



Amministrazione e altre attività

Cloud Insights

NetApp
June 28, 2024

Sommario

- Amministrazione e altre attività 1
- API Cloud Insights 1
- Monitoraggio dell'ambiente 12

Amministrazione e altre attività

API Cloud Insights

L'API Cloud Insights consente ai clienti NetApp e ai vendor di software indipendenti (ISV) di integrare Cloud Insights con altre applicazioni, come CMDB o altri sistemi di ticketing.

Tenere presente che le API Cloud Insights sono disponibili in base all'edizione corrente:

Tipo API	Di base	Standard	Premium
Unità di acquisizione	✓	✓	✓
Raccolta di dati	✓	✓	✓
Avvisi		✓	✓
Risorse		✓	✓
Acquisizione dei dati		✓	✓
Gestione dei log		✓	✓

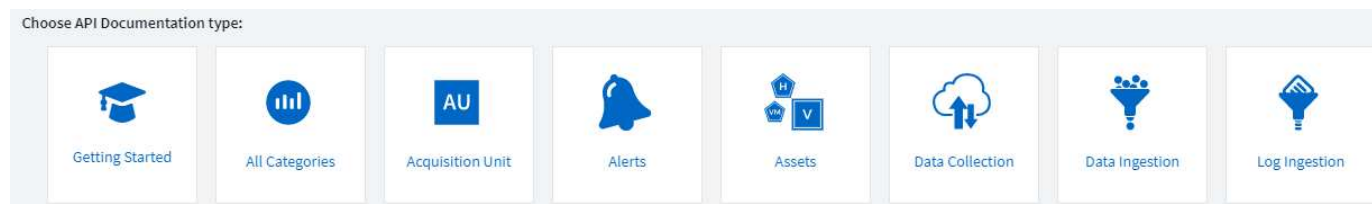
Inoltre, il tuo Cloud Insights "[ruolo del set di funzionalità](#)" Determina le API a cui è possibile accedere. I ruoli utente e ospite hanno meno privilegi rispetto al ruolo Amministratore. Ad esempio, se si ha il ruolo di amministratore in Monitor e Optimize, ma il ruolo di utente in Reporting, è possibile gestire tutti i tipi di API tranne Data Warehouse.

Requisiti per l'accesso API

- Per concedere l'accesso viene utilizzato un modello API Access Token.
- La gestione del token API viene eseguita dagli utenti Cloud Insights con il ruolo di amministratore.

Documentazione API (Swagger)

Le informazioni API più recenti si trovano accedendo a Cloud Insights e accedendo a **Amministratore > accesso API**. Fare clic sul collegamento **documentazione API**.



La documentazione API è basata su Swagger, che fornisce una breve descrizione e informazioni sull'utilizzo dell'API e consente di provarla nel proprio ambiente. A seconda del ruolo dell'utente e/o dell'edizione di Cloud Insights, i tipi di API disponibili possono variare.

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

```
{}
```

Token di accesso API

Prima di utilizzare l'API Cloud Insights, è necessario creare uno o più **token di accesso API**. I token di accesso vengono utilizzati per tipi di API specifici e possono concedere permessi di lettura e/o scrittura. È inoltre possibile impostare la scadenza per ciascun token di accesso. Tutte le API dei tipi specificati sono valide per il token di accesso. Ogni token non contiene un nome utente o una password.

Per creare un token di accesso:

- Fare clic su **Admin > API Access** (Amministratore > accesso API)
- Fare clic su **+token di accesso API**
 - Immettere il nome del token
 - Selezionare i tipi di API
 - Specificare le autorizzazioni concesse per questo accesso API
 - Specificare la scadenza del token



Il token sarà disponibile solo per la copia negli Appunti e il salvataggio durante il processo di creazione. I token non possono essere recuperati dopo la loro creazione, pertanto si consiglia vivamente di copiarli e salvarli in una posizione sicura. Verrà richiesto di fare clic sul pulsante **Copy API Access Token** (Copia token di accesso API) prima di chiudere la schermata di creazione del token.

È possibile disattivare, attivare e revocare i token. È possibile attivare i token disattivati.

I token garantiscono l'accesso generico alle API dal punto di vista del cliente, gestendo l'accesso alle API nell'ambito del proprio tenant. Gli amministratori dei clienti possono concedere e revocare questi token senza il coinvolgimento diretto del personale back-end di Cloud Insights.

L'applicazione riceve un token di accesso dopo che un utente ha autenticato e autorizzato l'accesso, quindi passa il token di accesso come credenziale quando chiama l'API di destinazione. Il token passato informa l'API che la portante del token è stata autorizzata ad accedere all'API ed eseguire azioni specifiche specificate dall'ambito concesso durante l'autorizzazione.

L'intestazione HTTP in cui viene passato il token di accesso è **X-CloudInsights-apiKey**:

Ad esempio, utilizzare quanto segue per recuperare le risorse di storage:

```
curl https://<tenant_host_name>/rest/v1/assets/storages -H 'X-CloudInsights-ApiKey:<API_Access-Token>'
Dove <API_Access-Token> è il token salvato durante la creazione dell'accesso API.
```

Consulta le pagine swagger per esempi specifici dell'API che desideri utilizzare.

Tipo API

L'API Cloud Insights è basata sulle categorie e attualmente contiene i seguenti tipi:

- IL tipo DI ASSET contiene API di risorse, query e ricerca.
 - Asset: Enumerare gli oggetti di primo livello e recuperare un oggetto specifico o una gerarchia di oggetti.
 - Query: Recuperare e gestire le query Cloud Insights.
 - Import (Importa): Consente di importare annotazioni o applicazioni e assegnarle agli oggetti
 - Search (Cerca): Consente di individuare un oggetto specifico senza conoscere l'ID univoco o il nome completo dell'oggetto.
- Il tipo DI RACCOLTA DATI viene utilizzato per recuperare e gestire i data collection.
- Il tipo DI ACQUISIZIONE DEI DATI viene utilizzato per recuperare e gestire i dati di acquisizione e le metriche personalizzate, ad esempio da agenti di Telegraf
- L'ACQUISIZIONE DEI LOG viene utilizzata per recuperare e gestire i dati dei log

Altri tipi e/o API potrebbero diventare disponibili nel tempo. Le informazioni API più recenti sono disponibili in ["Documentazione API Swagger"](#).

Si noti che i tipi di API a cui un utente ha accesso dipendono anche da ["Ruolo dell'utente"](#) Sono presenti in ogni set di funzionalità Cloud Insights (monitoraggio, sicurezza del carico di lavoro, reporting).

Attraversamento dell'inventario

In questa sezione viene descritto come attraversare una gerarchia di oggetti Cloud Insights.

Oggetti di livello superiore

I singoli oggetti vengono identificati nelle richieste tramite URL univoco (chiamato "self" in JSON) e richiedono la conoscenza del tipo di oggetto e dell'ID interno. Per alcuni degli oggetti di primo livello (host, storage e così via), L'API REST fornisce l'accesso all'insieme completo.

Il formato generale di un URL API è:

```
https://<tenant>/rest/v1/<type>/<object>
```

Ad esempio, per recuperare tutti gli storage da un tenant denominato `_mysite.c01.cloudinsights.netapp.com_`, l'URL della richiesta è:

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

Figli e oggetti correlati

Gli oggetti di livello superiore, come Storage, possono essere utilizzati per passare ad altri oggetti figlio e correlati. Ad esempio, per recuperare tutti i dischi per uno storage specifico, concatenare l'URL "self" dello storage con `/disks`, ad esempio:

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

Si espande

Molti comandi API supportano il parametro **espandi**, che fornisce ulteriori dettagli sull'oggetto o sugli URL per gli oggetti correlati.

L'unico parametro di espansione comune è *Expands*. La risposta contiene un elenco di tutte le espansi specifiche disponibili per l'oggetto.

Ad esempio, quando si richiede quanto segue:

```
https://<tenant>/rest/v1/assets/storages/2782?expand=_expands
```

L'API restituisce tutte le espansi disponibili per l'oggetto come segue:

```

{
  "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 Resources"
    },
    "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"
    }
  },
  ".....":

```

Ogni espansione contiene dati, un URL o entrambi. Il parametro `expand` supporta attributi multipli e nidificati, ad esempio:

```
https://<tenant>/rest/v1/assets/storages/2782?expand=performance,storageResources.storage
```

Expand consente di trasferire molti dati correlati in un'unica risposta. NetApp consiglia di non richiedere troppe informazioni contemporaneamente; ciò può causare un peggioramento delle performance.

Per scoraggiarlo, non è possibile espandere le richieste di raccolte di livello superiore. Ad esempio, non è possibile richiedere l'espansione dei dati per tutti gli oggetti di storage contemporaneamente. I client devono recuperare l'elenco di oggetti e scegliere gli oggetti specifici da espandere.

Dati sulle performance

I dati sulle performance vengono raccolti su molti dispositivi come campioni separati. Ogni ora (impostazione predefinita), Cloud Insights aggrega e riepiloga i campioni di performance.

L'API consente di accedere sia ai campioni che ai dati riepilogati. Per un oggetto con dati sulle performance, è disponibile un riepilogo delle performance come `expand=performance`. Le serie temporali della cronologia delle performance sono disponibili attraverso `expand=performance.history` annidato.

Esempi di oggetti dati sulle performance includono:

- StoragePerformance
- StoragePoolPerformance
- Performance di portperformance
- DiskPerformance

Una metrica delle performance ha una descrizione e un tipo e contiene una raccolta di riepiloghi delle performance. Ad esempio, latenza, traffico e velocità.

Un Riepilogo delle performance contiene una descrizione, un'unità, un'ora di inizio del campione, un'ora di fine del campione e un insieme di valori riepilogati (corrente, min, max, media, ecc.) calcolati da un singolo contatore delle performance in un intervallo di tempo (1 ora, 24 ore, 3 giorni e così via).

<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,
      "sum": null,
      "isDownsampled": false
    }
  }
}
```

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

Il dizionario dei dati sulle prestazioni risultante dispone delle seguenti chiavi:

- "Self" è l'URL univoco dell'oggetto

- "cronologia" è l'elenco di coppie di valori di timestamp e mappa dei contatori
- Ogni altra chiave del dizionario ("diskThroughput" e così via) è il nome di una metrica delle performance.

Ogni tipo di oggetto dati sulle performance ha un insieme unico di metriche delle performance. Ad esempio, l'oggetto performance della macchina virtuale supporta "diskThroughput" come metrica delle performance. Ogni metrica di performance supportata è di una determinata "performanceCategory" presentata nel dizionario delle metriche. Cloud Insights supporta diversi tipi di metriche delle performance elencati più avanti in questo documento. Ogni dizionario delle metriche di performance avrà anche il campo "description" (Descrizione) che è una descrizione leggibile di questa metrica di performance e una serie di voci del contatore di riepilogo delle performance.

Il contatore Performance Summary è il riepilogo dei contatori delle performance. Presenta i valori aggregati tipici come min, max e AVG per un contatore e anche l'ultimo valore osservato, l'intervallo di tempo per i dati riepilogati, il tipo di unità per il contatore e le soglie per i dati. Solo le soglie sono facoltative; gli altri attributi sono obbligatori.

Sono disponibili riepiloghi delle performance per i seguenti tipi di contatori:

- Read – Riepilogo per le operazioni di lettura
- Scrittura – Riepilogo per operazioni di scrittura
- Total (totale): Riepilogo di tutte le operazioni. Può essere superiore alla semplice somma di lettura e scrittura; può includere altre operazioni.
- Total Max (massimo totale): Riepilogo di tutte le operazioni. Questo è il valore totale massimo nell'intervallo di tempo specificato.

Metriche delle performance degli oggetti

L'API può restituire metriche dettagliate per gli oggetti nel tuo ambiente, ad esempio:

- Metriche delle performance dello storage come IOPS (numero di richieste di input/output al secondo), latenza o throughput.
- Metriche delle prestazioni dello switch, ad esempio utilizzo del traffico, dati BB Credit Zero o errori delle porte.

Vedere "[Documentazione API Swagger](#)" per informazioni sulle metriche per ciascun tipo di oggetto.

Dati della cronologia delle performance

I dati della cronologia vengono presentati nei dati delle performance come un elenco di coppie di timestamp e mappe dei contatori.

I contatori della cronologia vengono denominati in base al nome dell'oggetto della metrica delle prestazioni. Ad esempio, l'oggetto performance della macchina virtuale supporta "diskThroughput", pertanto la mappa della cronologia conterrà chiavi denominate "diskThroughput.Read", "diskThroughput.write" e "diskThroughput.total".



Timestamp è in formato UNIX Time.

Di seguito viene riportato un esempio di dati JSON relativi alle performance per un disco:

```

"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
    }
  ]
]

```

Oggetti con attributi di capacità

Gli oggetti con attributi di capacità utilizzano tipi di dati di base e CapacityItem per la rappresentazione.

CapacityItem

CapacityItem è una singola unità logica di capacità. Ha "valore" e "highThreshold" in unità definite dal relativo oggetto padre. Supporta inoltre una mappa di dettaglio opzionale che spiega come viene costruito il valore della capacità. Ad esempio, la capacità totale di uno storagePool da 100 TB sarebbe un CapacityItem con un valore di 100. La ripartizione potrebbe indicare 60 TB allocati per "dati" e 40 TB per "snapshot".

Nota

"HighThreshold" rappresenta le soglie definite dal sistema per le metriche corrispondenti, che un client può utilizzare per generare avvisi o segnali visivi su valori che non rientrano negli intervalli configurati accettabili.

Di seguito viene illustrata la capacità di StoragePools con contatori di capacità multipli:

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

Utilizzo di Search per cercare oggetti

L'API di ricerca è un semplice punto di accesso al sistema. L'unico parametro di input per l'API è una stringa in formato libero e il JSON risultante contiene un elenco categorizzato di risultati. I tipi sono diversi tipi di risorse dall'inventario, ad esempio storage, host, datastore e così via. Ogni tipo contiene un elenco di oggetti del tipo che corrispondono ai criteri di ricerca.



Cloud Insights è una soluzione estensibile (ampiamente aperta) che consente integrazioni con sistemi di orchestrazione, gestione aziendale, controllo delle modifiche e ticketing di terze parti, oltre a integrazioni CMDB personalizzate.

L'API RESTful di Cloud Insight è un punto primario di integrazione che consente uno spostamento semplice ed efficace dei dati e consente agli utenti di ottenere un accesso perfetto ai propri dati.

Disattivazione o revoca di un token API

Per disattivare temporaneamente un token API, nella pagina di elenco dei token API, fare clic sul menu "tre punti" dell'API e selezionare *Disable*. Puoi riattivare il token in qualsiasi momento utilizzando lo stesso menu e selezionando *Enable*.

Per rimuovere in modo permanente un token API, selezionare "revoca" dal menu. Non è possibile riattivare un token revocato; è necessario creare un nuovo token.

<input type="checkbox"/>	Name ↑	Description	Token	API Type	Permission	Expires On	Status
<input type="checkbox"/>	10.197.120.70		...RpTMJ4	Data Ingestion	Write Only	11/06/2021	Expired 
	22		...nUBDhe	Data Ingestion	Write Only	06/17/2022	Enabled
	22TOKEN2010560		...8gXq7K	All Categories	Read Only	06/17/2022	Enabled
	ActiveQ_POC_token		...scmES6	Data Ingestion	Read/Write	11/12/2021	Expired 

- Disable
- Edit Description
- Revoke

Rotazione dei token di accesso API scaduti

I token di accesso API hanno una data di scadenza. Quando un token di accesso API scade, gli utenti devono generare un nuovo token (di tipo *Data Ingestion* con permessi di lettura/scrittura) e riconfigurare Telegraf per utilizzare il token appena generato invece del token scaduto. La procedura riportata di seguito illustra in dettaglio la procedura da seguire.

Kubernetes

Si noti che questi comandi utilizzano lo spazio dei nomi predefinito "netapp-monitoring". Se è stato impostato uno spazio dei nomi personalizzato, sostituire tale spazio dei nomi in questi e in tutti i comandi e file successivi.

Nota: Se si dispone dell'ultimo NetApp Kubernetes Monitoring Operator installato e si utilizza un token di accesso API rinnovabile, i token in scadenza verranno sostituiti automaticamente da token di accesso API nuovi/aggiornati. Non è necessario eseguire i passaggi manuali elencati di seguito.

- Modifica l'operatore di monitoraggio NetApp Kubernetes.

```
kubectl -n netapp-monitoring edit agent agent-monitoring-netapp
* Modificare il valore _spec.output-sink.api-key_, sostituendo il vecchio token API con il nuovo token API.
```

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

RHEL/CentOS e Debian/Ubuntu

- Modificare i file di configurazione di Telegraf e sostituire tutte le istanze del vecchio token API con il nuovo token API.

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

```
sudo systemctl restart telegraf
```

Windows

- Per ogni file di configurazione di Telegraf in *C: File di programma telegraf telegraf.d*, sostituire tutte le istanze del vecchio token API con il nuovo token API.

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

- Riavviare Telegraf.

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

Monitoraggio dell'ambiente

Controllo

Per identificare le modifiche previste (per il monitoraggio) o impreviste (per la risoluzione dei problemi), è possibile visualizzare un audit trail degli eventi del sistema Cloud Insights e delle attività dell'utente.

Visualizzazione degli eventi controllati

Per visualizzare la pagina Audit, fare clic su **Admin > Audit** nel menu. Viene visualizzata la pagina Audit, che fornisce i seguenti dettagli per ciascuna voce di audit:

- **Ora** - Data e ora dell'evento o dell'attività
- **Utente** - l'utente che ha avviato l'attività
- **Ruolo** - ruolo dell'utente in Cloud Insights (guest, utente, amministratore)
- **IP** - l'indirizzo IP associato all'evento
- **Azione** - tipo di attività, ad esempio Login, Crea, Aggiorna
- **Categoria** - la categoria di attività
- **Dettagli** - Dettagli dell'attività

Visualizzazione delle voci di audit

Esistono diversi modi per visualizzare le voci di audit:

- È possibile visualizzare le voci di audit scegliendo un periodo di tempo specifico (1 ora, 24 ore, 3 giorni, ecc.).
- È possibile modificare l'ordinamento delle voci in crescente (freccia su) o decrescente (freccia giù) facendo clic sulla freccia nell'intestazione della colonna.

Per impostazione predefinita, la tabella visualizza le voci in ordine decrescente.

- È possibile utilizzare i campi di filtro per visualizzare solo le voci desiderate nella tabella. Fare clic sul pulsante [+] per aggiungere altri filtri.

The screenshot shows a filter bar at the top with three active filters: 'Category Management', 'User Tony', and 'Action Any'. Below the filter bar, a table titled 'Audit (15)' is visible. The table has columns for 'Time', 'User', 'Role', and 'IP'. A dropdown menu is open over the 'Action' filter, showing a list of actions with checkboxes: 'Create' (checked), 'Delete' (checked), 'Update' (checked), 'Enable' (unchecked), 'Disable' (unchecked), and 'Accept' (unchecked).

Ulteriori informazioni sul filtraggio

Per perfezionare il filtro, è possibile utilizzare una delle seguenti opzioni:

Filtro	Che cosa fa	Esempio	Risultato
* (Asterisco)	consente di cercare tutto	vol*rhel	restituisce tutte le risorse che iniziano con "vol" e terminano con "rhel"
? (punto interrogativo)	consente di cercare un numero specifico di caratteri	BOS-PRD??-S12	Restituisce BOS-PRD 12 -S12, BOS-PRD 23 -S12 e così via
OPPURE	consente di specificare più entità	FAS2240, CX600 O FAS3270	Restituisce FAS2440, CX600 o FAS3270
NO	consente di escludere il testo dai risultati della ricerca	NON EMC*	Restituisce tutto ciò che non inizia con "EMC"
<i>Nessuno</i>	Cerca vuoto/NULL/None in qualsiasi campo dove selezionato	<i>Nessuno</i>	restituisce risultati in cui il campo di destinazione non è vuoto
Non *	Come per <i>None</i> , ma puoi anche utilizzare questo modulo per cercare i valori NULL nei campi <i>text-only</i>	Non *	restituisce risultati in cui il campo di destinazione non è vuoto.
""	ricerca una corrispondenza esatta	"NetApp""	Restituisce i risultati contenenti la stringa letterale esatta <i>NetApp</i> *

Se racchiudi una stringa di filtro tra virgolette doppie, Insight tratta tutto ciò che va dalla prima all'ultima quotazione come una corrispondenza esatta. Tutti i caratteri speciali o gli operatori all'interno delle virgolette saranno trattati come valori letterali. Ad esempio, il filtraggio per ""* restituirà risultati che sono un asterisco letterale; in questo caso, l'asterisco non verrà trattato come carattere jolly. Gli operatori O e NON verranno

trattati come stringhe letterali se racchiusi tra virgolette doppie.

Eventi e azioni verificati

Gli eventi e le azioni controllati da Cloud Insights possono essere classificati nelle seguenti aree:

- **Account utente:** Accesso, disconnessione, modifica del ruolo, ecc.

Esempio: *Utente **Tony Lavoie** collegato da **10.1.120.15**, agente utente **Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36**, metodo(i) di login **BlueXP Portal Login***

- **Acquisition Unit** (unità di acquisizione): Creare, eliminare, ecc.

Esempio: *Unità di acquisizione **AU-Boston-1** rimossa.*

- **Data Collector:** Aggiungere, rimuovere, modificare, posticipare/riprendere, modificare l'unità di acquisizione, avvio/arresto, ecc.

Esempio: *Origine dati **laboratorio FlexPod** rimosso, vendor **NetApp**, modello **Software di gestione dati ONTAP**, ip **192.168.106.5**.*

- **Applicazione:** Aggiungere, assegnare a un oggetto, rimuovere, ecc.

Esempio: *Volume interno **ocisedev:t1appSVM01:t1appFlexVol01** aggiunto all'applicazione **Test App**.*

- **Annotation:** Aggiunta, assegnazione, rimozione, azioni delle regole di annotazione, modifiche dei valori delle annotazioni, ecc.

Esempio: *Valore di annotazione **Boston** aggiunto al tipo di annotazione **SalesOffice**.*

- **Query:** Aggiungere, rimuovere, ecc.

Esempio: *Aggiunta di **_query query di vendita TL**.*

- **Monitor:** Aggiungere, rimuovere, ecc.

Esempio: *Monitor **AGGR Size - Avvisi ci Notifications Dev** aggiornato*


- **Notifica:** Modifica email, ecc.

Esempio: *Creazione del destinatario **ci-alerts-notifications-dl***

Esportazione di eventi di audit

È possibile esportare i risultati della visualizzazione Audit in un file .CSV, che consente di analizzare i dati o importarli in un'altra applicazione.

Fasi

1. Nella pagina Audit, impostare l'intervallo di tempo desiderato e i filtri desiderati. Cloud Insights esporterà solo le voci di audit che corrispondono al filtro e all'intervallo di tempo impostati.
2. Fare clic sul pulsante *Export*  nella parte superiore destra della tabella.

Gli eventi di audit visualizzati verranno esportati in un file .CSV, fino a un massimo di 10,000 righe.

Conservazione dei dati di audit

La quantità di tempo in cui Cloud Insights conserva i dati di audit si basa sull'edizione:

- Basic Edition: I dati di audit vengono conservati per 30 giorni
- Edizioni Standard e Premium: I dati di audit vengono conservati per 1 anno più 1 giorno

Le voci di audit precedenti al tempo di conservazione vengono eliminate automaticamente. Non è richiesta alcuna interazione da parte dell'utente.

Risoluzione dei problemi

Qui troverai suggerimenti per la risoluzione dei problemi con Audit.

Problema:	Provare questo:
Vengono visualizzati messaggi di audit che indicano che un monitor è stato esportato.	L'esportazione di una configurazione di monitor personalizzata viene generalmente utilizzata dai tecnici NetApp durante lo sviluppo e il test delle nuove funzionalità. Se non si prevede di visualizzare questo messaggio, esaminare le azioni dell'utente indicato nell'azione verificata o contattare il supporto.

Active IQ

NetApp "Active IQ" Offre una serie di visualizzazioni, analytics e altri servizi di supporto ai clienti NetApp per i loro sistemi hardware/software. I dati riportati da Active IQ possono migliorare la risoluzione dei problemi di sistema e fornire informazioni sull'ottimizzazione e sull'analisi predittiva dei dispositivi.



ActiveIQ non è disponibile nell'edizione federale di Cloud Insights.

Cloud Insights raccoglie i **rischi** per qualsiasi sistema storage NetApp Clustered Data ONTAP monitorato e segnalato da Active IQ. I rischi segnalati per i sistemi storage vengono raccolti automaticamente da Cloud Insights nell'ambito della raccolta dei dati da tali dispositivi. È necessario aggiungere il data collector appropriato a Cloud Insights per raccogliere le informazioni sui rischi Active IQ.

Cloud Insights non mostra i dati di rischio per i sistemi ONTAP che non sono monitorati e segnalati da Active IQ.

I rischi riportati sono riportati in Cloud Insights nelle pagine di destinazione delle risorse di *storage* e *storage node*, nella tabella "rischi". La tabella mostra i dettagli del rischio, la categoria di rischio e il potenziale impatto del rischio e fornisce anche un link alla pagina Active IQ che riepiloga tutti i rischi per il nodo di storage (è richiesto l'accesso all'account di supporto NetApp).

Risks				
108 items found Filter...				
Object ↑	Risk Detail	Category	Potential Impact	Source
tawny01	The following certificates have expired or are expiring within 30 days: Expired: 53CF9553, 53C504D4, 53D671B4, Expiring within 30 days: None	System Configuration	Clients may not be able to connect to the cluster over secure (SSL based) protocols.	Active IQ ↗
tawny01	None of the NIS servers configured for SVM(s) tawny_svm_oci_markic can be contacted.	CIFS Protocol	Potential CIFS and NFS outages may occur.	Active IQ ↗
tawny01	ONTAP version 8.3.2 has entered the Self-Service Support period.	ONTAP	Self-Service Support is the time period where NetApp does not provide support for a version of a software product, but related documentation is still available on the NetApp Support Site.	Active IQ ↗

Il numero di rischi segnalati viene visualizzato anche nel widget Riepilogo della landing page, con un link alla pagina Active IQ appropriata. In una landing page di *storage*, il conteggio è una somma dei rischi di tutti i nodi di storage sottostanti.

Storage Summary

<p>Model: FAS6210</p> <p>Vendor: NetApp</p> <p>Family: FAS6200</p> <p>Serial Number: 1-80-000013</p> <p>IP: 10.197.143.25</p>	<p>Microcode Version: 8.3.2 clustered Data ONTAP</p> <p>Raw Capacity: 80,024.3 GB</p> <p>Latency - Total: 0.77 ms</p> <p>IOPS - Total: 1,819.19 IO/s</p> <p>Throughput - Total: 41.69 MB/s</p>	<p>Management: HTTPS://10.197.143.25:443</p> <p>FC Fabrics Connected: 0</p> <p>Performance Policies:</p> <div style="border: 2px solid blue; border-radius: 15px; padding: 5px; display: inline-block;"> <p>Risks: 108 risks detected by Active IQ ↗</p> </div>
--	---	---

Apertura della pagina Active IQ

Quando si fa clic sul collegamento a una pagina Active IQ, se non si è ancora effettuato l'accesso all'account Active IQ, attenersi alla seguente procedura per visualizzare la pagina Active IQ relativa al nodo di storage.

1. Nel widget Riepilogo Cloud Insights o nella tabella rischi, fai clic sul link "Active IQ".
2. Accedi al tuo account NetApp Support. Viene visualizzata direttamente la pagina del nodo di storage in Active IQ.

Query per i rischi

In Cloud Insights, è possibile aggiungere la colonna **monitoring.count** a una query del nodo storage o storage. Se il risultato restituito include sistemi storage monitorati con Active IQ, la colonna monitoring.count visualizza il numero di rischi per il sistema o il nodo storage.

Dashboard

È possibile creare widget (ad esempio grafico a torta, widget tabella, barra, colonna, grafico a dispersione, E single value widgets) per visualizzare i rischi di oggetti per i nodi storage e storage per i sistemi NetApp Clustered Data ONTAP monitorati da Active IQ. È possibile selezionare "rischi oggetto" come colonna o metrica in questi widget, dove Storage o Storage Node sono l'oggetto di interesse.

Object Risks by Array

12 items found

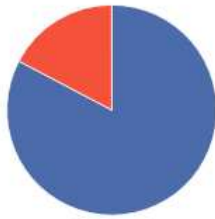
Name	Object Risks ↓
tawny	110
rtp-sa-select01	23
rtp-sa-cl02	N/A
rtp-sa-cl07	N/A
oci-phonehome	N/A
durlabprdfs01	N/A
oci-3070-01	N/A

Object Risks by Node

25 items found

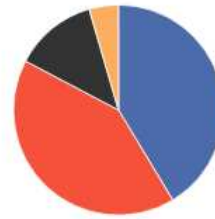
Name	Object Risks ↓
tawny02	55
tawny01	55
rtp-sa-select01-1	17
rtp-sa-select01-2	6
tnode02	N/A
rtp-sa-cl06-01	N/A
rtp-sa-cl06-02	N/A

Object Risks by Storage



■ tawny ■ rtp-sa-select01

Object Risks by Storage Node



■ tawny02 ■ tawny01 ■ rtp-sa-select01-1 ■ rtp-sa-select01-2

Total Storage Risks

133.00
Object Risks

Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.