Verwaltung und andere Aufgaben

Cloud Insights

NetApp
July 26, 2024

Inhalt

Verwaltung und andere Aufgaben

Cloud Insights API

Die Cloud Insights API ermöglicht NetApp Kunden und unabhängigen Software-Anbietern (ISVs) die Integration von Cloud Insights in andere Applikationen wie CMDB- oder andere Ticketsysteme.

Beachten Sie, dass Cloud Insights APIs entsprechend Ihrer aktuellen Ausgabe verfügbar sind:

API-Typ	Basic	Standard	Premium
Erfassungseinheit	✔	✔	✔
Datenerfassung	✔	✔	✔
Meldungen		✔	✔
Ressourcen		✔	✔
Datenaufnahme		✔	✔
Aufnahme Protokollieren		✔	✔

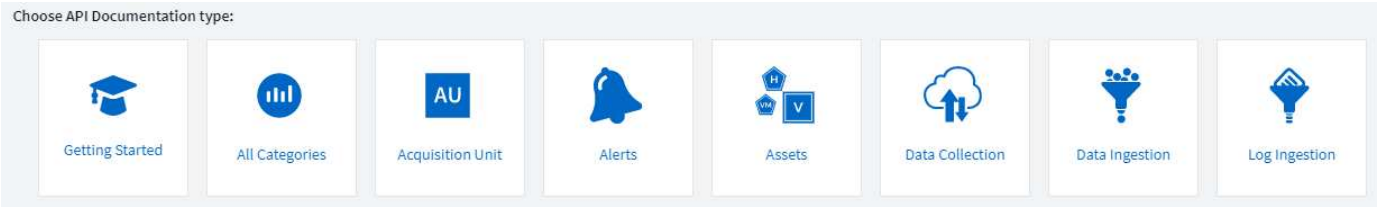
Darüber hinaus Ihr Cloud Insights "Funktionsgruppe Rolle" Bestimmt, auf welche APIs Sie zugreifen können. Benutzer- und Gastrollen haben weniger Berechtigungen als Administratorrolle. Wenn Sie z. B. in Überwachen und Optimieren eine Administratorrolle haben, die Rolle Benutzer jedoch in Reporting verwendet wird, können Sie alle API-Typen außer Data Warehouse verwalten.

Anforderungen für den API-Zugriff

- Ein API-Zugriffstoken-Modell wird verwendet, um den Zugriff zu gewähren.
- Das Management von API-Token wird von Cloud Insights-Benutzern mit der Administratorrolle durchgeführt.

API-Dokumentation (Swagger)

Die neuesten API-Informationen finden Sie, indem Sie sich bei Cloud Insights anmelden und zu **Admin > API Acccess** navigieren. Klicken Sie auf den Link **API Documentation**.



Die API-Dokumentation ist Swagger-basiert, die eine kurze Beschreibung und Verwendungsinformationen für die API, und ermöglicht es Ihnen, es in Ihrer Umgebung zu testen. Je nach Benutzerrolle und/oder Cloud Insights Edition können die für Sie verfügbaren API-Typen variieren.

ASSETS.annotations

POST `/assets/annotations` Create annotation definition

Parameters | Try it out

No parameters

Request body | application/json

Request body should include required name, type, optional description and enumValues (if enum type). Enums should contain name and label. Example:

```
{
    "name": "StorageLocation",
    "type": "FIXED_ENUM",
    "description": "Storage Location",
    "enumValues": [
        {
          "name": "PT_LISBON",
          "label": "Lisbon (Portugal)"
        },
        {
          "name": "US_WALTHAM",
          "label": "Waltham (USA)"
        }
    ]
}
```

Example Value | Schema

```
{}
```

API-Zugriffs-Tokens

Bevor Sie die Cloud Insights-API verwenden, müssen Sie ein oder mehrere **API-Zugriffstoken** erstellen. Access Tokens werden für angegebene API-Typen verwendet und können Lese- und/oder Schreibberechtigungen gewähren. Sie können auch die Ablauffrist für jedes Access Token festlegen. Alle APIs unter den angegebenen Typen sind für das Access-Token gültig. Jedes Token ist ungültig für einen Benutzernamen oder ein Kennwort.

So erstellen Sie ein Access Token:

- Klicken Sie auf **Admin > API Access**
- Klicken Sie auf **+API Access Token**
  - Geben Sie Den Namen Des Tokens Ein
  - Wählen Sie API-Typen aus
  - Geben Sie die Berechtigungen an, die für diesen API-Zugriff gewährt wurden
  - Legen Sie Den Ablauf Des Tokens Fest

> Ihr Token kann nur während des Erstellungsvorgangs in die Zwischenablage kopiert und gespeichert werden. Token können nicht abgerufen werden, nachdem sie erstellt wurden. Daher wird dringend empfohlen, das Token zu kopieren und an einem sicheren Ort zu speichern. Sie werden aufgefordert, auf die Schaltfläche **Copy API Access Token** zu klicken, bevor Sie den Bildschirm zur Tokenerstellung schließen können.

Sie können Token deaktivieren, aktivieren und widerrufen. Deaktivierte Token können aktiviert werden.

Tokens gewähren aus Kundensicht allgemeinen Zugang zu APIs; Management des Zugriffs auf APIs im Umfang ihres eigenen Mandanten. Kundenadministratoren können diese Token ohne direkte Beteiligung von Cloud Insights Back-End-Mitarbeitern erteilen und widerrufen.

Die Anwendung erhält ein Zugriffstoken, nachdem ein Benutzer den Zugriff erfolgreich authentifiziert und autorisiert hat, und übergibt das Access Token dann als Berechtigung, wenn es die Ziel-API anruft. Das übergebene Token informiert die API, dass der Inhaber des Tokens berechtigt ist, auf die API zuzugreifen und bestimmte Aktionen durchzuführen, die vom Umfang festgelegt wurden, der während der Autorisierung gewährt wurde.

Der HTTP-Header, in dem das Access Token übergeben wird, ist **X-CloudInsights-ApiKey:**.

Verwenden Sie zum Abrufen von Lagerbeständen beispielsweise Folgendes:

```
 curl https://<tenant_host_name>/rest/v1/assets/storages -H 'X-
CloudInsights-ApiKey:<API_Access_Token>'
Wobei _<API_Access_Token>_ das Token ist, das Sie bei der Erstellung des
API-Zugriffs gespeichert haben.
```

Beispiele für die API, die Sie verwenden möchten, finden Sie auf den Seiten der Schwagger.

API-Typ

Die Cloud Insights-API ist kategoribasiert und enthält derzeit die folgenden Typen:

- DER ASSET-Typ enthält Asset-, Abfrage- und Such-APIs.
  - Assets: Listen Sie Objekte der obersten Ebene auf und rufen Sie ein bestimmtes Objekt oder eine Objekthierarchie ab.
  - Abfrage: Abrufen und Verwalten von Cloud Insights-Abfragen.
  - Import: Importieren Sie Anmerkungen oder Anwendungen und weisen Sie sie Objekten zu
  - Suche: Suchen Sie ein bestimmtes Objekt, ohne die eindeutige ID oder den vollständigen Namen des Objekts zu kennen.
- DER DATENERFASSUNGSTYP dient zum Abrufen und Verwalten von Datensammlern.
- Mit DEM AUFNAHMERUNGSTYP können Aufnahmedaten und benutzerdefinierte Metriken abgerufen und gemanagt werden, beispielsweise von Telegraf-Agenten
- MITHILFE DER PROTOKOLLAUFNAHME werden Protokolldaten abgerufen und gemanagt

Weitere Typen und/oder APIs können im Laufe der Zeit verfügbar sein. Die neuesten API-Informationen finden Sie im "API-Swagger-Dokumentation".

Beachten Sie, dass die API-Typen, auf die ein Benutzer Zugriff hat, auch vom abhängen "Benutzerrolle" Sie

werden in allen Cloud Insights Funktionen eingesetzt (Monitoring, Workload-Sicherheit, Berichterstellung).

Inventurtraversal

In diesem Abschnitt wird beschrieben, wie eine Hierarchie von Cloud Insights-Objekten durchlaufen wird.

Objekte Der Obersten Ebene

Einzelne Objekte werden in Anfragen durch eine eindeutige URL (in JSON als „selbst“ bezeichnet) identifiziert und erfordern Kenntnisse über Objekttyp und interne ID Für einige der Objekte der obersten Ebene (Hosts, Storage usw.) bietet DIE REST API Zugriff auf die vollständige Sammlung.

Das allgemeine Format einer API-URL lautet:

```
 https://<tenant>/rest/v1/<type>/<object>
Um beispielsweise alle Speicher von einem Mandanten mit dem Namen
_mysite.c01.cloudinsights.netapp.com_ abzurufen, lautet die Anfrage-URL:
```

```
https://mysite.c01.cloudinsights.netapp.com/rest/v1/assets/storages
```

Kinder und verwandte Objekte

Objekte auf oberster Ebene, wie z. B. Speicherung, können für andere Kinder und verwandte Objekte verwendet werden. Zum Beispiel, um alle Datenträger für einen bestimmten Speicher abzurufen, verketten Sie die Speicher-URL „selbst“ mit „/Disks“, zum Beispiel:

```
https://<tenant>/rest/v1/assets/storages/4537/disks
```

Erweitert

Viele API-Befehle unterstützen den Parameter **Expand**, der zusätzliche Details zum Objekt oder URLs für verwandte Objekte enthält.

Der gemeinsame Expand-Parameter ist *Expands*. Die Antwort enthält eine Liste aller verfügbaren spezifischen Expands für das Objekt.

Beispiel: Wenn Sie Folgendes anfordern:

```
 https://<tenant>/rest/v1/assets/storages/2782?expand=_expands
Die API gibt alle verfügbaren Expands für das Objekt wie folgt zurück:
```

```
{
    "id": "1247936",
      "self": "/rest/v1/assets/storages/1247936",
      "name": "amsprdclu01",
      "simpleName": "amsprdclu01",
      "naturalKey": "5DF483F0-1729-11DC-9A79-123478563412",
      "ip": "10.64.0.132",
      "serialNumber": "1-80-000011",
      "model": "FAS3270,FAS6290",
      "vendor": "NetApp",
      "microcodeVersion": "8.1.3 clustered Data ONTAP",
      "capacity": {
        "description": "Storage Capacity",
        "unitType": "MB",
        "total": {
          "value": 8.23185105E8
        },
        "storagePools": {
          "value": 5.43220974E8
        }
      },
      "isActive": true,
      "createTime": "2013-05-07T16:52:21-0700",
      "family": "FAS3200,FAS6200",
      "managementUrl": null,
      "virtualizedType": "STANDARD",
      "protocols":
      [
        "NAS",
        "NFS",
        "CIFS",
        "FC",
        "ISCSI"
      ],
      "_expands": {
        "performance": {
          "url": "/rest/v1/assets/storages/1247936/performance",
          "name": "Performance Data"
        },
        "storageNodes": {
          "url": "/rest/v1/assets/storages/1247936/storageNodes",
          "name": "Storage Storage Nodes"
        },
        "storagePools": {
          "url": "/rest/v1/assets/storages/1247936/storagePools",
          "name": "Storage Storage Pools"
        },
        "storageResources": {
          "url": "/rest/v1/assets/storages/1247936/storageResources",
          "name": "Storage Storage Resourcs"
        },
        "internalVolumes": {
          "url": "/rest/v1/assets/storages/1247936/internalVolumes",
          "name": "Storage Internal Volumes"
        },
        "volumes": {
          "url": "/rest/v1/assets/storages/1247936/volumes",
          "name": "Storage Volumes"
        },
        "disks": {
          "url": "/rest/v1/assets/storages/1247936/disks",
          "name": "Disks"
        },
        "datasources": {
          "url": "/rest/v1/assets/storages/1247936/datasources",
          "name": "Storage Datasources"
        },
        "ports": {
          "url": "/rest/v1/assets/storages/1247936/ports",
          "name": "Storage Ports"
        },
        "annotations": {
          "url": "/rest/v1/assets/storages/1247936/annotations",
          "name": "Storage Annotations"
        },
        "qtrees": {
          "url": "/rest/v1/assets/storages/1247936/qtrees",
          "name": "Qtrees"
        },
```

Jede Erweiterung enthält Daten, eine URL oder beides. Der Parameter Expand unterstützt mehrere und verschachtelte Attribute, z. B.:

```
 https://<tenant>/rest/v1/assets/storages/2782?expand=performance,storageR
esources.storage
Mit Expand lassen sich zahlreiche verwandte Daten in einer einzigen Lösung
integrieren. NetApp rät Ihnen, nicht zu viele Informationen gleichzeitig
anzufordern. Dies kann zu einer Verschlechterung der Performance führen.
```

Um dies zu entmutigen, können Anfragen nach Beständen der obersten Ebene nicht erweitert werden. Beispielsweise können Sie keine Expand-Daten für alle Speicherobjekte gleichzeitig anfordern. Die Clients müssen die Liste der Objekte abrufen und dann spezifische Objekte auswählen, die erweitert werden sollen.

Performance-Daten

Performancedaten werden über viele Geräte als separate Proben erfasst. Jede Stunde (Standard) Cloud Insights aggregiert und fasst Performance-Muster zusammen.

Die API ermöglicht den Zugriff auf sowohl die Proben als auch auf die zusammengefassten Daten. Bei einem Objekt mit Performance-Daten ist eine Performance-Zusammenfassung als *Expand=Performance* verfügbar. Die Zeitreihen für den Leistungsverlauf sind über die verschachtelte_Expand=Performance.history_ verfügbar.

Beispiele für Performance-Datenobjekte:

- Storage Performance
- StoragePoolPerformance
- PortPerformance
- DiskPerformance

Eine Leistungsmetric hat eine Beschreibung und einen Typ und enthält eine Sammlung von Leistungsübersichten. Beispiel: Latenz, Datenverkehr und Rate.

Eine Leistungsübersicht enthält eine Beschreibung, Einheit, Beispielstartzeit, Probenendzeit und eine Sammlung von zusammengefassten Werten (Strom, min, max, avg usw.), die aus einem einzelnen Leistungszähler über einen Zeitbereich (1 Stunde, 24 Stunden, 3 Tage usw.) berechnet werden.

https://tenant.cloudinsights.netapp.com/rest/v1/assets/storages/1/performance?expand=history

Details

Response body


```
{
  "self": "/rest/v1/assets/storages/1/performance",
  "cacheHitRatio": {
    "read": {
      "description": "Cache Hit Ratio - Read",
      "unitType": "%",
      "start": null,
      "end": null,
      "current": null,
      "min": null,
      "max": null,
      "avg": null,
      "sum": null,
      "isDownsampled": false
    },
    "write": {
      "description": "Cache Hit Ratio - Write",
      "unitType": "%",
      "start": null,
      "end": null,
      "current": null,
      "min": null,
      "max": null,
      "avg": null
```


Self

Performance Metric

Response body


```
    }
  },
  "history": [
    [
      1578418848140,
      {
        "latency.total": 1.30578,
        "latency.read": 3.64681,
        "ioDensity.read": 9.62065,
        "iops.write": 686.35502,
        "ioDensity.total": 31.36259,
        "capacity.raw": 80024.92772,
        "throughput.read": 7.32371,
        "iops.total": 1488.7974,
        "latency.write": 0.39495,
        "ioDensity.write": 14.45856,
        "iops.read": 456.69703,
        "capacity.storagePools": 56058.1041,
        "throughput.write": 14.59581,
        "throughput.total": 21.91953
      }
    ],
    [
      1578419748198,
```


History

Timestamp

Counter Values

Das resultierende Wörterbuch für Leistungsdaten enthält die folgenden Schlüssel:

- „Selbst“ ist die eindeutige URL des Objekts

- „History“ ist die Liste der Paare von Zeitstempel und Karte von Zählerwerten
- Jeder andere Wörterbuchschlüssel („diskThrughput“ usw.) ist der Name einer Leistungsmetrik.

Jeder Performance-Datenobjekttyp verfügt über einen eigenen Satz von Performance-Kennzahlen. Das Performance-Objekt der virtuellen Maschine unterstützt beispielsweise „diskThrughput“ als Leistungskennzahl. Jede unterstützte Leistungsmetrik ist eine bestimmte „performanceCategory“, die im metrischen Wörterbuch dargestellt wird. Cloud Insights unterstützt verschiedene Performance-Kennzahlen, die später in diesem Dokument aufgeführt sind. Jedes Wörterbuch der Leistungsmetrik hat auch das Feld „Beschreibung“, das eine vom Menschen lesbare Beschreibung dieser Leistungsmetrik und eine Reihe von Zähleinträgen mit Leistungszusammenfassung ist.

Der Zähler der Leistungsübersicht ist die Zusammenfassung der Leistungsindikatoren. Er zeigt typische aggregierte Werte wie Min., Max. Und Avg für einen Zähler sowie den neuesten beobachteten Wert, den Zeitbereich für zusammengefasste Daten, den Einheitstyp für Zähler und die Schwellenwerte für Daten. Nur Schwellenwerte sind optional; die restlichen Attribute müssen angegeben werden.

Leistungsübersichten stehen für diese Zählertypen zur Verfügung:

- Lesen – Zusammenfassung für Lesevorgänge
- Write – Zusammenfassung für Schreibvorgänge
- Gesamt: Zusammenfassung für alle Operationen. Es kann höher sein als die einfache Summe von Lesen und Schreiben; es kann auch andere Operationen.
- Total Max – Zusammenfassung für alle Operationen. Dies ist der maximale Gesamtwert im angegebenen Zeitbereich.

Kennzahlen Für Die Objekt-Performance

Die API kann detaillierte Metriken für Objekte in Ihrer Umgebung zurückgeben, z. B.:

- Storage-Performance-Kennzahlen wie IOPS (Anzahl der ein-/Ausgabe-Anfragen pro Sekunde), Latenz oder Durchsatz.
- Kennzahlen zur Switch-Performance, z. B. Datenverkehrsnutzung, BB Credit Zero Daten oder Port-Fehler.

Siehe "API-Swagger-Dokumentation" Weitere Informationen zu Metriken für die einzelnen Objekttypen.

Performance-Verlaufsdaten

Verlaufsdaten werden in Leistungsdaten als Liste der Zeitstempel- und Zählermaps-Paare präsentiert.

Verlaufszähler werden basierend auf dem Objektnamen der Performance-Metrik benannt. Das Performance-Objekt der virtuellen Maschine unterstützt beispielsweise „diskThrughput“, so dass die Geschichtskarte Schlüssel mit den Namen „diskThrughput.read“, „diskThrughput.write“ und „diskThrughput.total“ enthält.

Zeitstempel befindet sich im UNIX-Zeitformat.

Dies ist ein Beispiel für einen Performance-Daten-JSON für eine Festplatte:

```
"performance": {
    "self": "/rest/v1/assets/disks/4013931/performance",
    "iops": {
      "performanceCategory": "IOPS",
      "description": "Disk IOPS",
      "read": {
        "description": "Disk Read Iops",
        "unitType": "IO/s",
        "start": 1399305599999,
        "end": 1402604368055,
        "current": 1,
        "min": 0,
        "max": 6,
        "avg": 0.5532
      },
  […]
     "total": {
        "description": "Disk Total Throughput",
        "unitType": "MB/s",
        "start": 1399305599999,
        "end": 1402604368055,
        "current": 0,
        "min": 0,
        "max": 2,
        "avg": 0.1702
      }
    },
    "history":
    [
      [
        1399300412690,
        {
          "utilization.total": 12,
          "iops.total": 26,
          "iops.write": 22,
          "iops.read": 4,
          "throughput.read": 0,
          "utilization.read": 2.12,
          "throughput.total": 5,
          "utilization.write": 10.24,
          "throughput.write": 5
```


Objekte mit Kapazitätsattributen

Objekte mit Kapazitätsattributen verwenden grundlegende Datentypen und das kapazitätItem zur Darstellung.

KapazitätArtikel

KapazitätItem ist eine einzige logische Einheit der Kapazität. Er hat „Wert“ und „highThreshold“ in Einheiten, die durch sein übergeordnetes Objekt definiert sind. Zudem unterstützt es eine optionale Übersichtskarte, in der die Konstruktion des Kapazitätswerts erläutert wird. So wäre beispielsweise die Gesamtkapazität eines 100 TB StoragePool ein KapazitätItem mit einem Wert von 100. Die Aufschlüsselung kann 60 TB für „Daten“ und 40 TB für „Snapshots“ zugewiesen zeigen.

Hinweis

> „HighThreshold“ stellt systemdefinierte Schwellenwerte für die entsprechenden Metriken dar, mit denen ein Kunde Alarme oder visuelle Hinweise auf Werte generieren kann, die außerhalb des zulässigen konfigurierten Messebereiches liegen.

Die folgende Anzeige zeigt die Kapazität von StoragePools mit mehreren Kapazitätszählern:

StoragePoolCapacity

```
Model properties:
{
 description: string
 unitType: 'MB' or 'GB' or 'TB' or 'KiB' or 'MiB' or 'TiB'
 total: CapacityItem
 used: CapacityItem
 provisioned: CapacityItem
 reservedCapacity: CapacityItem
 softLimit: Double
 rawToUsableRatio: Double
 isDedupeEnabled: boolean
 dedupeSavings: NumericValueWithUnit
 isCompressionEnabled: boolean
 compressionSavings: NumericValueWithUnit
 isThinProvisioningSupported: boolean
}
```

close

Suchen von Objekten mit Suchen

Die Such-API ist ein einfacher Einstiegspunkt zum System. Der einzige Eingabeparameter für die API ist eine freie Zeichenfolge, und der resultierende JSON enthält eine kategorisierte Liste der Ergebnisse. Typen sind verschiedene Asset-Typen aus dem Inventar, z. B. Speicher, Hosts, Datenspeicher usw. Jeder Typ würde eine Liste von Objekten des Typs enthalten, die den Suchkriterien entsprechen.

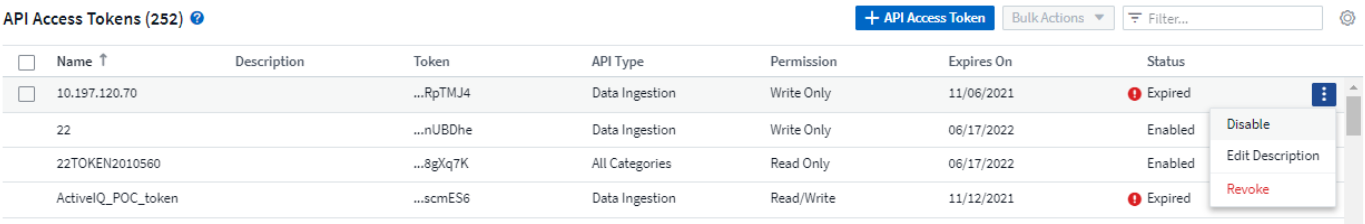
Cloud Insights ist eine erweiterbare (offene) Lösung, die die Integration in Orchestrierungs-, Business-Management-, Änderungs- und Ticketsysteme anderer Anbieter sowie in individuelle CMDB-Integrationen ermöglicht.

Die RESTful API von Cloud Insight ist ein primärer Integrationspunkt für eine einfache und effektive Datenverschiebung und ermöglicht Anwendern nahtlosen Zugriff auf ihre Daten.

Deaktivieren oder Deaktivieren eines API-Tokens

Um ein API-Token vorübergehend zu deaktivieren, klicken Sie auf der API-Token-Listenseite auf das Menü „drei Punkte“ für die API und wählen Sie *Disable*. Sie können das Token jederzeit über dasselbe Menü wieder aktivieren und *Enable* auswählen.

Um ein API-Token dauerhaft zu entfernen, wählen Sie im Menü die Option „Widerruf“. Sie können ein entzogen Token nicht erneut aktivieren; Sie müssen ein neues Token erstellen.



Token für abgelaufenen API-Zugriff werden gedreht

Die Token für den API-Zugriff haben ein Ablaufdatum. Wenn ein API-Zugriffstoken abläuft, müssen Benutzer ein neues Token generieren (vom Typ *Datenaufnahme* mit Lese-/Schreibberechtigungen) und Telegraf neu konfigurieren, um das neu generierte Token anstelle des abgelaufenen Tokens zu verwenden. In den folgenden Schritten wird die Vorgehensweise beschrieben.

Kubernetes

Beachten Sie, dass diese Befehle den Standard-Namespace „netapp-Monitoring“ verwenden. Wenn Sie Ihren eigenen Namespace festgelegt haben, ersetzen Sie diesen Namespace in diesen und allen nachfolgenden Befehlen und Dateien.

Hinweis: Wenn Sie die neueste Installation von NetApp Kubernetes Monitoring Operator und ein erneuerbares API-Zugriffstoken verwenden, werden auslaufende Tokens automatisch durch neue/aktualisierte API-Zugriffs-Tokens ersetzt. Die unten aufgeführten manuellen Schritte müssen nicht ausgeführt werden.

- Bearbeiten Sie den NetApp Kubernetes Monitoring Operator.

```
 kubectl -n netapp-monitoring edit agent agent-monitoring-netapp
* Ändern Sie den Wert _spec.output-sink.API-key_ und ersetzen Sie das
alte API-Token durch das neue API-Token.
```

```
spec:
…
  output-sink:
  - api-key:<NEW_API_TOKEN>
```

RHEL/CentOS und Debian/Ubuntu

- Bearbeiten Sie die Telegraf-Konfigurationsdateien und ersetzen Sie alle Instanzen des alten API-Tokens durch das neue API-Token.

```
 sudo sed -i.bkup 's/<OLD_API_TOKEN>/<NEW_API_TOKEN>/g'
/etc/telegraf/telegraf.d/*.conf
* Telegraf Neu Starten.
```

```
sudo systemctl restart telegraf
```

Windows

- Ersetzen Sie für jede Telegraf-Konfigurationsdatei in *C:\Programme\telegraf\telegraf.d* alle Instanzen des alten API-Tokens durch das neue API-Token.

```
cp <plugin>.conf <plugin>.conf.bkup
(Get-Content <plugin>.conf).Replace('<OLD_API_TOKEN>',
'<NEW_API_TOKEN>') | Set-Content <plugin>.conf
```

- Telegraf Neu Starten.

```
Stop-Service telegraf
Start-Service telegraf
```

Monitoring Ihrer Umgebung

Prüfung

Zum Identifizieren von Änderungen, die sowohl erwartet (zur Nachverfolgung) als auch unerwartet (zur Fehlerbehebung), können Sie einen Audit-Trail der Cloud Insights-Systemereignisse und Benutzeraktivitäten anzeigen.

Anzeigen Von Geprüften Ereignissen

Um die Seite „Audit“ anzuzeigen, klicken Sie im Menü auf **Admin > Audit**. Die Seite „Audit“ wird angezeigt und enthält die folgenden Details für jeden Audit-Eintrag:

- **Zeit** - Datum und Uhrzeit der Veranstaltung oder Aktivität
- **Benutzer** - der Benutzer, der die Aktivität initiiert hat
- **Rolle** - die Rolle des Benutzers in Cloud Insights (Gast, Benutzer, Administrator)
- **IP** - die IP-Adresse, die dem Ereignis zugeordnet ist
- **Aktion** - Art der Aktivität, z. B. Login, Erstellen, Aktualisieren
- **Kategorie** - die Kategorie der Aktivität
- **Details** - Details zur Aktivität

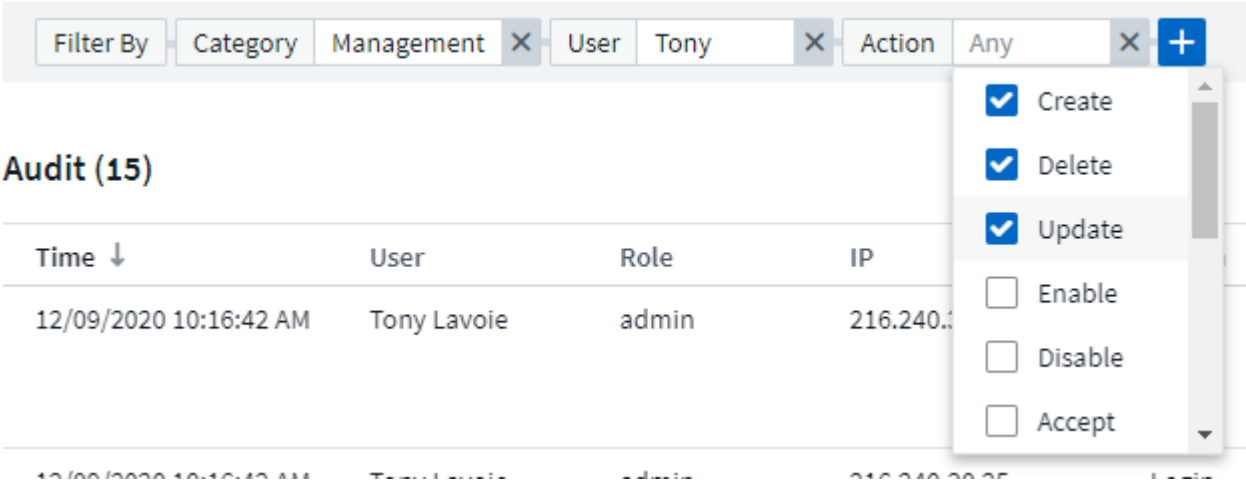
Anzeigen von Audit-Einträgen

Es gibt verschiedene Möglichkeiten, Audit-Einträge anzuzeigen:

- Sie können Audit-Einträge anzeigen, indem Sie einen bestimmten Zeitraum (1 Stunde, 24 Stunden, 3 Tage usw.) auswählen.
- Sie können die Sortierreihenfolge der Einträge entweder auf aufsteigend (nach-oben-Pfeil) oder absteigend (nach-unten-Pfeil) ändern, indem Sie auf den Pfeil in der Spaltenüberschrift klicken.

  Standardmäßig werden in der Tabelle die Einträge in absteigender Reihenfolge angezeigt.

- Mit den Filterfeldern können Sie nur die Einträge anzeigen, die in der Tabelle angezeigt werden sollen. Klicken Sie auf die Schaltfläche [+], um weitere Filter hinzuzufügen.



Mehr zum Filtern

Sie können einen der folgenden Optionen verwenden, um Ihren Filter zu verfeinern:

Filtern	Das macht es	Beispiel	Ergebnis
* (Sternchen)	Ermöglicht Ihnen die Suche nach allem	vol.	Gibt alle Ressourcen zurück, die mit „vol“ beginnen und mit „RHEL“ enden
? (Fragezeichen)	Ermöglicht die Suche nach einer bestimmten Anzahl von Zeichen	BOS-PRD??-S12	Gibt BOS-PRD zurück***12_ -S12, BOS-PRD23_***-S12 und so weiter
ODER	Ermöglicht Ihnen die Angabe mehrerer Elemente	FAS2240, CX600 ODER FAS3270	Gibt eine beliebige von FAS2440, CX600 oder FAS3270 zurück
NICHT	Ermöglicht das Ausschließen von Text aus den Suchergebnissen	NICHT EMC*	Liefert alles zurück, was nicht mit „EMC“ beginnt
Keine	Sucht in einem beliebigen Feld nach leer/Null/Keine	*Keine*	Gibt Ergebnisse zurück, bei denen das Zielfeld nicht leer ist
Nicht *	Wie bei *None* oben, aber Sie können dieses Formular auch verwenden, um in *Text-only*-Feldern nach Null-Werten zu suchen	Nicht *	Gibt Ergebnisse zurück, bei denen das Zielfeld nicht leer ist.
„“	Sucht nach einer genauen Übereinstimmung	„NetApp*“	Liefert Ergebnisse mit der exakten Zeichenfolge *NetApp**

Wenn Sie einen Filter in doppelte Anführungszeichen einschließen, behandelt Insight alles zwischen dem ersten und dem letzten Zitat als exakte Übereinstimmung. Alle Sonderzeichen oder Operatoren in den Angeboten werden als Literale behandelt. Wenn Sie beispielsweise nach „*“ filtern, erhalten Sie Ergebnisse, die ein wortwörtlicher Stern sind; das Sternchen wird in diesem Fall nicht als Platzhalter behandelt. Die Operatoren OR und NOT werden auch als Literalzeichenfolgen behandelt, wenn sie in doppelten Anführungszeichen eingeschlossen sind.

Geprüfte Ereignisse und Maßnahmen

Die von Cloud Insights auditierten Ereignisse und Maßnahmen können in die folgenden allgemeinen Bereiche unterteilt werden:

- **Benutzerkonto**: Anmelden, Abmelden, Rollenänderung, etc

  Beispiel: *User **Tony Lavoie** angemeldet von **10.1.120.15**, User Agent **Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, wie Gecko) Chrome/85.0.4183.121 Safari/537.36**, Login-Methode(en) **BlueXP Portal Login***

- **Erfassungseinheit**: Erstellen, löschen usw.

  Beispiel: *Acquisition Unit **AU-Boston-1** entfernt*.

- **Data Collector**: Hinzufügen, entfernen, ändern, verschieben/fortsetzen, Erfassungseinheit ändern, Start/Stopp usw.

  Beispiel: *Datasource **FlexPod Lab** entfernt, Anbieter **NetApp**, Modell **ONTAP Datenmanagement-Software**, ip **192.168.106.5***.

- **Anwendung**: Hinzufügen, Objekt zuweisen, entfernen, etc

  Beispiel: *Internes Volumen **ocisedev:t1appSVM01:t1appFlexVol01** zur Anwendung hinzugefügt **Test App***.

- **Anmerkung**: Hinzufügen, zuweisen, entfernen, Anmerkungsregeln Aktionen, Anmerkungswert ändert sich, Usw.

  Beispiel: *Anmerkungswert **Boston** wurde dem Anmerkungstyp **SalesOffice*** hinzugefügt.

- **Abfrage**: Hinzufügen, entfernen, etc

  Beispiel: *Query **TL Sales Query** wird hinzugefügt*.

- **Monitor**: Hinzufügen, entfernen, etc

  Beispiel: Monitor *Aggr Size - CI Alerts Notifications Dev* aktualisiert

- **Benachrichtigung**: E-Mail ändern, etc

  Beispiel: Empfänger *ci-Alerts-notifications-dl* erstellt

Audit-Ereignisse Werden Exportiert

Sie können die Ergebnisse Ihrer Audit-Anzeige in eine .CSV-Datei exportieren, mit der Sie die Daten analysieren oder in eine andere Anwendung importieren können.

Schritte

1. Legen Sie auf der Seite „Audit“ den gewünschten Zeitbereich und alle gewünschten Filter fest. Cloud Insights exportiert nur die Audit-Einträge, die dem eingestellten Filter- und Zeitbereich entsprechen.
2. Klicken Sie auf die Schaltfläche *Export* Rechts oben am Tisch.

Die angezeigten Audit-Ereignisse werden in eine .CSV-Datei mit maximal 10,000 Zeilen exportiert.

Aufbewahrung von Audit-Daten

Wie lange Cloud Insights Audit-Daten aufbewahrt, hängt von Ihrer Edition ab:

- Basic Edition: Audit-Daten werden 30 Tage lang aufbewahrt
- Standard- und Premium-Editionen: Audit-Daten werden für 1 Jahr plus 1 Tag aufbewahrt

Überwachungseinträge, die älter als die Aufbewahrungszeit sind, werden automatisch gelöscht. Es ist keine Benutzerinteraktion erforderlich.

Fehlerbehebung

Hier finden Sie Vorschläge zur Fehlerbehebung bei Audit-Problemen.

Problem:	Teste das:
Ich sehe die Meldungen von Audit, die mir sagen, dass ein Monitor exportiert wurde.	Der Export einer benutzerdefinierten Monitorkonfiguration wird von NetApp Technikern üblicherweise bei der Entwicklung und dem Testen neuer Funktionen verwendet. Wenn Sie diese Meldung nicht erwarten, sollten Sie die in der geprüften Aktion genannten Maßnahmen des Benutzers oder den Support des Kontakts untersuchen.

Active IQ

NetApp "Active IQ" Bietet NetApp Kunden eine Reihe von Visualisierungen, Analysen und anderen Support-Services für ihre Hardware- und Softwaresysteme. Die von Active IQ gemeldeten Daten können die Fehlerbehebung bei Systemproblemen verbessern und auch Einblicke in Optimierungs- und vorausschauende Analysen für Ihre Geräte bieten.

ActiveIQ ist in der Cloud Insights Bundesausgabe nicht verfügbar.

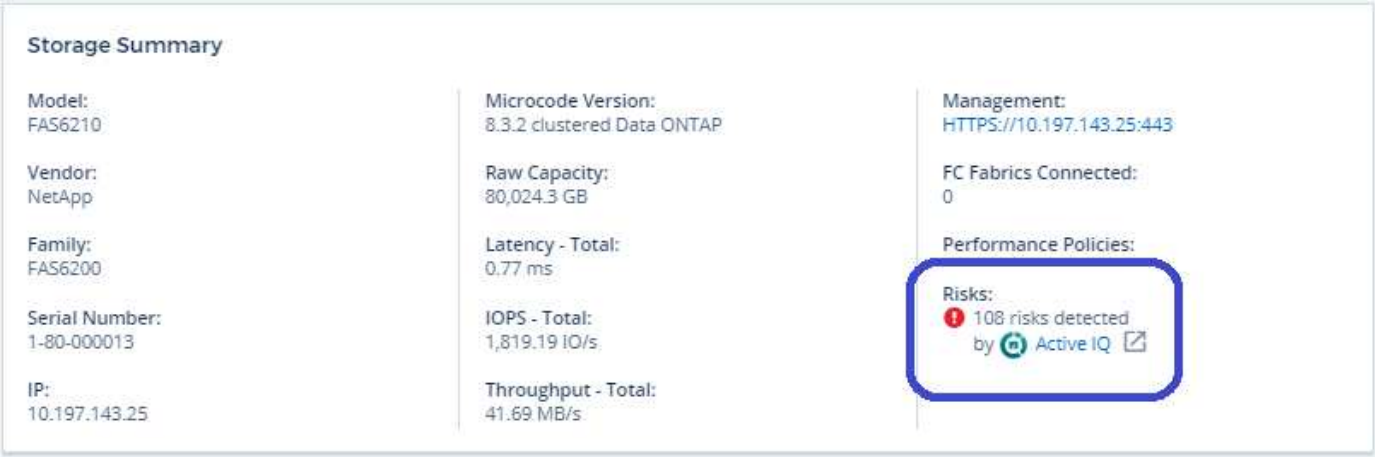
Cloud Insights sammelt die **Risiken** für jedes NetApp Clustered Data ONTAP Storage-System, das von Active IQ überwacht und gemeldet wird. Die für die Storage-Systeme gemeldeten Risiken werden automatisch von Cloud Insights im Rahmen der Datenerfassung dieser Geräte erfasst. Sie müssen den entsprechenden Datensammler zu Cloud Insights hinzufügen, um Active IQ-Risikoinformationen zu sammeln.

Cloud Insights zeigt keine Risikodaten bei ONTAP Systemen an, die nicht von Active IQ überwacht und gemeldet werden.

Die gemeldeten Risiken werden in Cloud Insights auf den Asset-Landing-Pages „ *Storage* und *Storage-Node*“ in der Tabelle „Risiken“ angezeigt. Die Tabelle enthält Risikodetails, Risikokategorie und potenzielle Auswirkungen des Risikos und einen Link zur Active IQ-Seite, die alle Risiken für den Storage-Node

(Anmeldung für einen NetApp Support Account erforderlich) enthält.

Eine Anzahl der gemeldeten Risiken wird auch im Widget „Zusammenfassung“ der Landing Page angezeigt. Der Link führt zur entsprechenden Active IQ-Seite. Auf einer Landing Page „*Storage*“ stellt die Anzahl die Risiken aller zugrunde liegenden Storage Nodes dar.



Active IQ-Seite wird geöffnet

Wenn Sie auf den Link zu einer Active IQ-Seite klicken und Sie derzeit nicht bei Ihrem Active IQ-Konto angemeldet sind, müssen Sie die folgenden Schritte durchführen, um die Active IQ-Seite für den Storage-Node anzuzeigen.

1. Klicken Sie im Widget „Cloud Insights Summary“ (Zusammenfassung) oder in der Risikokabelle auf den Link „Active IQ“.
2. Melden Sie sich bei Ihrem NetApp Support Konto an. Sie werden direkt zur Seite Storage-Node in Active IQ weitergeleitet.

Abfrage nach Risiken

In Cloud Insights können Sie die Spalte **Monitoring.count** einer Speicherabfrage oder Speicherknoten hinzufügen. Wenn das zurückgegebene Ergebnis aus Active IQ-überwachten Storage-Systemen besteht, wird in der Spalte Monitoring.count die Anzahl der Risiken für das Storage-System oder den Node angezeigt.

Dashboards

Sie können Widgets erstellen (z. B. Kreisdiagramm, Tabelle-Widget, Balken, Spalte, Streudiagramm, Und Widgets mit einem Mehrwert) zur Visualisierung der Objektrisiken für Storage- und Storage-Nodes für von Active IQ überwachte NetApp Clustered Data ONTAP Systeme „Objektrisiken“ können in diesen Widgets als

Spalte oder Metrik ausgewählt werden, wobei Storage oder Storage Node das Objekt des Fokus ist.