data Sense necesita una conexión de red a cada subred de Cloud Volumes ONTAP o a cada sistema ONTAP en las instalaciones. Los firewalls o las reglas de enrutamiento para Cloud Volumes ONTAP deben permitir conexiones entrantes desde la instancia de detección de datos. Asegúrese de que estos puertos estén abiertos a la instancia de Data Sense: • Para NFS: 111 y 2049 • Para CIFS - 139 y 445 Las políticas de exportación de volúmenes NFS deben permitir el acceso desde la instancia de Data Sense.

Tipo de conexión	Puertos	Descripción
Sentido de los datos <> Active Directory	389 (TCP Y UDP), 636 (TCP), 3268 (TCP) Y 3269 (TCP)	Debe tener un Active Directory ya configurado para los usuarios de su empresa. Además, Data Sense necesita credenciales de Active Directory para analizar volúmenes CIFS. Debe tener la información de Active Directory: • DNS Server IP Address o varias direcciones IP • Nombre de usuario y contraseña para el servidor • Nombre de dominio (nombre de Active Directory) • Si utiliza o no un LDAP seguro (LDAPS) • Puerto de servidor LDAP (normalmente 389 para LDAP y 636 para LDAP seguro)

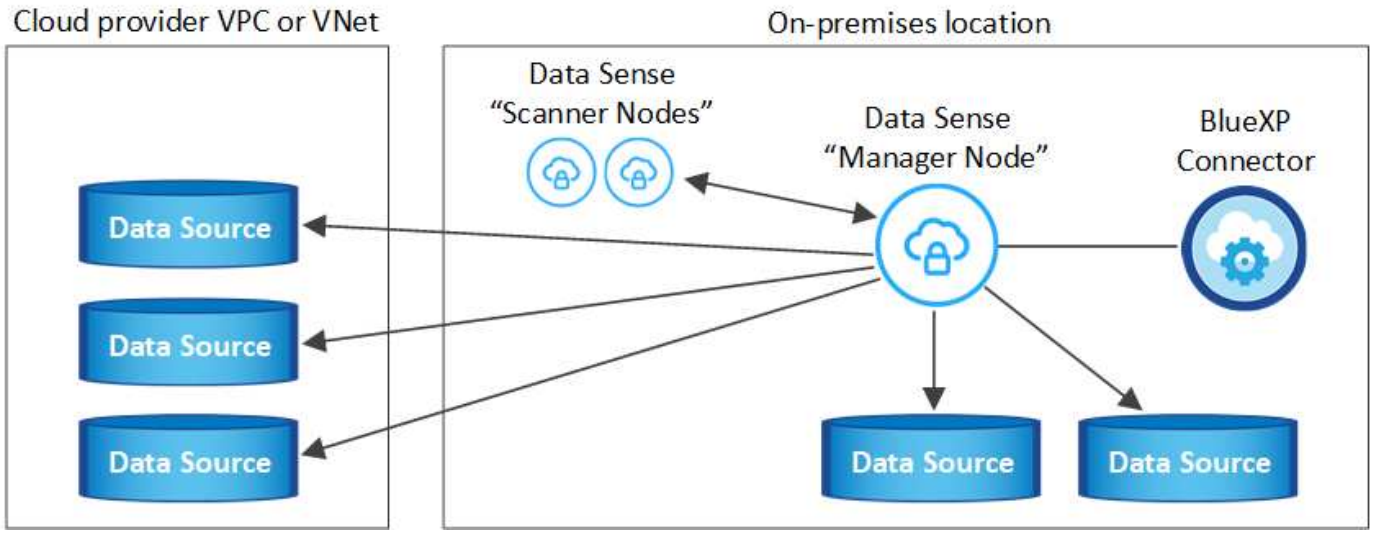
Si utiliza varios hosts de detección de datos para proporcionar potencia de procesamiento adicional para analizar sus fuentes de datos, tendrá que habilitar puertos y protocolos adicionales. "Consulte los requisitos de puerto adicionales".

Ponga en marcha la detección de datos en las instalaciones

En configuraciones típicas, instalará el software en un único sistema host. Consulte estos pasos aquí.



En configuraciones de gran tamaño en las que va a escanear petabytes de datos, puede incluir varios hosts para proporcionar una capacidad de procesamiento adicional. Consulte estos pasos aquí.



Consulte Preparar el sistema host Linux y.. Revisión de requisitos previos Para ver la lista completa de requisitos antes de poner en marcha Cloud Data Sense.

Las actualizaciones del software Data Sense se automatizan siempre que la instancia tenga conectividad a Internet.

Cloud Data Sense no puede analizar actualmente bloques de S3, Azure NetApp Files o FSX para ONTAP cuando el software está instalado en las instalaciones. En estos casos, deberá poner en marcha un conector e instancia aparte de detección de datos en el cloud y en "Cambiar entre conectores" para sus diferentes fuentes de datos.

Instalación de un solo host para configuraciones típicas

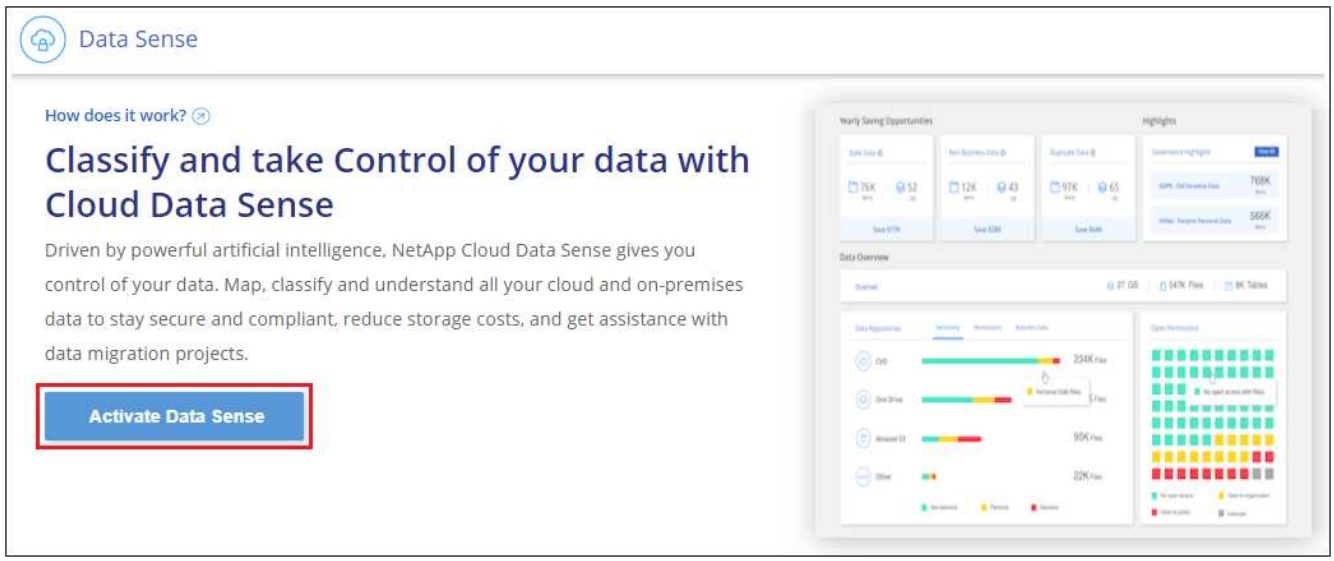
Siga estos pasos al instalar el software Data Sense en un solo host local.

Lo que necesitará

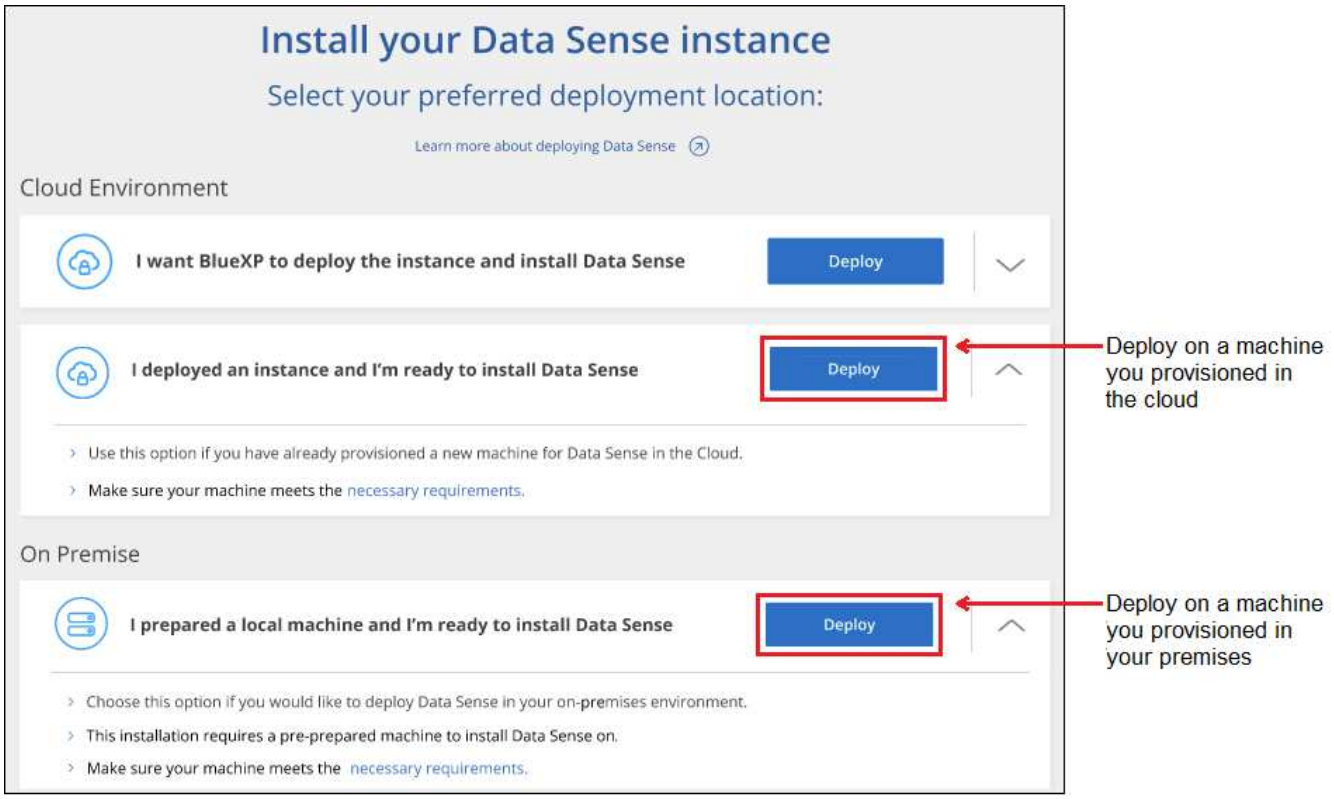
- Compruebe que su sistema Linux cumple con el requisitos del host.
- Compruebe que el sistema tiene instalados los dos paquetes de software de requisitos previos (Docker Engine y Python 3).
- Asegúrese de tener privilegios de usuario raíz en el sistema Linux.
- Si utiliza un proxy y está realizando intercepción TLS, deberá conocer la ruta en el sistema Data Sense Linux donde están almacenados los certificados de CA TLS.
- Compruebe que su entorno sin conexión cumple con las necesidades permisos y conectividad.

Pasos

1. Descargue el software Cloud Data Sense del "Sitio de soporte de NetApp". El archivo que debe seleccionar se denomina **DATASENSE-INSTALLER-<version>.tar.gz**.
2. Copie el archivo del instalador en el host Linux que tiene previsto utilizar (mediante `scp` o algún otro método).
3. En BlueXP, seleccione **Gobierno > Clasificación**.
4. Haga clic en **Activar detección de datos**.



5. En función de si está implementando una instancia en la nube o una instancia en sus instalaciones, haga clic en el botón **Deploy** correspondiente para iniciar el asistente de implementación de Data Sense.



6. Aparece el cuadro de diálogo *Deploy Data Sense on local*. Copie el comando proporcionado y péguelo en un archivo de texto para poder usarlo más tarde y haga clic en **Cerrar**. Por ejemplo:

```
sudo ./install.sh -a 12345 -c 27AG75 -t 2198qq
```

7. Descomprima el archivo del instalador en el equipo host; por ejemplo:

```
tar -xzf DATASENSE-INSTALLER-V1.21.0.tar.gz
```

8. Cuando el instalador lo solicite, puede introducir los valores necesarios en una serie de mensajes o puede proporcionar los parámetros necesarios como argumentos de línea de comandos al instalador.

   Tenga en cuenta que el instalador realiza una comprobación previa para asegurarse de que el sistema y los requisitos de red están en su lugar para una instalación correcta.

Introduzca los parámetros según se le solicite:	Introduzca el comando Full:
a. Pegue la información que ha copiado del paso 6: `sudo ./install.sh -a <account_id> -c <agent_id> -t <token>` b. Introduzca la dirección IP o el nombre de host del equipo host de Data Sense para que pueda accederse a él mediante la instancia de Connector. c. Introduzca la dirección IP o el nombre de host de la máquina host de BlueXP Connector para que pueda accederse a ella mediante la instancia de detección de datos. d. Introduzca los detalles del proxy según se le solicite. Si su conector BlueXP ya utiliza un proxy, no es necesario volver a introducir esta información ya que detección de datos utilizará automáticamente el proxy utilizado por el conector.	También puede crear el comando completo por adelantado, proporcionando los parámetros de host y proxy necesarios: `sudo ./install.sh -a <account_id> -c <agent_id> -t <token> --host <ds_host> --manager-host <cm_host> --proxy-host <proxy_host> --proxy-port <proxy_port> --proxy-scheme <proxy_scheme> --proxy -user <proxy_user> --proxy-password <proxy_password> --cacert-folder-path <ca_cert_dir>`

   Valores de variable:

   - *account_id* = ID de cuenta de NetApp
   - *Agent_id* = ID del conector
   - *token* = token de usuario jwt
   - *DS_host* = dirección IP o nombre de host del sistema Data Sense Linux.
   - *Cm_host* = dirección IP o nombre de host del sistema BlueXP Connector.
   - *proxy_host* = IP o nombre de host del servidor proxy si el host está detrás de un servidor proxy.
   - *proxy_Port* = Puerto para conectarse al servidor proxy (predeterminado 80).
   - *Proxy_Scheme* = combinación de conexiones: https o http (valor predeterminado http).
   - *proxy_USER* = Usuario autenticado para conectarse al servidor proxy, si se requiere autenticación básica.
   - *proxy_password* = Contraseña del nombre de usuario especificado.
   - *CA_cert_dir* = Ruta en el sistema Data Sense Linux que contiene paquetes de certificados de CA TLS adicionales. Sólo es necesario si el proxy está realizando intercepción TLS.

Resultado

El instalador de Cloud Data Sense instala paquetes, registra la instalación e instala Data Sense. La instalación puede tardar entre 10 y 20 minutos.

Si hay conectividad sobre el puerto 8080 entre el equipo host y la instancia de conector, verá el progreso de instalación en la ficha detección de datos de BlueXP.

El futuro

En la página Configuración puede seleccionar los orígenes de datos que desea analizar.

También puede hacerlo "Configure la licencia de Cloud Data Sense" en este momento. No se le cobrará hasta que finalice su prueba gratuita de 30 días.

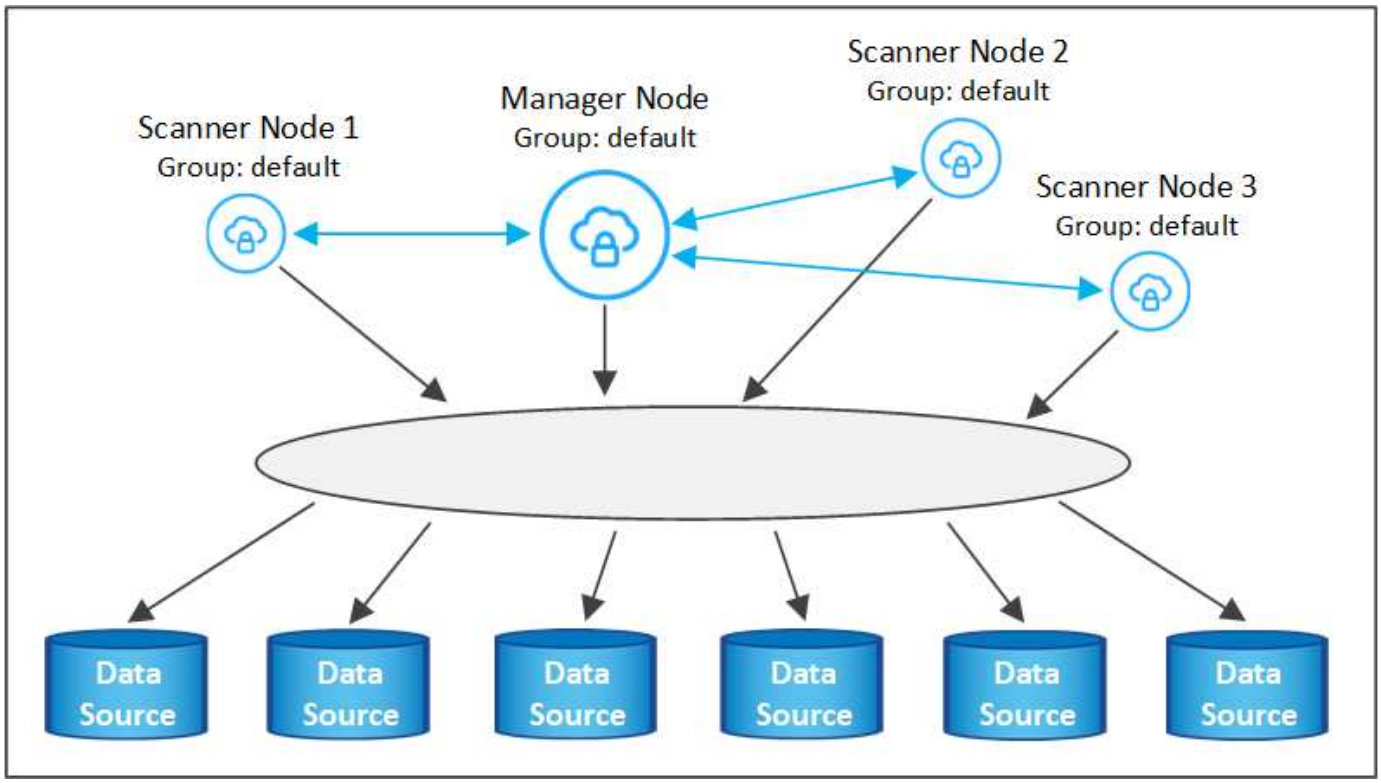
Agregar nodos de escáner a una implementación existente

Puede añadir más nodos de escáner si necesita más potencia de procesamiento de escaneado para analizar sus orígenes de datos. Puede añadir los nodos del escáner inmediatamente después de instalar el nodo Manager, o bien puede añadir un nodo de escáner más adelante. Por ejemplo, si se da cuenta de que la cantidad de datos de uno de sus orígenes de datos se ha duplicado o triplicado en tamaño después de 6 meses, puede añadir un nuevo nodo de escáner para ayudar con el análisis de datos.

Existen dos formas de añadir nodos de escáner adicionales:

- agregue un nodo para ayudarle a analizar todos los orígenes de datos
- agregar un nodo para ayudarle a escanear un origen de datos específico o un grupo específico de orígenes de datos (normalmente basado en la ubicación)

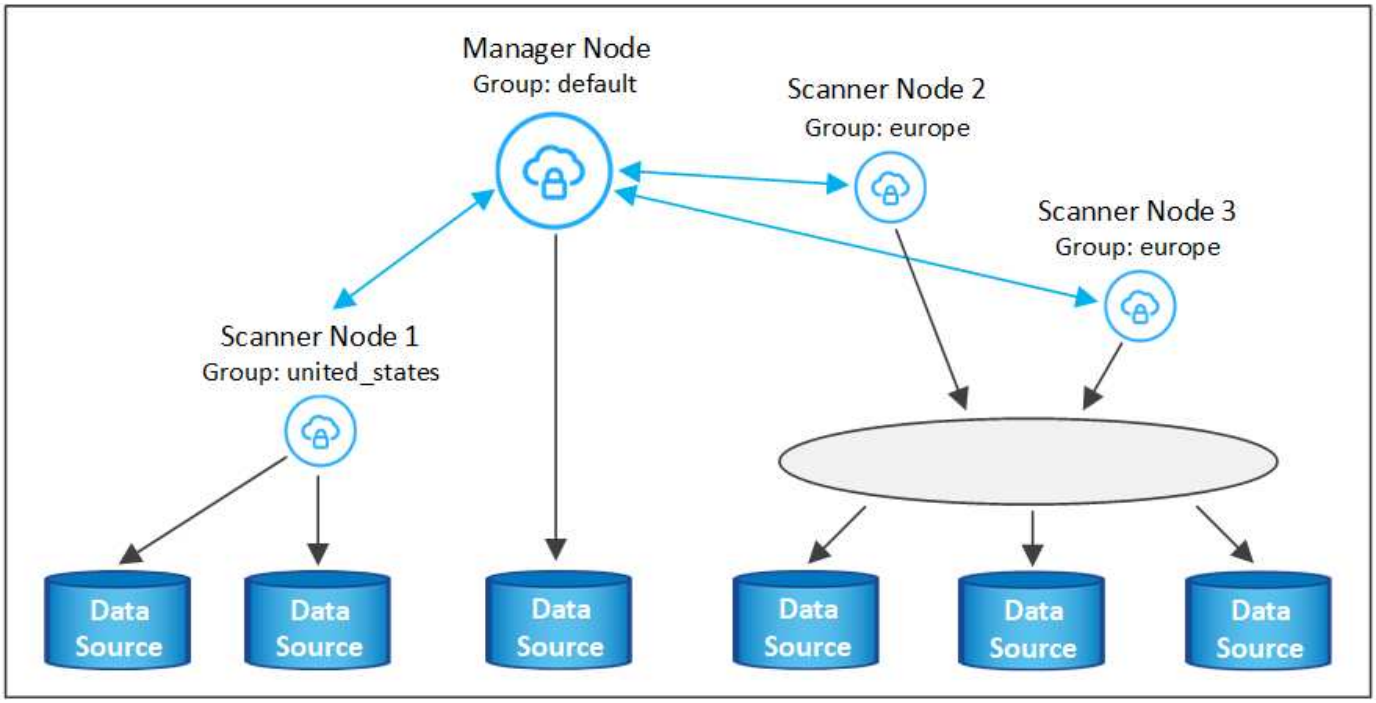
De forma predeterminada, los nuevos nodos de escáner que agregue se agregarán al pool general de recursos de digitalización. Esto se denomina "grupo de escáner predeterminado". En la siguiente imagen, hay 1 nodo de administrador y 3 nodos de escáner en el grupo "predeterminado" que están analizando todos los datos de los 6 orígenes de datos.



Si tiene ciertos orígenes de datos que desea analizar mediante nodos de escáner que están físicamente más cercanos a los orígenes de datos, puede definir un nodo de escáner o un grupo de nodos de escáner, para analizar un origen de datos específico o un grupo de orígenes de datos. En la siguiente imagen, hay 1 nodo

de administrador y 3 nodos de escáner.

- El nodo Administrador está en el grupo "predeterminado" y está analizando 1 origen de datos
- El nodo 1 del escáner se encuentra en el grupo "estados Unidos" y está analizando 2 orígenes de datos
- Los nodos de escáner 2 y 3 se encuentran en el grupo "europa" y comparten las tareas de escaneo para 3 fuentes de datos



Los grupos de análisis de detección de datos se pueden definir como áreas geográficas independientes en las que se almacenan los datos. Puede implementar varios nodos de escáner de detección de datos en todo el mundo y elegir un grupo de escáner para cada nodo. De esta forma, cada nodo de escáner analizará los datos más cercanos. Cuanto más cerca esté el nodo del escáner de los datos, mejor será porque reduce la latencia de red tanto como sea posible mientras escanea datos.

Puede elegir los grupos de escáneres que desea agregar a Data Sense y elegir sus nombres. El sentido de datos no impone que un nodo asignado a un grupo de escáner llamado "europa" se implemente en Europa.

Siga estos pasos para instalar nodos adicionales del escáner de detección de datos:

1. Prepare los sistemas host Linux que actuarán como nodos del escáner
2. Descargue el software Data Sense en estos sistemas Linux
3. Ejecute un comando en el nodo Administrador para identificar los nodos del escáner
4. Siga los pasos para implementar el software en los nodos del escáner (y para definir opcionalmente un "grupo de escáner" para determinados nodos del escáner)
5. Si ha definido un grupo de escáner, en el nodo Administrador:
    a. Abra el archivo "working_Environment_to_scanner_group_config.yml" y defina los entornos de trabajo que explorarán cada grupo de escáneres
    b. Ejecute la siguiente secuencia de comandos para registrar esta información de asignación en todos los nodos del escáner: `update_we_scanner_group_from_config_file.sh`

Lo que necesitará

- Compruebe que todos los sistemas Linux para los nodos del escáner cumplen con el requisitos del host.
- Compruebe que los sistemas tienen instalados los dos paquetes de software de requisitos previos (Docker Engine y Python 3).
- Asegúrese de tener privilegios de usuario raíz en los sistemas Linux.
- Compruebe que su entorno cumple con las necesidades permisos y conectividad.
- Debe tener las direcciones IP de los hosts del nodo Scanner que desea añadir.
- Debe tener la dirección IP del sistema host del nodo Data Sense Manager
- Debe tener la dirección IP o el nombre de host del sistema Connector, su ID de cuenta de NetApp, su identificador de cliente conector y el token de acceso de usuario. Si tiene previsto utilizar grupos de escáner, deberá conocer el identificador de entorno de trabajo de cada origen de datos de su cuenta. Consulte los pasos ***Prerrequisito*** siguientes para obtener esta información.
- Deben habilitarse los siguientes puertos y protocolos en todos los hosts:

Puerto	Protocolos	Descripción
2377	TCP	Comunicaciones de gestión de clústeres
7946	TCP, UDP	Comunicación entre nodos
4789	UDP	Superpone el tráfico de red
50	ESP	Tráfico de red de superposición (ESP) IPsec cifrada
111	TCP, UDP	Servidor NFS para compartir archivos entre los hosts (necesario de cada nodo de escáner al nodo de administración)
2049	TCP, UDP	Servidor NFS para compartir archivos entre los hosts (necesario de cada nodo de escáner al nodo de administración)

- Si está utilizando `firewalld` En sus máquinas de Data Sense, le recomendamos que la habilite antes de instalar Data Sense. Ejecute los siguientes comandos para configurar `firewalld` Para que sea compatible con Data Sense:

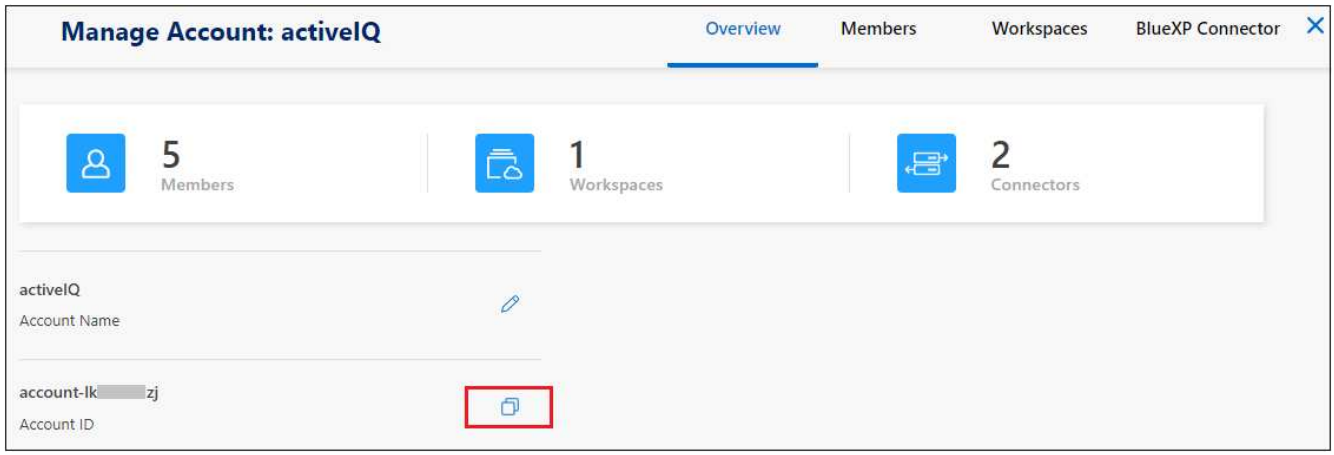
```
firewall-cmd --permanent --add-service=http
firewall-cmd --permanent --add-service=https
firewall-cmd --permanent --add-port=80/tcp
firewall-cmd --permanent --add-port=8080/tcp
firewall-cmd --permanent --add-port=443/tcp
firewall-cmd --permanent --add-port=2377/tcp
firewall-cmd --permanent --add-port=7946/udp
firewall-cmd --permanent --add-port=7946/tcp
firewall-cmd --permanent --add-port=4789/udp
firewall-cmd --reload
```

  Si activa `firewalld` Después de instalar Data Sense, debe reiniciar docker.

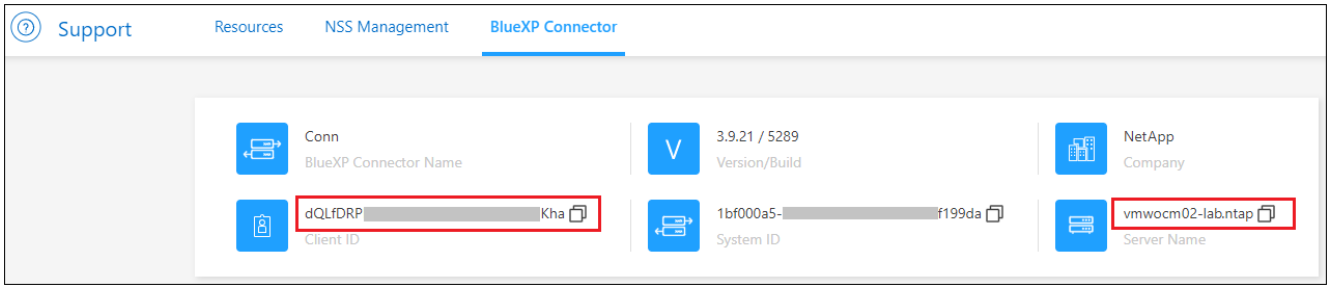
Requisitos previos

Siga estos pasos para obtener el identificador de cuenta de NetApp, el identificador de cliente del conector, el nombre de servidor del conector y el token de acceso de usuario necesarios para añadir nodos de escáner.

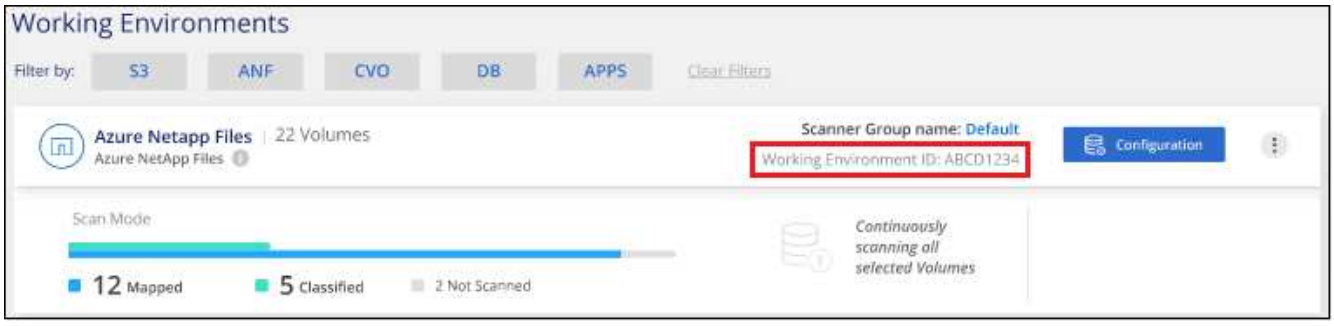
1. En la barra de menús de BlueXP, haga clic en **cuenta > Administrar cuentas**.



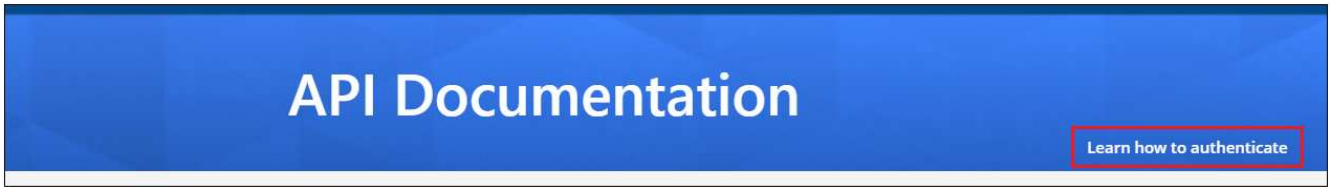
2. Copie el *ID de cuenta*.
3. En la barra de menús de BlueXP, haga clic en **Ayuda > Soporte > conector BlueXP**.



4. Copie el conector *Client ID* y el *Server Name*.
5. Si tiene previsto utilizar grupos de escáneres, en la ficha Configuración de detección de datos , copie el identificador de entorno de trabajo de cada entorno de trabajo que desee agregar a un grupo de escáneres.



6. Vaya a la "Centro de desarrollo de documentación de API" Y haga clic en **aprender a autenticar**.



7. Siga las instrucciones de autenticación y copie el *access token* de la respuesta.

Pasos

1. En el nodo de Data Sense Manager, ejecute el script "add_scanner_node.sh". Por ejemplo, este comando añade 2 nodos de escáner:

   ```
   sudo ./add_scanner_node.sh -a <account_id> -c <client_id> -m <cm_host> -h
   <ds_manager_ip> -n <node_private_ip_1,node_private_ip_2> -t <user_token>
   ```

   Valores de variable:

   - *account_id* = ID de cuenta de NetApp
   - *Client_id* = ID de cliente del conector
   - *Cm_host* = dirección IP o nombre de host del sistema conector
   - *DS_Manager_ip* = Dirección IP privada del sistema de nodos de Data Sense Manager
   - *Node_Private_ip* = direcciones IP de los sistemas de nodos del escáner de detección de datos (varias IP de nodos del escáner están separadas por una coma)
   - *USER_token* = token de acceso de usuario JWT

2. Antes de que finalice la secuencia de comandos add_scanner_node, aparecerá un cuadro de diálogo con el comando de instalación necesario para los nodos del escáner. Copie el comando y guárdelo en un archivo de texto. Por ejemplo:

   ```
   sudo ./node_install.sh -m 10.11.12.13 -t ABCDEF1s35212 -u red95467j
   ```

3. En el host **cada nodo del escáner**:

   a. Copie el archivo de instalación de Data Sense (**DATASENSE-INSTALLER-<version>.tar.gz**) en el equipo host (usando `scp` o algún otro método).

   b. Descomprima el archivo del instalador.

   c. Pegue y ejecute el comando que copió en el paso 2.

   d. Si desea agregar un nodo de escáner a un "grupo de escáner", agregue el parámetro **-r <scanner_group_name>** al comando. De lo contrario, el nodo del escáner se agrega al grupo "predeterminado".

      Cuando la instalación termina en todos los nodos del escáner y se han Unido al nodo del administrador, el script "add_scanner_node.sh" también finaliza. La instalación puede tardar entre 10 y 20 minutos.

4. Si ha agregado algún nodo de escáner a un grupo de escáner, vuelva al nodo Administrador y realice las dos tareas siguientes:

   a. Abra el archivo "/opt/netapp/Datashense/working_Environment_to_scanner_group_config.yml" e introduzca la asignación para la que los grupos de escáneres exploran entornos de trabajo específicos. Deberá tener el *ID de entorno de trabajo* para cada origen de datos. Por ejemplo, las siguientes entradas agregan 2 entornos de trabajo al grupo de escáneres "europa" y 2 al grupo de escáneres "estados Unidos":

```
scanner_groups:
 europe:
   working_environments:
     - "working_environment_id1"
     - "working_environment_id2"
 united_states:
   working_environments:
     - "working_environment_id3"
     - "working_environment_id4"
```

El grupo "predeterminado" analiza cualquier entorno de trabajo que no se agregue a la lista; debe tener al menos un nodo de administrador o escáner en el grupo "predeterminado".

b. Ejecute la siguiente secuencia de comandos para registrar esta información de asignación en todos los nodos del escáner:
`/opt/netapp/Datasense/tools/update_we_scanner_group_from_config_file.sh`

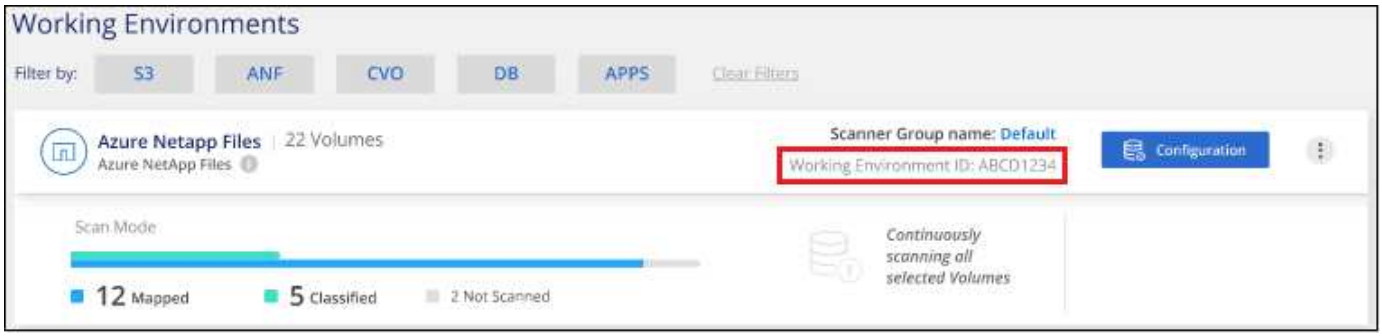
Resultado

Data Sense se configura con los nodos Manager y Scanner para analizar todos sus orígenes de datos.

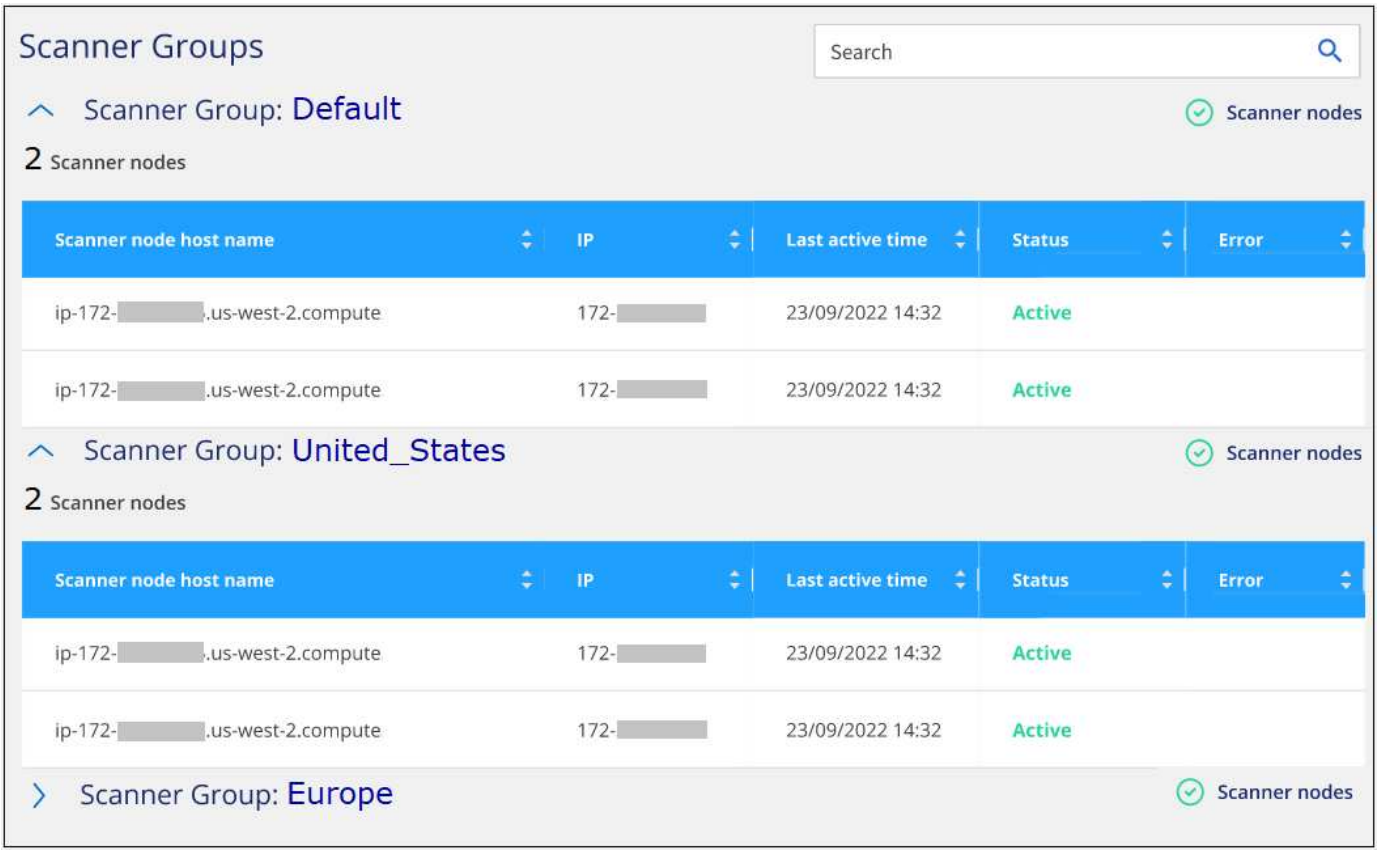
El futuro

En la página Configuración puede seleccionar los orígenes de datos que desea analizar, si aún no lo ha hecho. Si ha creado grupos de escáner, los nodos de escáner del grupo correspondiente escanean cada origen de datos.

Puede ver el nombre del grupo de escáneres de cada entorno de trabajo en la página Configuración.



También puede ver la lista de todos los grupos de escáneres junto con la dirección IP y el estado de cada nodo de escáner del grupo en la parte inferior de la página Configuración.



Puede hacerlo "Configure la licencia de Cloud Data Sense" en este momento. No se le cobrará hasta que finalice su prueba gratuita de 30 días.

Instalación de varios hosts para configuraciones grandes

En configuraciones de gran tamaño en las que va a escanear petabytes de datos, puede incluir varios hosts para proporcionar una capacidad de procesamiento adicional. Cuando se utilizan varios sistemas host, el sistema principal se denomina *Manager node* y los sistemas adicionales que proporcionan potencia de procesamiento adicional se denominan *Scanner Nodes*.

Siga estos pasos cuando instale software Data Sense en varios hosts locales al mismo tiempo. Tenga en cuenta que no puede utilizar "grupos de escáneres" al implementar varios hosts de esta forma.

Lo que necesitará

- Verifique que todos los sistemas Linux para los nodos Manager y Scanner se adapten al requisitos del host.
- Compruebe que los sistemas tienen instalados los dos paquetes de software de requisitos previos (Docker Engine y Python 3).
- Asegúrese de tener privilegios de usuario raíz en los sistemas Linux.
- Compruebe que su entorno cumple con las necesidades permisos y conectividad.
- Debe tener las direcciones IP de los hosts de nodos de escáner que desee utilizar.
- Deben habilitarse los siguientes puertos y protocolos en todos los hosts:

Puerto	Protocolos	Descripción
2377	TCP	Comunicaciones de gestión de clústeres

Puerto	Protocolos	Descripción
7946	TCP, UDP	Comunicación entre nodos
4789	UDP	Superpone el tráfico de red
50	ESP	Tráfico de red de superposición (ESP) IPsec cifrada
111	TCP, UDP	Servidor NFS para compartir archivos entre los hosts (necesario de cada nodo de escáner al nodo de administración)
2049	TCP, UDP	Servidor NFS para compartir archivos entre los hosts (necesario de cada nodo de escáner al nodo de administración)

Pasos

1. Siga los pasos 1 a 7 de la Instalación de un solo host en el nodo de gestión.
2. Como se muestra en el paso 8, cuando el instalador lo solicite, puede introducir los valores necesarios en una serie de peticiones o puede proporcionar los parámetros necesarios como argumentos de línea de comandos al instalador.

   Además de las variables disponibles para una instalación de un solo host, se utiliza una nueva opción **-n <node_ip>** para especificar las direcciones IP de los nodos del escáner. Las varias IP de nodos de escáner están separadas por una coma.

   Por ejemplo, este comando añade 3 nodos de escáner:
   ```
   sudo ./install.sh -a <account_id> -c <agent_id> -t <token> --host <ds_host>
   --manager-host <cm_host> -n <node_ip1>,<node_ip2>,<node_ip3> --proxy-host
   <proxy_host> --proxy-port <proxy_port> --proxy-scheme <proxy_scheme> --proxy
   -user <proxy_user> --proxy-password <proxy_password>
   ```
3. Antes de que se complete la instalación del nodo de gestión, se mostrará un cuadro de diálogo con el comando de instalación necesario para los nodos del escáner. Copie el comando y guárdelo en un archivo de texto. Por ejemplo:

   ```
   sudo ./node_install.sh -m 10.11.12.13 -t ABCDEF-1-3u69m1-1s35212
   ```
4. En el host **cada nodo del escáner**:
   a. Copie el archivo de instalación de Data Sense (**DATASENSE-INSTALLER-<version>.tar.gz**) en el equipo host (usando `scp` o algún otro método).
   b. Descomprima el archivo del instalador.
   c. Pegue y ejecute el comando que copió en el paso 3.

      Cuando la instalación finalice en todos los nodos de escáner y se han Unido al nodo de gestión, también se completa la instalación del nodo de gestión.

Resultado

El instalador de Cloud Data Sense finaliza la instalación de los paquetes y registra la instalación. La instalación puede tardar entre 10 y 20 minutos.

El futuro

En la página Configuración puede seleccionar los orígenes de datos que desea analizar.

También puede hacerlo "Configure la licencia de Cloud Data Sense" en este momento. No se le cobrará hasta que finalice su prueba gratuita de 30 días.

Implemente Cloud Data Sense en un host sin acceso a Internet

Complete unos pasos para poner en marcha Cloud Data Sense en un host en un sitio local que no tiene acceso a Internet. Este tipo de instalación es perfecta para sus sitios seguros.

Tenga en cuenta que también puede "Ponga en marcha el sentido de los datos en un sitio local con acceso a Internet".

Orígenes de datos compatibles

Cuando se instala de esta manera (a veces denominado sitio "sin conexión" o "oscuro"), Data Sense solo puede analizar datos de orígenes de datos que también son locales del sitio local. En este momento, Data Sense puede analizar las siguientes fuentes de datos **locales**:

- Sistemas ONTAP en las instalaciones
- Esquemas de base de datos
- Cuentas locales de SharePoint (SharePoint Server)
- Recursos compartidos de archivos NFS o CIFS de terceros
- Almacenamiento de objetos que utiliza el protocolo simple Storage Service (S3)

En situaciones especiales en las que necesita una instalación BlueXP muy segura, pero también desea analizar datos locales de cuentas de OneDrive o de cuentas de SharePoint Online, puede utilizar el instalador sin conexión de Data Sense y proporcionar acceso a Internet a unos pocos extremos seleccionados. Consulte Requisitos especiales para SharePoint y OneDrive para obtener más detalles.

Actualmente no hay compatibilidad para escanear cuentas Cloud Volumes ONTAP, Azure NetApp Files, FSX para ONTAP, AWS S3 o Google Drive cuando Data Sense se implementa en un sitio oscuro.

Limitaciones

La mayoría de las funciones de detección de datos funcionan cuando se implementa en un sitio sin acceso a Internet. Sin embargo, algunas funciones que requieren acceso a Internet no son compatibles, por ejemplo:

- Administración de etiquetas de Microsoft Azure Information Protection (AIP)
- Envío de alertas por correo electrónico a usuarios de BlueXP cuando determinadas políticas críticas devuelven resultados
- Configuración de funciones de BlueXP para usuarios diferentes (por ejemplo, Administrador de cuentas o Visor de cumplimiento)
- Copiar y sincronizar archivos de origen mediante Cloud Sync
- Recibiendo comentarios de usuarios
- Actualizaciones de software automatizadas desde BlueXP

  Tanto el conector BlueXP como el sensor de datos requerirán actualizaciones manuales periódicas para

habilitar nuevas funciones. Puede ver la versión de Data Sense en la parte inferior de las páginas de la interfaz de usuario de Data Sense. Compruebe la "Notas de la versión de Cloud Data Sense" para ver las nuevas funciones de cada versión y si desea esas funciones. A continuación, puede seguir los pasos a. "Actualice el conector BlueXP" y.. Actualice su software de detección de datos.

Inicio rápido

Empiece rápidamente siguiendo estos pasos o desplácese hacia abajo hasta las secciones restantes para obtener todos los detalles.

Instale el conector BlueXP

Si aún no tiene un conector instalado en su sitio local sin conexión, "Despliegue el conector" Ahora en un host Linux.

Revise los requisitos previos de detección de datos

Compruebe que su sistema Linux cumple con el requisitos del host, que tiene todo el software necesario instalado y que su entorno sin conexión cumple con el necesario permisos y conectividad.

Descargue e implemente Data Sense

Descargue el software Cloud Data Sense del sitio de soporte de NetApp y copie el archivo del instalador en el host Linux que tiene pensado utilizar. A continuación, inicie el asistente de instalación y siga las indicaciones para implementar la instancia de Cloud Data Sense.

Suscríbase al servicio Cloud Data Sense

Los primeros 1 TB de datos que analiza Cloud Data Sense en BlueXP son gratuitos durante 30 días. Se requiere una licencia BYOL de NetApp para continuar con el análisis de los datos después de ese punto.

Instale el conector BlueXP

Si aún no tiene un conector BlueXP instalado en su sitio local fuera de línea, "Despliegue el conector" En un host Linux del sitio sin conexión.

Prepare el sistema host Linux

El software de detección de datos debe ejecutarse en un host que cumpla con requisitos específicos del sistema operativo, requisitos de RAM, requisitos de software, etc. No se admite la detección de datos en un host que se comparte con otras aplicaciones; el host debe ser un host dedicado.

- **Sistema operativo**: Red Hat Enterprise Linux o CentOS versiones 8.0 a 8.7
  - CentOS Stream 8 también es compatible
  - Se pueden utilizar las versiones 7.8 o 7.9, pero la versión de kernel de Linux debe ser 4.0 o posterior
  - El sistema operativo debe ser capaz de instalar Docker Engine
- **Disco**: SSD con 500 GIB disponibles en /, o.

- 100 GIB disponibles en /opt
- 400 GIB disponibles en /var
- 5 GIB en /tmp

- **RAM**: 64 GB (la memoria de intercambio debe estar desactivada en el host)
- **CPU**: 16 núcleos

  Tenga en cuenta que puede implementar la detección de datos en un sistema con menos CPU y menos RAM, pero existen limitaciones al utilizar estos sistemas. Consulte "Con un tipo de instancia más pequeño" para obtener más detalles.

- **Software adicional**: Debe instalar el siguiente software en el host antes de instalar Data Sense:
  - Docker Engine versión 19.3.1 o posterior. "Ver las instrucciones de instalación".
  - Python 3 versión 3.6 o posterior. "Ver las instrucciones de instalación".
- * Consideraciones de Firewalld*: Si usted está planeando utilizar `firewalld`, Le recomendamos que lo habilite antes de instalar Data Sense. Ejecute los siguientes comandos para configurar `firewalld` Para que sea compatible con Data Sense:

```
firewall-cmd --permanent --add-service=http
firewall-cmd --permanent --add-service=https
firewall-cmd --permanent --add-service=mysql
firewall-cmd --permanent --add-port=80/tcp
firewall-cmd --permanent --add-port=8080/tcp
firewall-cmd --permanent --add-port=443/tcp
firewall-cmd --permanent --add-port=555/tcp
firewall-cmd --permanent --add-port=3306/tcp
firewall-cmd --reload
```

  Si activa `firewalld` Después de instalar Data Sense, debe reiniciar docker.

La dirección IP del sistema host Data Sense no se puede cambiar tras la instalación.

Verifique los requisitos previos de BlueXP y Data Sense

Revise los siguientes requisitos previos para asegurarse de que dispone de una configuración compatible antes de implementar Cloud Data Sense.

- Asegúrese de que Connector tiene permisos para implementar recursos y crear grupos de seguridad para la instancia de Cloud Data Sense. Puede encontrar los últimos permisos de BlueXP en "Las políticas proporcionadas por NetApp".
- Asegúrese de que puede mantener en funcionamiento Cloud Data Sense. La instancia de Cloud Data Sense tiene que seguir para poder analizar sus datos de forma continua.
- Garantice la conectividad del navegador web con Cloud Data Sense. Después de habilitar Cloud Data Sense, asegúrese de que los usuarios acceden a la interfaz BlueXP desde un host que tiene una conexión a la instancia de detección de datos.

  La instancia de Data Sense utiliza una dirección IP privada para garantizar que los datos indexados no

sean accesibles para otros. Como resultado, el navegador web que utiliza para acceder a BlueXP debe tener una conexión a esa dirección IP privada. Esta conexión puede provenir de un host que está dentro de la misma red que la instancia de Data Sense.

Verifique que todos los puertos necesarios estén habilitados

Debe asegurarse de que todos los puertos necesarios estén abiertos para la comunicación entre el conector, detección de datos, Active Directory y sus orígenes de datos.

Tipo de conexión	Puertos	Descripción
Conector <> detección de datos	8080 (TCP), 443 (TCP) y 80	El grupo de seguridad del conector debe permitir el tráfico entrante y saliente a través del puerto 443 hacia y desde la instancia de detección de datos. Asegúrese de que el puerto 8080 está abierto para que pueda ver el progreso de la instalación en BlueXP.
Conector <> clúster ONTAP (NAS)	443 (TCP)	BlueXP detecta los clústeres de ONTAP mediante HTTPS. Si utiliza directivas de firewall personalizadas, deben cumplir los siguientes requisitos: • El host del conector debe permitir el acceso HTTPS de salida a través del puerto 443. Si el conector está en la nube, el grupo de seguridad predefinido permite todas las comunicaciones salientes. • El clúster ONTAP debe permitir el acceso HTTPS de entrada a través del puerto 443. La política de firewall "mgmt" predeterminada permite el acceso HTTPS entrante desde todas las direcciones IP. Si ha modificado esta directiva predeterminada o si ha creado su propia directiva de firewall, debe asociar el protocolo HTTPS con esa directiva y habilitar el acceso desde el host de Connector.

Tipo de conexión	Puertos	Descripción
Detección de los datos <> clúster de ONTAP	• Para NFS: 111 (TCP\UDP) y 2049 (TCP\UDP) • Para CIFS: 139 (TCP\UDP) y 445 (TCP\UDP)	Data Sense necesita una conexión de red a cada subred de Cloud Volumes ONTAP o a cada sistema ONTAP en las instalaciones. Los grupos de seguridad para Cloud Volumes ONTAP deben permitir conexiones entrantes desde la instancia de detección de datos. Asegúrese de que estos puertos estén abiertos a la instancia de Data Sense: • Para NFS: 111 y 2049 • Para CIFS - 139 y 445 Las políticas de exportación de volúmenes NFS deben permitir el acceso desde la instancia de Data Sense.
Sentido de los datos <> Active Directory	389 (TCP Y UDP), 636 (TCP), 3268 (TCP) Y 3269 (TCP)	Debe tener un Active Directory ya configurado para los usuarios de su empresa. Además, Data Sense necesita credenciales de Active Directory para analizar volúmenes CIFS. Debe tener la información de Active Directory: • DNS Server IP Address o varias direcciones IP • Nombre de usuario y contraseña para el servidor • Nombre de dominio (nombre de Active Directory) • Si utiliza o no un LDAP seguro (LDAPS) • Puerto de servidor LDAP (normalmente 389 para LDAP y 636 para LDAP seguro)

Si utiliza varios hosts de detección de datos para proporcionar potencia de procesamiento adicional para analizar sus fuentes de datos, tendrá que habilitar puertos y protocolos adicionales. "Consulte los requisitos de puerto adicionales".

Requisitos especiales para SharePoint y OneDrive

Cuando se implementa BlueXP y Data Sense en un sitio sin acceso a Internet, puede analizar archivos en cuentas de SharePoint Online y OneDrive proporcionando acceso a Internet a unos pocos extremos seleccionados.

Las cuentas locales de SharePoint instaladas localmente se pueden analizar sin proporcionar acceso a Internet.

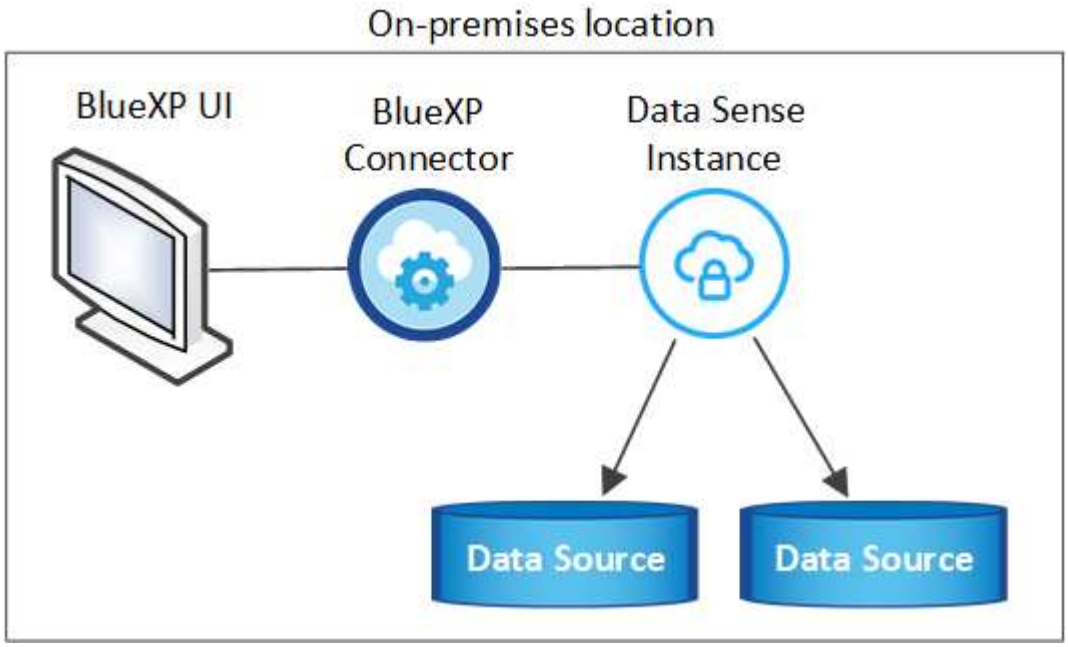
Puntos finales	Específico
\login.microsoft.com \graph.microsoft.com	Comunicación con los servidores de Microsoft para iniciar sesión en el servicio en línea seleccionado.

Puntos finales	Específico
https://api.bluexp.netapp.com	Comunicación con el servicio BlueXP, que incluye cuentas de NetApp.

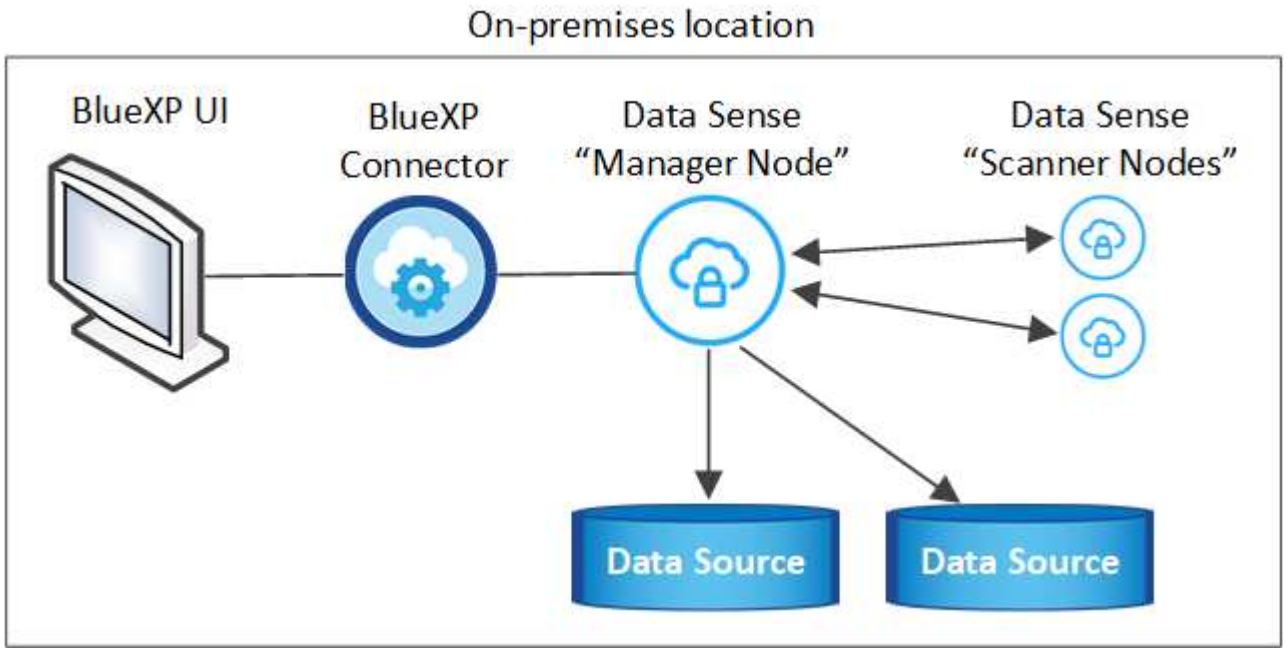
Sólo se requiere acceso a *api.bluexp.netapp.com* durante las conexiones iniciales con estos servicios externos.

Ponga en marcha Data Sense

En configuraciones típicas, instalará el software en un único sistema host. "Consulte estos pasos aquí".



En configuraciones de gran tamaño en las que va a escanear petabytes de datos, puede incluir varios hosts para proporcionar una capacidad de procesamiento adicional. "Consulte estos pasos aquí".



Instalación de un solo host para configuraciones típicas

Siga estos pasos al instalar el software Data Sense en un solo host local en un entorno sin conexión.

Lo que necesitará

- Compruebe que su sistema Linux cumple con el requisitos del host.
- Compruebe que ha instalado los dos paquetes de software de requisitos previos (Docker Engine y Python 3).
- Asegúrese de tener privilegios de usuario raíz en el sistema Linux.
- Compruebe que su entorno sin conexión cumple con las necesidades permisos y conectividad.

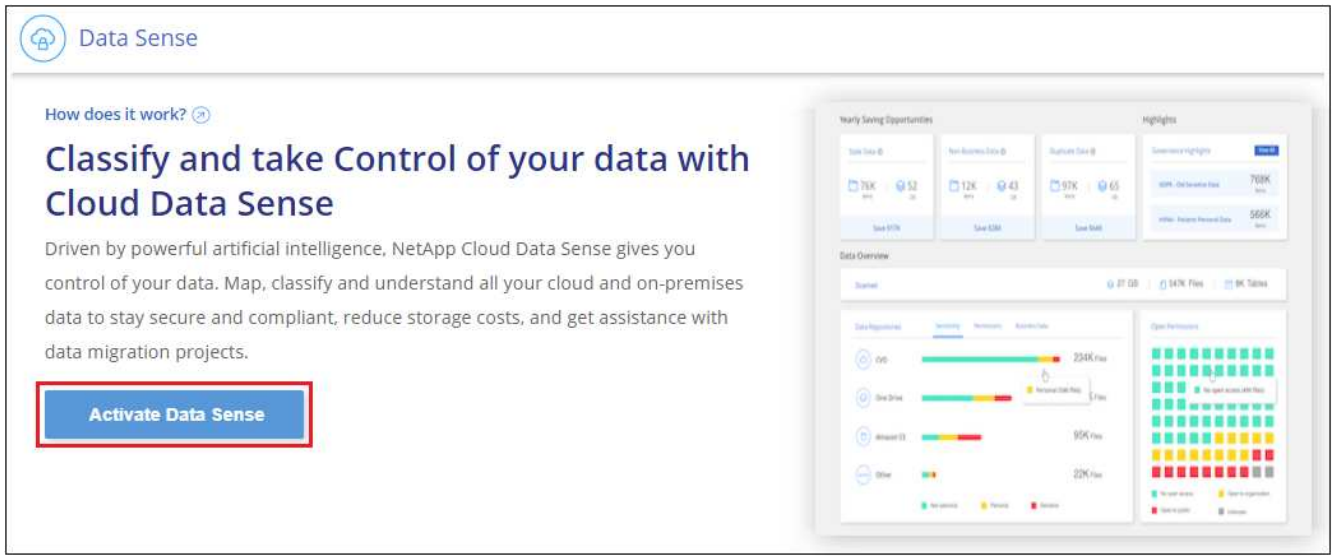
Pasos

1. En un sistema configurado en Internet, descargue el software Cloud Data Sense del "Sitio de soporte de NetApp". El archivo que debe seleccionar se llama **DataSense-offline-Bundle-<version>.tar.gz**.
2. Copie el paquete de instalador en el host Linux que planea utilizar en el sitio oscuro.
3. Descomprima el paquete del instalador en el equipo host; por ejemplo:

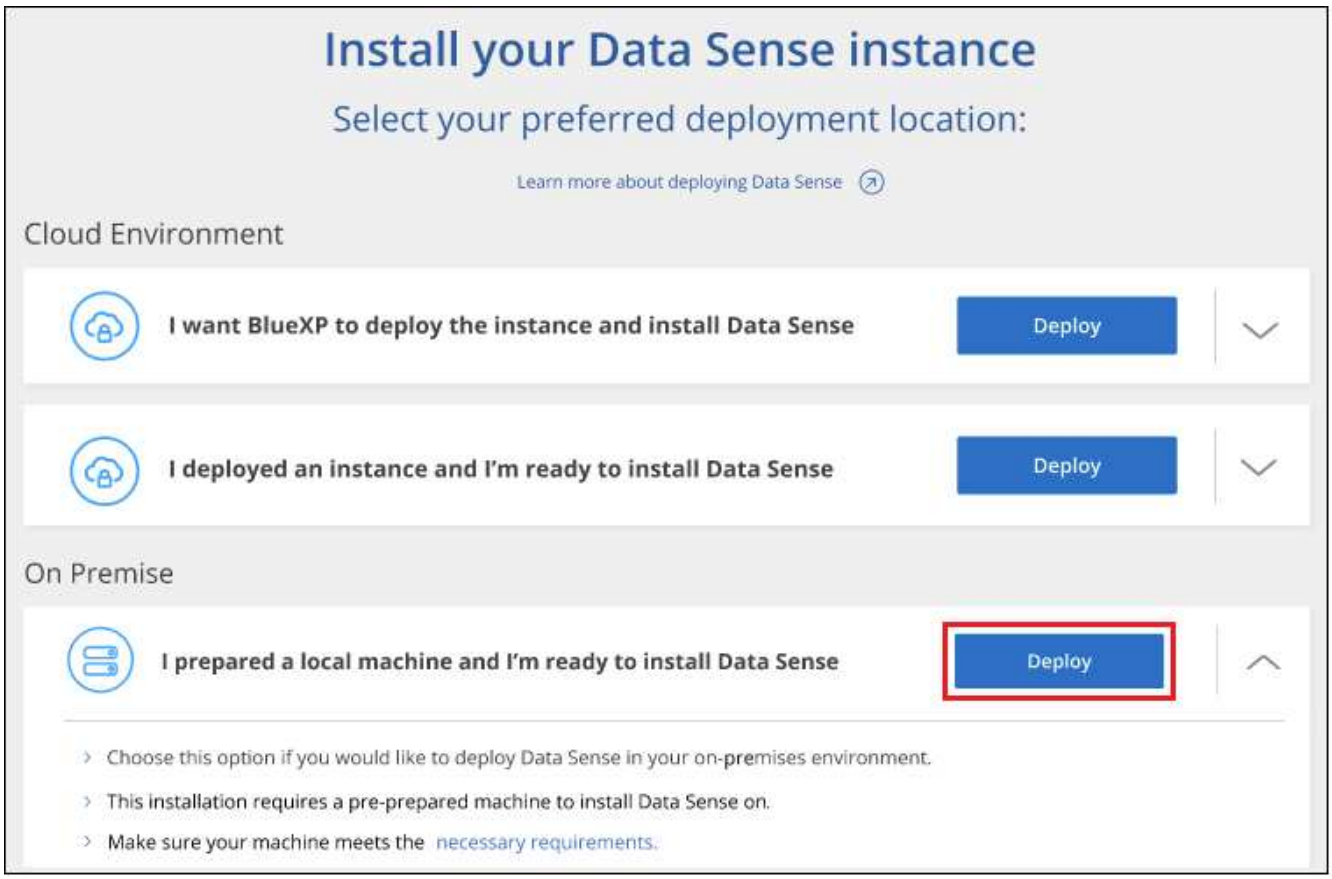
   ```
   tar -xzf DataSense-offline-bundle-v1.21.0.tar.gz
   ```

   Esto extrae el software requerido y el archivo de instalación actual **cc_onprem_installer.tar.gz**.

4. Inicie BlueXP y seleccione **Gobierno > Clasificación**.
5. Haga clic en **Activar detección de datos**.



6. Haga clic en **desplegar** para iniciar el asistente de implementación en las instalaciones.



7. Aparece el cuadro de diálogo *Deploy Data Sense on local*. Copie el comando proporcionado y péguelo en un archivo de texto para poder usarlo más tarde y haga clic en **Cerrar**. Por ejemplo:

   ```
   sudo ./install.sh -a 12345 -c 27AG75 -t 2198qq --darksite
   ```

8. Descomprima el archivo de instalación en el equipo host; por ejemplo:

   ```
   tar -xzf cc_onprem_installer.tar.gz
   ```

9. Cuando el instalador lo solicite, puede introducir los valores necesarios en una serie de mensajes o puede proporcionar los parámetros necesarios como argumentos de línea de comandos al instalador:

   Tenga en cuenta que el instalador realiza una comprobación previa para asegurarse de que el sistema y los requisitos de red están en su lugar para una instalación correcta.

Introduzca los parámetros según se le solicite:	Introduzca el comando Full:
a. Pegue la información que ha copiado del paso 7: `sudo ./install.sh -a <account_id> -c <agent_id> -t <token> --darksite` b. Introduzca la dirección IP o el nombre de host del equipo host de Data Sense para que pueda accederse a él mediante la instancia de Connector. c. Introduzca la dirección IP o el nombre de host de la máquina host de BlueXP Connector para que pueda accederse a ella mediante la instancia de detección de datos.	También puede crear el comando completo por adelantado, proporcionando los parámetros de host necesarios: `sudo ./install.sh -a <account_id> -c <agent_id> -t <token> --host <ds_host> --manager-host <cm_host> --no-proxy --darksite`

Valores de variable:

- *account_id* = ID de cuenta de NetApp
- *Agent_id* = ID del conector
- *token* = token de usuario jwt
- *DS_host* = dirección IP o nombre de host del sistema Data Sense Linux.
- *Cm_host* = dirección IP o nombre de host del sistema BlueXP Connector.

Resultado

El instalador de Data Sense instala paquetes, registra la instalación e instala Data Sense. La instalación puede tardar entre 10 y 20 minutos.

Si hay conectividad sobre el puerto 8080 entre el equipo host y la instancia de conector, verá el progreso de instalación en la ficha detección de datos de BlueXP.

El futuro

En la página Configuration puede seleccionar el local "Clústeres de ONTAP en las instalaciones" y.. "oracle" que desea escanear.

También puede hacerlo "Configure las licencias BYOL para Cloud Data Sense" Desde la página de cartera digital en este momento. No se le cobrará hasta que finalice su prueba gratuita de 30 días.

Instalación de varios hosts para configuraciones grandes

En configuraciones de gran tamaño en las que va a escanear petabytes de datos, puede incluir varios hosts para proporcionar una capacidad de procesamiento adicional. Cuando se utilizan varios sistemas host, el sistema principal se denomina *Manager node* y los sistemas adicionales que proporcionan potencia de procesamiento adicional se denominan *Scanner Nodes*.

Siga estos pasos cuando instale software Data Sense en varios hosts locales en un entorno sin conexión.

Lo que necesitará

- Verifique que todos los sistemas Linux para los nodos Manager y Scanner se adapten al requisitos del host.

- Compruebe que ha instalado los dos paquetes de software de requisitos previos (Docker Engine y Python 3).
- Asegúrese de tener privilegios de usuario raíz en los sistemas Linux.
- Compruebe que su entorno sin conexión cumple con las necesidades permisos y conectividad.
- Debe tener las direcciones IP de los hosts de nodos de escáner que desee utilizar.
- Deben habilitarse los siguientes puertos y protocolos en todos los hosts:

Puerto	Protocolos	Descripción
2377	TCP	Comunicaciones de gestión de clústeres
7946	TCP, UDP	Comunicación entre nodos
4789	UDP	Superpone el tráfico de red
50	ESP	Tráfico de red de superposición (ESP) IPsec cifrada
111	TCP, UDP	Servidor NFS para compartir archivos entre los hosts (necesario de cada nodo de escáner al nodo de administración)
2049	TCP, UDP	Servidor NFS para compartir archivos entre los hosts (necesario de cada nodo de escáner al nodo de administración)

Pasos

1. Siga los pasos 1 a 8 de la "Instalación de un solo host" en el nodo de gestión.
2. Como se muestra en el paso 9, cuando el instalador lo solicite, puede introducir los valores necesarios en una serie de peticiones o puede proporcionar los parámetros necesarios como argumentos de línea de comandos al instalador.

   Además de las variables disponibles para una instalación de un solo host, se utiliza una nueva opción **-n <node_ip>** para especificar las direcciones IP de los nodos del escáner. Las IP de varios nodos están separadas por una coma.

   Por ejemplo, este comando añade 3 nodos de escáner:
   ```
   sudo ./install.sh -a <account_id> -c <agent_id> -t <token> --host <ds_host>
   --manager-host <cm_host> -n <node_ip1>,<node_ip2>,<node_ip3> --no-proxy
   --darksite
   ```
3. Antes de que se complete la instalación del nodo de gestión, se mostrará un cuadro de diálogo con el comando de instalación necesario para los nodos del escáner. Copie el comando y guárdelo en un archivo de texto. Por ejemplo:

   ```
   sudo ./node_install.sh -m 10.11.12.13 -t ABCDEF-1-3u69m1-1s35212
   ```
4. En el host **cada nodo del escáner**:
   a. Copie el archivo de instalación de Data Sense (**cc_onprem_installer.tar.gz**) en el equipo host.
   b. Descomprima el archivo del instalador.
   c. Pegue y ejecute el comando que copió en el paso 3.

      Cuando la instalación finalice en todos los nodos de escáner y se han Unido al nodo de gestión, también se completa la instalación del nodo de gestión.

Resultado

El instalador de Cloud Data Sense finaliza la instalación de los paquetes y registra la instalación. La instalación puede tardar entre 15 y 25 minutos.

El futuro

En la página Configuration puede seleccionar el local "Clústeres de ONTAP en las instalaciones" y local "oracle" que desea escanear.

También puede hacerlo "Configure las licencias BYOL para Cloud Data Sense" Desde la página de cartera digital en este momento. No se le cobrará hasta que finalice su prueba gratuita de 30 días.

Actualice el software de detección de datos

Dado que el software Data Sense se actualiza regularmente con las nuevas funciones, debe entrar en una rutina para comprobar si hay nuevas versiones periódicamente para asegurarse de que está utilizando el software y las funciones más recientes. Deberá actualizar el software Data Sense manualmente porque no hay conectividad a Internet para realizar la actualización automáticamente.

Antes de empezar

- El software de detección de datos puede actualizarse una versión principal cada vez. Por ejemplo, si tiene instalada la versión 1.18.x, sólo podrá actualizar a 1.19.x. Si tiene varias versiones principales detrás, tendrá que actualizar el software varias veces.
- Compruebe que el software del conector en las instalaciones se ha actualizado a la versión más reciente disponible. "Consulte los pasos de actualización del conector".

Pasos

1. En un sistema configurado en Internet, descargue el software Cloud Data Sense del "Sitio de soporte de NetApp". El archivo que debe seleccionar se llama **DataSense-offline-Bundle-<version>.tar.gz**.
2. Copie el paquete de software en el host Linux en el que se instaló Data Sense en el sitio oscuro.
3. Descomprima el paquete de software en el equipo host; por ejemplo:

   ```
   tar -xvf DataSense-offline-bundle-v1.21.0.tar.gz
   ```

   Esto extrae el archivo de instalación **cc_onprem_installer.tar.gz**.

4. Descomprima el archivo de instalación en el equipo host; por ejemplo:

   ```
   tar -xzf cc_onprem_installer.tar.gz
   ```

   Esto extrae la secuencia de comandos de actualización **start_darksite_upgrade.sh** y cualquier software de terceros requerido.

5. Ejecute el script de actualización en el equipo host, por ejemplo:

   ```
   start_darksite_upgrade.sh
   ```

Resultado

El software Data Sense se actualiza en el host. La actualización puede tardar entre 5 y 10 minutos.

Tenga en cuenta que no es necesaria ninguna actualización en los nodos de escáner si ha implementado Data Sense en varios sistemas host para analizar configuraciones muy grandes.

Puede verificar que el software se ha actualizado comprobando la versión en la parte inferior de las páginas de la interfaz de usuario de detección de datos.

Información de copyright

Información de la marca comercial