Referencia

BlueXP classification

NetApp
April 03, 2024

Tabla de contenidos

Referencia

Tipos de instancia de clasificación de BlueXP admitidos

El software de clasificación de BlueXP debe ejecutarse en un host que cumpla con los requisitos específicos del sistema operativo, los requisitos de RAM, los requisitos de software, etc. Al poner en marcha la clasificación de BlueXP en el cloud, le recomendamos que utilice un sistema con las características «grandes» para disfrutar de todas las funciones.

Puedes poner en marcha la clasificación de BlueXP en un sistema con menos CPU y menos RAM, pero existen algunas limitaciones al usar estos sistemas menos potentes. "Obtenga información sobre estas limitaciones".

En las siguientes tablas, si el sistema marcado como «predeterminado» no está disponible en la región donde instalas la clasificación de BlueXP, se implementará el siguiente sistema de la tabla.

Tipos de instancia de AWS

Tamaño del sistema	Especificaciones	Tipo de instancia
Extra grande	32 CPU, 128 GB de RAM, 1 TiB GP3 SSD	"m6i.8xlarge" (predeterminado)
Grande	16 CPU, 64 GB de RAM, 500 GIB de SSD	"m6i.4xgrande" (por defecto) m6a.4xlarge m5a.4xlarge m5.4xlarge m4.4xlarge
Mediano	8 CPU, 32 GB de RAM, 200 GIB de SSD	"m6i.2xgrande" (por defecto) m6a.2xlarge m5a.2xlarge m5.2xlarge m4.2xlarge
Pequeño	8 CPU, 16 GB de RAM, 100 GIB de SSD	"cera.2xlarge" (predeterminado) c5a.2xgrande c5.2xgrande c4.2xgrande

Tipos de instancia de Azure

Tamaño del sistema	Especificaciones	Tipo de instancia
Extra grande	32 CPU, 128 GB de RAM, disco de SO (2.048 GiB, rendimiento mínimo de 250 MB/s) y disco de datos (1 TiB SSD, rendimiento mínimo de 750 MB/s)	"Standard_D32_v3" (predeterminado)
Grande	16 CPU, 64 GB de RAM, 500 GIB de SSD	"Standard_D16s_v3" (predeterminado)

Tipos de instancia de GCP

Tamaño del sistema	Especificaciones	Tipo de instancia
Grande	16 CPU, 64 GB de RAM, 500 GIB de SSD	"n2-estándar-16" (predeterminado) n2d-standard-16 n1-standard-16

Metadatos recogidos de orígenes de datos

La clasificación de BlueXP recopila ciertos metadatos al realizar análisis de clasificación en los datos de tus orígenes de datos y entornos de trabajo. La clasificación de BlueXP puede acceder a la mayoría de los metadatos que necesitamos para clasificar los datos, pero hay algunas fuentes en las que no podemos acceder a los datos que necesitamos.

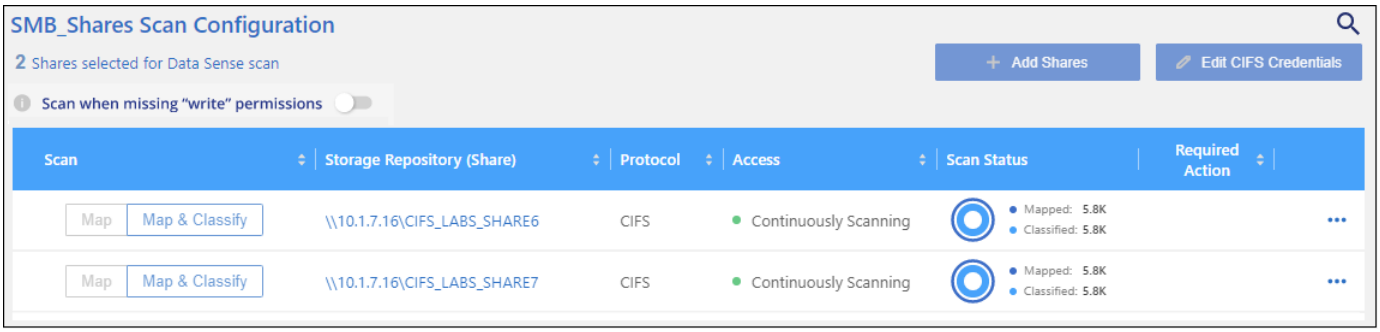
	Metadatos	CIFS	NFS
Sellos de tiempo	*Tiempo de creación*	Disponible	No disponible (no se admite en Linux)
	Hora del último acceso	Disponible	Disponible
	Hora de última modificación	Disponible	Disponible
Permisos	*Permisos abiertos*	Si el grupo "TODOS" tiene acceso al archivo, se considera "abierto a la organización"	Si "otros" tienen acceso al archivo, se considera "abierto a la organización"
	Acceso de usuarios/grupos	La información de usuarios y grupos se toma de LDAP	No disponible (los usuarios NFS suelen gestionarse localmente en el servidor; por tanto, el mismo individuo puede tener un UID diferente en cada servidor)

- La clasificación de BlueXP no extrae el «tiempo de último acceso» de los siguientes orígenes de datos: SharePoint Online, SharePoint on-premises (SharePoint Server), OneDrive, Google Drive y Amazon S3, y bases de datos.
- Las versiones anteriores del sistema operativo Windows (por ejemplo, Windows 7 y Windows 8) desactivan la recopilación del atributo de tiempo de último acceso de forma predeterminada porque puede afectar al rendimiento del sistema. Cuando no se recopila este atributo, se afectará el análisis de clasificación de BlueXP que se basa en el «tiempo de último acceso». Puede habilitar la recopilación de la última hora de acceso en estos sistemas Windows antiguos si es necesario.

Marca de hora del último acceso

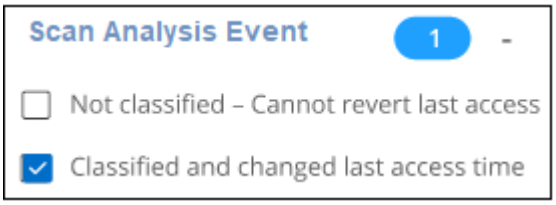
Cuando la clasificación de BlueXP extrae datos de recursos compartidos de archivos, el sistema operativo los considera accediendo a los datos y cambia la «última hora de acceso» conforme a ello. Tras el análisis, la clasificación de BlueXP intenta revertir la hora del último acceso a la marca de tiempo original. Si la clasificación de BlueXP no tiene permisos de atributos de escritura en CIFS, u permisos de escritura en NFS, el sistema no podrá revertir la hora del último acceso a la marca de tiempo original. Los volúmenes ONTAP configurados con SnapLock tienen permisos de solo lectura y además no pueden revertir la última hora de acceso a la marca de tiempo original.

De forma predeterminada, si la clasificación de BlueXP no tiene estos permisos, el sistema no analizará esos archivos en tus volúmenes porque la clasificación de BlueXP no puede revertir la «última hora de acceso» a la marca de tiempo original. Sin embargo, si no le importa si la última hora de acceso se restablece a la hora original en sus archivos, puede hacer clic en el interruptor **Escanear cuando faltan permisos de "atributos de escritura"** en la parte inferior de la página de configuración para que la clasificación de BlueXP escanee los volúmenes independientemente de los permisos.



Esta funcionalidad se puede aplicar a sistemas ONTAP en las instalaciones, Cloud Volumes ONTAP, Azure NetApp Files, FSX para ONTAP y recursos compartidos de archivos no de NetApp.

Tenga en cuenta que hay un filtro en la página de investigación llamado *Scan Analysis Event* que le permite mostrar los archivos que no se clasificaron porque la clasificación de BlueXP no pudo revertir la última hora a la que se accedió. O los archivos que estaban clasificados aunque la clasificación de BlueXP no pudieron revertir la última hora de acceso.



Las selecciones de filtro son:

- "No clasificado — no se puede revertir el tiempo del último acceso" - muestra los archivos que no se han clasificado debido a que faltan permisos de escritura.
- «Hora de último acceso clasificada y actualizada»: Muestra los archivos clasificados y la clasificación de BlueXP no pudo restablecer la fecha original de último acceso. Este filtro sólo es relevante para entornos en los que ha activado **Buscar cuando faltan permisos de "atributos de escritura"**.

Si es necesario, puede exportar estos resultados a un informe para poder ver qué archivos se están analizando o no debido a permisos. "Obtenga más información sobre el informe de investigación de datos".

Inicia sesión en el sistema de clasificación de BlueXP

A veces es posible que tengas que iniciar sesión en el sistema de clasificación de BlueXP para poder acceder a los archivos de registro o editar los archivos de configuración.

Cuando la clasificación de BlueXP está instalada en un equipo Linux en las instalaciones o en un equipo Linux implementado en la nube, puedes acceder al archivo de configuración y al script directamente.

Cuando se pone en marcha la clasificación de BlueXP en la nube, necesitas SSH para la instancia de

clasificación de BlueXP. Debe SSH al sistema introduciendo el usuario y la contraseña, o usando la clave SSH que ha proporcionado durante la instalación de BlueXP Connector. El comando SSH es:

```
 ssh -i <path_to_the_ssh_key> <machine_user>@<datasense_ip>
* <path_to_the_ssh_key> = ubicación de claves de autenticación ssh
* <machine_user>.:
```

+
Para AWS: Utilice <ec2-user>
Para Azure: Utilice el usuario creado para la instancia de BlueXP
** Para GCP: Utilice el usuario creado para la instancia de BlueXP

- <datasense_ip> = dirección IP de la instancia de la máquina virtual

Tenga en cuenta que deberá modificar las reglas entrantes del grupo de seguridad para acceder al sistema en la nube. Para obtener más información, consulte:

- "Reglas del grupo de seguridad en AWS"
- "Reglas de grupos de seguridad en Azure"
- "Reglas de firewall en Google Cloud"

API de clasificación de BlueXP

Las funcionalidades de clasificación de BlueXP que están disponibles en la interfaz de usuario web también están disponibles en la API de Swagger.

Hay cuatro categorías definidas en la clasificación de BlueXP que se corresponden con las pestañas de la interfaz de usuario:

- Investigación
- Cumplimiento de normativas
- Gobernanza
- Configuración

Las API de la documentación de Swagger te permiten buscar, agregar datos, realizar un seguimiento de tus escaneos y crear acciones como copiar, mover y otras.

Descripción general

La API le permite realizar las siguientes funciones:

- Información de exportación
  - Todo lo que está disponible en la interfaz de usuario se puede exportar a través de la API (con la excepción de los informes)
  - Los datos se exportan en formato JSON (fácil de analizar y enviar a aplicaciones de 3rd partes, como Splunk).
- Cree consultas utilizando las sentencias AND y OR, incluya y excluya información y mucho más.

Por ejemplo, puede localizar archivos *sin* Información personal identificable específica (PII) (funcionalidad no disponible en la interfaz de usuario). También puede excluir campos específicos para la operación de exportación.

- Realice acciones
  - Actualice las credenciales de CIFS
  - Ver y cancelar acciones
  - Vuelva a explorar los directorios
  - Elimine, copie, etiquete y asigne usuarios a los datos
  - Clonar y copiar archivos
  - Exportar datos

La API es segura y utiliza el mismo método de autenticación que la interfaz de usuario. Puede encontrar información sobre la autenticación en: https://docs.netapp.com/us-en/bluexp-automation/platform/get_identifiers.html

Acceder a la referencia de API de Swagger

Para entrar en Swagger, necesitarás la dirección IP de tu instancia de clasificación de BlueXP. En el caso de una puesta en marcha de cloud, utilizará la dirección IP pública. Entonces tendrás que entrar en este punto final:

https://<classification_ip>/documentación

Ejemplo que utiliza las API

En el siguiente ejemplo se muestra una llamada API para copiar archivos.

Solicitud API

Inicialmente, necesitará obtener todos los campos y opciones relevantes para un entorno de trabajo para ver todos los filtros en la pestaña Investigación.

```
curl -X GET "http://{classification_ip}/api/{classification_version}
/search/options?data_mode=ALL_EXTRACTABLE" -H "accept: application/json"
-H "Authorization: Bearer eyJhbGciOiJSUzI1NiIsInR…… " -H "x-agent-id:
hOXsZNvnA5LsthwMILtjL9xZFYBQxAwMclients"
```

Respuesta

```
{
  "options": [
    {
      "active_directory_affected": false,
      "data_mode": "ALL_SCANNED",
      "field": "string",
      "is_rulable": true,
      "name": "string",
```

```
      "operators": [
        "EQUALS"
      ],
      "optional_values": [
        {}
      ],
      "secondary": {},
      "server_data": false,
      "type": "TEXT"
    }
  ]
}
{
  "options": [
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "POLICIES",
      "name": "Policies",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "EXTRACTION_STATUS_RANGE",
      "name": "Scan Analysis Status",
      "operators": [
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "SCAN_ANALYSIS_ERROR",
      "name": "Scan Analysis Event",
      "operators": [
        "IN"
      ],
      "server_data": true,
```

```
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "PUBLIC_ACCESS",
      "name": "Open Permissions",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": true,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "USERS_PERMISSIONS_COUNT_RANGE",
      "name": "Number of Users with Access",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": true,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "USER_GROUP_PERMISSIONS",
      "name": "User / Group Permissions",
      "operators": [
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "FILE_OWNER",
      "name": "File Owner",
      "operators": [
        "EQUALS",
        "CONTAINS"
      ],
```

```
      "server_data": true,
      "type": "TEXT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "ENVIRONMENT_TYPE",
      "name": "Working Environment Type",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "ENVIRONMENT",
      "name": "Working Environment",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_SCANNED",
      "field": "SCAN_TASK",
      "name": "Storage Repository",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "FILE_PATH",
      "name": "File / Directory Path",
      "operators": [
        "MULTI_CONTAINS",
```

```
        "MULTI_EXCLUDE"
      ],
      "server_data": true,
      "type": "MULTI_TEXT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_DASHBOARD_EXTRACTABLE",
      "field": "CATEGORY",
      "name": "Category",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "PATTERN_SENSITIVITY_LEVEL",
      "name": "Sensitivity Level",
      "operators": [
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "NUMBER_OF_IDENTIFIERS",
      "name": "Number of identifiers",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "PATTERN_PERSONAL",
      "name": "Personal Data",
      "operators": [
```

```
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "PATTERN_SENSITIVE",
      "name": "Sensitive Personal Data",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "DATA_SUBJECT",
      "name": "Data Subject",
      "operators": [
        "EQUALS",
        "CONTAINS"
      ],
      "server_data": true,
      "type": "TEXT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "DIRECTORIES",
      "field": "DIRECTORY_TYPE",
      "name": "Directory Type",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "FILE_TYPE",
```

```
      "name": "File Type",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "FILE_SIZE_RANGE",
      "name": "File Size",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "FILE_CREATION_RANGE_RETENTION",
      "name": "Created Time",
      "operators": [
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "DISCOVERED_TIME_RANGE",
      "name": "Discovered Time",
      "operators": [
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "FILE_LAST_MODIFICATION_RETENTION",
```

```
      "name": "Last Modified",
      "operators": [
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "FILE_LAST_ACCESS_RANGE_RETENTION",
      "name": "Last Accessed",
      "operators": [
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "FILES",
      "field": "IS_DUPLICATE",
      "name": "Duplicates",
      "operators": [
        "EQUALS",
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "FILES",
      "field": "FILE_HASH",
      "name": "File Hash",
      "operators": [
        "EQUALS",
        "IN"
      ],
      "server_data": true,
      "type": "TEXT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "USER_DEFINED_STATUS",
```

```
      "name": "Tags",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "ASSIGNED_TO",
      "name": "Assigned to",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    }
  ]
}
```

Utilizaremos esa respuesta en nuestros parámetros de solicitud para filtrar los archivos deseados que queremos copiar.

Puede aplicar una acción en varios elementos. Los tipos de acción compatibles incluyen: Mover, eliminar, copiar, asignar a, FlexClone, exportar datos, volver a explorar y etiquetar.

Crearemos la acción de copia:

Solicitud API

Esta próxima API es esa API de acción y te permite crear múltiples acciones.

```
curl -X POST "http://
{classification_ip}/api//{classification_version}/actions" -H "accept:
application/json" -H "Authorization: Bearer eyJhbGciOiJSUzI1NiIsInR…… "
-H "x-agent-id: hOXsZNvnA5LsthwMILtjL9xZFYBQxAwMclients " -H "Content-
Type: application/json" -d "{ \"action_type\": \"COPY\", \"data_mode\":
\"FILES\", \"policy_id\": 0, \"request_params\": { destination_nfs_path:
"{ontap_ip}:/{share_name} " },
\"requested_query\":{"condition":"AND","rules":[{"field":"ENVIRONMENT_TYPE
","operator":"IN","value":["ONPREM"]},{"field":"CATEGORY","operator":"IN",
"value":["21"]}]}}"
```

Respuesta

La respuesta devolverá el objeto de acción, de modo que pueda utilizar las API GET y DELETE para obtener el estado de la acción o cancelarla.


```
{
  "action_type": "COPY",
  "creation_time": "2023-08-08T12:37:21.705Z",
  "data_mode": "FILES",
  "end_time": "2023-08-08T12:37:21.705Z",
  "estimated_time_to_complete": 0,
  "id": 0,
  "policy_id": 0,
  "policy_name": "string",
  "priority": 0,
  "request_params": {},
  "requested_query": {},
  "result": {
    "error_message": "string",
    "failed": 0,
    "in_progress": 0,
    "succeeded": 0,
    "total": 0
  },
  "start_time": "2023-08-08T12:37:21.705Z",
  "status": "QUEUED",
  "title": "string",
  "user_id": "string"
}
```