Referenz

BlueXP classification

NetApp
April 03, 2024

Inhalt

Referenz

Unterstützte BlueXP Klassifizierungs-Instanztypen

Die BlueXP Klassifizierungssoftware muss auf einem Host ausgeführt werden, der bestimmte Betriebssystemanforderungen, RAM-Anforderungen, Software-Anforderungen usw. erfüllt. Bei der Implementierung der BlueXP Klassifizierung in der Cloud empfehlen wir, ein System mit den „großen“ Merkmalen zu verwenden, um den vollen Funktionsumfang zu erhalten.

Sie können die BlueXP Klassifizierung auf einem System mit weniger CPUs und weniger RAM implementieren. Bei der Nutzung dieser weniger leistungsstarken Systeme bestehen jedoch einige Einschränkungen. "Informieren Sie sich über diese Einschränkungen".

Wenn in den folgenden Tabellen das als „Standard“ markierte System in der Region, in der Sie die BlueXP-Klassifizierung installieren, nicht verfügbar ist, wird das nächste System in der Tabelle bereitgestellt.

AWS-Instanztypen

Systemgröße	Spezifikationen	Instanztyp
Extra Groß	32 CPUs, 128 GB RAM, 1 tib gp3-SSD	"M6i.8xlarge" (Standard)
Groß	16 CPUs, 64 GB RAM, 500 gib SSD	"M6i.4xlarge" (Standard) m6a.4xlarge m5a.4xlarge m5.4xlarge m4.4xlarge
Mittel	8 CPUs, 32 GB RAM, 200 gib SSD	"M6i.2xlarge" (Standard) m6a.2xlarge m5a.2xlarge m5.2xlarge m4.2xlarge
Klein	8 CPUs, 16 GB RAM, 100 gib SSD	"c6a.2xlarge" (Standard) c5a.2xlarge c5.2xlarge c4.2xlarge

Azure Instanztypen

Systemgröße	Spezifikationen	Instanztyp
Extra Groß	32 CPUs, 128 GB RAM, BS-Festplatte (2,048 gib, min. 250 MB/s Durchsatz) und Datenfestplatte (1 tib SSD, min. 750 MB/s Durchsatz)	"Standard_D32_v3" (Standard)
Groß	16 CPUs, 64 GB RAM, 500 gib SSD	"Standard_D16s_v3" (Standard)

GCP-Instanztypen

Systemgröße	Spezifikationen	Instanztyp
Groß	16 CPUs, 64 GB RAM, 500 gib SSD	"n2-Standard-16" (Standard) n2d-Standard-16 n1-Standard-16

Metadaten, die aus Datenquellen erhoben werden

Die BlueXP Klassifizierung erfasst bestimmte Metadaten, wenn Klassifizierungs-Scans für Daten aus Datenquellen und Arbeitsumgebungen durchgeführt werden. Die BlueXP Klassifizierung kann auf die meisten Metadaten zugreifen, die wir für die Klassifizierung Ihrer Daten benötigen. Es gibt jedoch einige Quellen, aus denen wir nicht auf die von uns benötigten Daten zugreifen können.

	Metadaten	CIFS	NFS
Zeitstempel	*Erstellungszeit*	Verfügbar	Nicht verfügbar (nicht unterstützt in Linux)
	Zeitpunkt des letzten Zugriffs	Verfügbar	Verfügbar
	Letzte Änderungszeit	Verfügbar	Verfügbar
Berechtigungen	*Berechtigungen öffnen*	Wenn die Gruppe „ALLE“ Zugriff auf die Datei hat, gilt sie als „für Organisation geöffnet“.	Wenn „andere“ Zugriff auf die Datei haben, gilt sie als „für Organisation geöffnet“.
	Benutzer/Gruppenzugriff	Benutzer- und Gruppeninformationen werden aus LDAP übernommen	Nicht verfügbar (NFS-Benutzer werden in der Regel lokal auf dem Server verwaltet, daher kann dieselbe Person eine andere UID auf jedem Server haben)

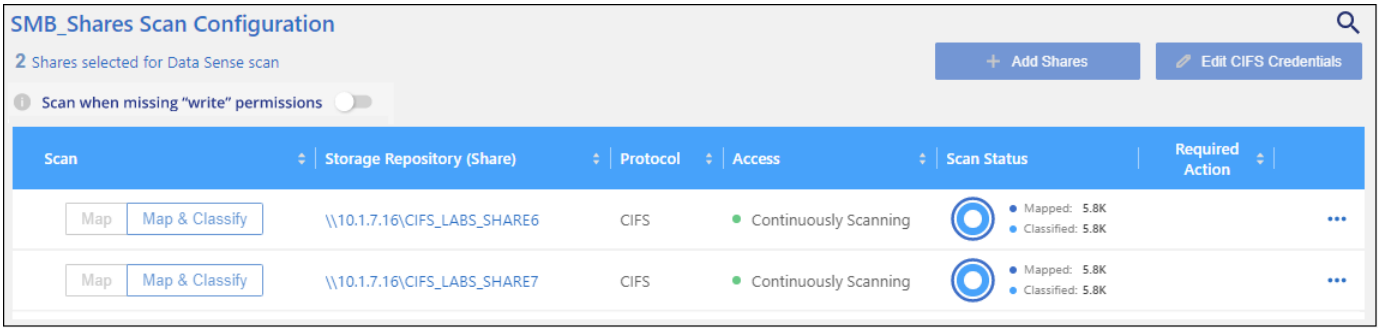
- Die BlueXP Klassifizierung extrahiert nicht den „Zeitpunkt des letzten Zugriffs“ aus den folgenden Datenquellen: SharePoint Online, SharePoint On-Premises (SharePoint Server), OneDrive, Google Drive und Amazon S3 sowie Datenbanken.
- Ältere Versionen des Windows-Betriebssystems (z. B. Windows 7 und Windows 8) deaktivieren standardmäßig die Sammlung des Attributs „Zeit des letzten Zugriffs“, da dies die Systemleistung beeinträchtigen kann. Wenn dieses Attribut nicht erfasst wird, ist die BlueXP Klassifizierungsanalyse, die auf dem Zeitpunkt des letzten Zugriffs basiert, betroffen. Bei Bedarf können Sie die Erfassung der letzten Zugriffszeit auf diesen älteren Windows-Systemen aktivieren.

Zeitstempel der letzten Zugriffszeit

Wenn die BlueXP Klassifizierung Daten aus File Shares extrahiert, berücksichtigt das Betriebssystem sie als Zugriff auf die Daten und ändert entsprechend den Zeitpunkt des letzten Zugriffs. Nach dem Scannen versucht die BlueXP Klassifizierung, die letzte Zugriffszeit auf den ursprünglichen Zeitstempel zurückzusetzen. Wenn die BlueXP Klassifizierung keine Schreibattributberechtigungen in CIFS oder Schreibberechtigungen in NFS hat, kann das System die letzte Zugriffszeit nicht auf den ursprünglichen Zeitstempel zurücksetzen. ONTAP Volumes, die mit SnapLock konfiguriert sind, haben schreibgeschützte Berechtigungen und können auch die letzte Zugriffszeit nicht auf den ursprünglichen Zeitstempel zurücksetzen.

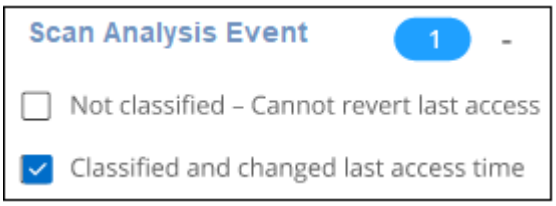
Wenn die BlueXP Klassifizierung diese Berechtigungen nicht besitzt, scannt das System standardmäßig diese Dateien in Ihren Volumes nicht, da die BlueXP Klassifizierung die „letzte Zugriffszeit“ nicht auf den ursprünglichen Zeitstempel zurücksetzen kann. Wenn es Ihnen jedoch egal ist, ob die letzte Zugriffszeit in Ihren Dateien auf die ursprüngliche Zeit zurückgesetzt wird, können Sie unten auf der Konfigurationsseite auf

den Schalter **Scan bei fehlenden Berechtigungen für "Schreibattribute"** klicken, damit die BlueXP-Klassifizierung die Volumes unabhängig von den Berechtigungen scannt.



Diese Funktionalität ist anwendbar auf On-Premises-ONTAP-Systeme, Cloud Volumes ONTAP, Azure NetApp Files, FSX for ONTAP und nicht-NetApp File Shares.

Beachten Sie, dass es einen Filter auf der Seite Untersuchung mit dem Namen *Scan Analysis Event* gibt, mit dem Sie entweder die Dateien anzeigen können, die nicht klassifiziert wurden, da die BlueXP-Klassifikation die letzte Zugriffszeit nicht rückgängig machen konnte. Oder die klassifizierten Dateien, auch wenn die BlueXP Klassifizierung den Zeitpunkt des letzten Zugriffs nicht zurücksetzen konnte.



Folgende Filteroptionen stehen zur Auswahl:

- „Nicht klassifiziert — kann letzte Zugriffszeit nicht rückgängig machen“ – zeigt die Dateien an, die aufgrund fehlender Schreibberechtigungen nicht klassifiziert wurden.
- „Zeitpunkt des letzten Zugriffs klassifiziert und aktualisiert“ – Hier werden die Dateien angezeigt, die klassifiziert wurden und die BlueXP-Klassifizierung konnte den Zeitpunkt des letzten Zugriffs nicht auf das ursprüngliche Datum zurücksetzen. Dieser Filter ist nur für Umgebungen relevant, in denen Sie **Scan bei fehlenden Berechtigungen für "Schreibattribute"** AKTIVIERT haben.

Bei Bedarf können Sie diese Ergebnisse in einen Bericht exportieren, damit Sie sehen können, welche Dateien aufgrund von Berechtigungen gescannt werden oder nicht. "Erfahren Sie mehr über den Untersuchungsbericht".

Melden Sie sich beim BlueXP Klassifizierungssystem an

Gelegentlich müssen Sie sich möglicherweise beim BlueXP Klassifizierungssystem anmelden, damit Sie auf Protokolldateien zugreifen oder Konfigurationsdateien bearbeiten können.

Wenn die BlueXP Klassifizierung auf einer lokalen Linux-Maschine oder auf einer in der Cloud implementierten Linux-Maschine installiert wird, können Sie direkt auf die Konfigurationsdatei und das Skript zugreifen.

Wenn die BlueXP Klassifizierung in der Cloud implementiert wird, müssen Sie SSH zur BlueXP Klassifizierungsinstanz verwenden. Sie können SSH auf dem System verwenden, indem Sie den Benutzer und das Kennwort eingeben oder den SSH-Schlüssel verwenden, den Sie während der Installation des BlueXP

Connectors angegeben haben. Der SSH-Befehl lautet:

```
 ssh -i <path_to_the_ssh_key> <machine_user>@<datasense_ip>
* <path_to_the_ssh_key> = Speicherort der ssh-Authentifizierungsschlüssel
* <machine_user>:
```

+
Für AWS: Verwenden Sie <ec2-user>
Für Azure: Verwenden Sie den für die BlueXP-Instanz erstellten Benutzer
** Für GCP: Verwenden Sie den für die BlueXP-Instanz erstellten Benutzer

- <dataense_ip> = IP-Adresse der virtuellen Maschineninstanz

Beachten Sie, dass Sie die Inbound-Regeln der Sicherheitsgruppe ändern müssen, um auf das System in der Cloud zuzugreifen. Weitere Informationen finden Sie unter:

- "Sicherheitsgruppenregeln in AWS"
- "Für Sicherheitsgruppen gibt es in Azure Regeln"
- "Firewall-Regeln in Google Cloud"

BlueXP Klassifizierungs-APIs

Die über die Web-UI verfügbaren BlueXP Klassifizierungsfunktionen sind auch über die Swagger-API verfügbar.

Die BlueXP Klassifizierung umfasst vier Kategorien, die den Registerkarten in der UI entsprechen:

- Untersuchung
- Compliance
- Governance
- Konfiguration

Die APIs in der Dokumentation von Swagger ermöglichen Ihnen, Daten zu durchsuchen, zu aggregieren, Ihre Scans zu verfolgen und Aktionen wie Kopieren, Verschieben und vieles mehr zu erstellen.

Überblick

Mit der API können Sie die folgenden Funktionen ausführen:

- Informationen exportieren
  - Alles, was in der Benutzeroberfläche verfügbar ist, kann über die API exportiert werden (mit Ausnahme von Berichten)
  - Daten werden in einem JSON-Format exportiert (Analyse und Verschiebung auf Applikationen von Drittanbietern wie Splunk ist einfach).
- Erstellen Sie Abfragen mit „UND“- und „ODER“-Anweisungen, schließen Sie Informationen ein und aus und vieles mehr.

  Beispielsweise können Sie Dateien *ohne* spezifische personenbezogene Daten (PII) suchen (Funktionalität

in der Benutzeroberfläche nicht verfügbar). Sie können auch bestimmte Felder für den Exportvorgang ausschließen.

- Führen Sie Aktionen aus
  - Aktualisieren Sie die CIFS-Anmeldeinformationen
  - Aktionen anzeigen und abbrechen
  - Verzeichnisse erneut scannen
  - Löschen, Kopieren, Beschriften und Zuweisen von Benutzern zu Daten
  - Dateien klonen und kopieren
  - Daten exportieren

Die API ist sicher und verwendet die gleiche Authentifizierungsmethode wie die UI. Informationen zur Authentifizierung finden Sie unter: https://docs.netapp.com/us-en/bluexp-automation/platform/get_identifiers.html

Zugriff auf die Swagger-API-Referenz

Um in Swagger zu kommen, benötigen Sie die IP-Adresse der BlueXP Klassifizierungsinstanz. Bei einer Cloud-Bereitstellung verwenden Sie die öffentliche IP-Adresse. Dann müssen Sie zu diesem Endpunkt gelangen:

\Https://<classification_ip>/Dokumentation

Beispiel mit den APIs

Das folgende Beispiel zeigt einen API-Aufruf zum Kopieren von Dateien.

API-Anfrage

Sie müssen zunächst alle relevanten Felder und Optionen für eine Arbeitsumgebung abrufen, um alle Filter auf der Registerkarte Untersuchung anzuzeigen.

```
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"
```

Antwort

```
{
  "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"
    }
  ]
}
```

Wir werden diese Antwort in unseren Anfrageparametern verwenden, um die gewünschten Dateien zu filtern, die wir kopieren möchten.

Sie können eine Aktion auf mehrere Elemente anwenden. Unterstützte Aktionstypen sind: Verschieben, löschen, kopieren, zuweisen, FlexClone, Daten exportieren, erneut scannen und beschriften.

Wir erstellen die Kopieraktion:

API-Anfrage

Diese nächste API ist die AktionAPI, und es ermöglicht Ihnen, mehrere Aktionen zu erstellen.

```
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"]}]}}"
```

Antwort

Die Antwort gibt das Aktionsobjekt zurück, sodass Sie mit den APIs get and delete den Status der Aktion

abrufen oder abbrechen können.


```
{
  "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"
}
```