



Data Collector Reference - Dienste Cloud Insights

NetApp
March 30, 2023

This PDF was generated from https://docs.netapp.com/de-de/cloudinsights/task_config_telegraf_node.html on March 30, 2023. Always check docs.netapp.com for the latest.

Inhaltsverzeichnis

- Data Collector Reference - Dienste 1
 - Erfassung Von Node-Daten 1
 - ActiveMQ Data Collector 3
 - Apache Data Collector 4
 - Consul Data Collector 7
 - Couchbase Data Collector 8
 - CouchDB Data Collector 9
 - Docker Data Collector 10
 - Elasticsearch Data Collector 17
 - Flik Data Collector 20
 - Hadoop Data Collector 26
 - HAProxy Data Collector 35
 - JVM Data Collector 41
 - Kafka Data Collector 44
 - Kibana Data Collector 48
 - Memcached Data Collector 49
 - MongoDB Data Collector 51
 - MySQL Data Collector 51
 - Netstat Data Collector 55
 - Nginx Data Collector 55
 - PostgreSQL Data Collector 56
 - Puppet Agent Data Collector 57
 - Redis Data Collector 59

Data Collector Reference - Dienste

Erfassung Von Node-Daten

Cloud Insights sammelt Kennzahlen von dem Knoten, auf dem Sie einen Agent installieren.

Installation

1. Wählen Sie unter **Admin > Data Collectors** ein Betriebssystem/eine Plattform aus. Beachten Sie, dass durch die Installation eines Datensammlers für die Integration (Kubernetes, Docker, Apache usw.) auch die Erfassung von Node-Daten konfiguriert wird.
2. Befolgen Sie die Anweisungen, um den Agenten zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.

Objekte und Zähler

Die folgenden Objekte und ihre Zähler werden als Node-Kennzahlen erfasst:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Knoten Dateisystem	Node-UUID-Gerätetyp	Node-IP Node-Name Node OS-Modus	Freie Inodes Free Inodes Total Inodes Used Total Used Total Used Total Used
Node-Festplatte	Node-UUID-Festplatte	Node-IP Node-Name Node OS	I/O-Zeit insgesamt IOPS in Bearbeitung Lesen von Bytes (pro s) Lesezeit insgesamt Lesevorgänge (pro s) gewichtete I/O-Zeit insgesamt Schreibbyte (pro s) Schreibzeit Gesamtzahl Schreibvorgänge (pro s) Aktuelle Festplattenwarteschlange Länge Schreibzeit I/O-Zeit
Node-CPU	Node-UUID-CPU	Node-IP Node-Name Node OS	System CPU Usage User CPU Usage Idle CPU Usage Prozessor CPU Usage Interrupt CPU Usage DPC CPU Usage

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Knoten	Node-UUID	Node-IP Node-Name Node OS	Kernel Boot Time Kernel Context Switches (per sec) Kernel Entropy Available Kernel Interrupts (per sec) Kernel processes Forked (per sec) Arbeitsspeicher Aktiver Speicher Verfügbar Gesamter Verfügbarer Speicher Gepufferter Speicher Im Cache Speicherlimit Speicher Speicher Bereitgestellt Als Speicher Schmutziger Speicher Freier Speicher Hoher Freier Speicher Hoher Gesamtspeicher Riesige Seitengröße Speicher Riesige Seiten Freier Speicher Riesige Seiten Gesamt Speicher Niedriger Freier Speicher Niedriger Speicher Gemappter Speicher Seitentabellen Speicher Gemeinsam Genutzter Speicher Slab Speicher Austausch Gecachten Speicher Austausch Freier Speicher Austausch Gesamt Speicher Verwendeter Gesamt- Speicher Verwendeter Speicher Vmalloc Chunk Speicher Vmalloc Gesamt-Speicher Vmalloc Verwendeter Speicher Wired Memory Writeback Total Memory Writeback Tmp Speicher Cache Fehler Speicheranforderung Null Fehler Speicherseiten Fehler Speicherseiten Fehler Speicherseiten- Speicher-Seiten-Speicher Nicht Gepageter Speicher Paged Memory Cache Core Memory Standby Cache Normaler Speicher Standby Cache Reserve Memory Transition Fehler Prozesse Blockierte Prozesse Dead Processes

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Node-Netzwerk	UUID der Netzwerkschnittstelle-Node	Node Name Node-IP Node OS	Bytes Empfangene Bytes Gesendete Pakete Ausgehende Pakete Ausgehende Pakete Ausgehende Pakete Ausgehende Pakete Paketfehler Empfangen Pakete Empfangene Fehler Pakete Empfangene Pakete Empfangene Pakete Empfangen Pakete

Einrichtung

Informationen zur Einrichtung und Fehlerbehebung finden Sie im ["Konfigurieren eines Agenten"](#) Seite.

MacOS-Speicherauslastung

Cloud Insights (via Telegraf) und macOS berichten über verschiedene Nummern für die Speichernutzung. Sowohl Telegraf als auch der Mac-Aktivitätsmonitor verwenden Metriken, die von `vm_stat` gesammelt wurden, jedoch wird die Gesamtspeichernutzung jeweils unterschiedlich berechnet.

Telegraf berechnet *Memory Used Total* wie folgt:

```
Memory Used Total = Memory Total - Memory Available Total
Wobei _Memory Available Total_ aus der Summe von „Pages free“ und „Pages inactive“ in _vm_stat_ abgeleitet wird.
```

Der Mac-Aktivitätsmonitor berechnet hingegen den verwendeten Speicher wie folgt:

```
Memory Used = App Memory + Wired Memory + Compressed
Wo?
```

- *App Memory* wird aus dem Unterschied zwischen „Anonymen Seiten“ und „Seiten auffindbar“ in `vm_stat`,
- *Wired Memory* wird von „Pages Wired Down“ in `vm_stat`, und abgeleitet
- *Compressed* wird aus „Seiten, die durch Kompressor belegt sind“ in `vm_stat` abgeleitet.

ActiveMQ Data Collector

Cloud Insights verwendet diesen Datensammler, um Metriken aus ActiveMQ zu erfassen.

Installation

1. Klicken Sie in **Admin > Data Collectors** auf **+Data Collector**. Wählen Sie unter **Services** ActiveMQ.

Wählen Sie das Betriebssystem oder die Plattform aus, auf dem der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agent für die Sammlung installiert haben oder einen Agent für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das zu erweitern "[Agenten-Installation](#)" Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel für diesen Datensammler aus. Sie können einen neuen Agent-Zugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agent Access Key** klicken. Best Practice: Verwenden Sie einen anderen Agent-Zugriffsschlüssel nur, wenn Sie Datensammler gruppieren möchten, zum Beispiel nach Betriebssystem/Plattform.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.

[ActiveMQ-Konfiguration]

Einrichtung

Informationen finden Sie unter "[ActiveMQ-Dokumentation](#)"

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
ActiveMQ-Warteschlange	Namespace Queue Port Server	Node Name Node-IP-Node-UUID	Anzahl Der Warteschlange Anzahl Der Kunden Anzahl Der Ausgleiche Anzahl Warteschlange Größe
ActiveMQ-Abonnenten	Namespace für Client-ID-Verbindungs-ID-Port-Server	Ist Active Destination Node Name Node IP Node UUID Node OS Selector Subscription	Anzahl Der Entsandten Absendete Warteschlange Anzahl Der Abgesandten Warteschlange Größe Anzahl Der Warteschlange Anzahl Der Ausstehenden Warteschlange Größe
ActiveMQ-Thema	Thema Port Server Namespace	Node Name Node-IP-Node-UUID-Node-OS	Anzahl Der Ausgleichen Anzahl Der Verbraucher Größe Der Anzahl Der Warteschlangen

Fehlerbehebung

Weitere Informationen finden Sie im "[Unterstützung](#)" Seite.

Apache Data Collector

Dieser Datensammler ermöglicht die Erfassung von Daten von Apache-Servern in Ihrer Umgebung.

Voraussetzungen

- Sie müssen Ihren Apache HTTP Server einrichten und ordnungsgemäß ausführen lassen
- Sie müssen über sudo- oder Administratorberechtigungen auf Ihrem Agent-Host/VM verfügen
- In der Regel ist das Apache *mod_Status*-Modul so konfiguriert, dass eine Seite am Speicherort `'/Server-Status?Auto'` des Apache-Servers angezeigt wird. Die Option *ExtendedStatus* muss aktiviert sein, um alle verfügbaren Felder zu erfassen. Informationen zum Konfigurieren des Servers finden Sie in der Apache-Moduldokumentation: https://httpd.apache.org/docs/2.4/mod/mod_status.html#enable

Installation

1. Klicken Sie in **Admin > Data Collectors** auf **+Data Collector**. Wählen Sie unter **Services** Apache aus.

Wählen Sie das Betriebssystem oder die Plattform aus, auf dem der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agent für die Sammlung installiert haben oder einen Agent für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das zu erweitern "[Agenten-Installation](#)" Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel für diesen Datensammler aus. Sie können einen neuen Agent-Zugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agent Access Key** klicken. Best Practice: Verwenden Sie einen anderen Agent-Zugriffsschlüssel nur, wenn Sie Datensammler gruppieren möchten, zum Beispiel nach Betriebssystem/Plattform.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.

[Apache-Konfiguration]

Einrichtung

Das Telegraf-Plugin für Apache's HTTP Server setzt auf das 'mod_Status'-Modul, um aktiviert zu werden. Wenn diese Option aktiviert ist, wird Apache HTTP Server einen HTML-Endpunkt anzeigen, der in Ihrem Browser angezeigt oder für die Extraktion des Status aller Apache HTTP Server-Konfigurationen gepatzt werden kann.

Kompatibilität:

Die Konfiguration wurde gegen Apache HTTP Server Version 2.4.38 entwickelt.

Aktivieren von mod_Status:

Das Aktivieren und Bereitstellen der 'mod_Status'-Module umfasst zwei Schritte:

- Modul wird aktivieren
- Legen Sie Statistiken aus dem Modul fest

Modul aktivieren:

Das Laden von Modulen wird durch die Konfigurationsdatei unter `'/usr/local/apache/conf/httpd.conf'` gesteuert. Bearbeiten Sie die config-Datei und heben Sie die folgenden Zeilen aus:

```
LoadModule status_module modules/mod_status.so
Include conf/extra/httpd-info.conf
```

Statistiken aus dem Modul offenlegen:

Die Offenlegung von 'mod_Status' wird durch die Konfigurationsdatei unter '/usr/local/apache2/conf/extra/httpd-info.conf' gesteuert. Stellen Sie sicher, dass Sie in dieser Konfigurationsdatei Folgendes haben (mindestens sind weitere Richtlinien vorhanden):

```
# Allow server status reports generated by mod_status,
# with the URL of http://servername/server-status
<Location /server-status>
    SetHandler server-status
</Location>

#
# ExtendedStatus controls whether Apache will generate "full" status
# information (ExtendedStatus On) or just basic information
(ExtendedStatus
# Off) when the "server-status" handler is called. The default is Off.
#
ExtendedStatus On
```

Detaillierte Anweisungen zum Modul „MOD_Status“ finden Sie im ["Apache-Dokumentation"](#)

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Apache	Namespace-Server	Node-IP-Knotenname-Port-Parent Server-Konfiguration der übergeordnete Server-Generation der MPM-Generation wird angehalten	Beschäftigte Arbeiter Bytes pro Anfrage Bytes pro Sekunde CPU Kinder System CPU Kinder Benutzer CPU Last CPU System CPU System CPU Benutzer asynchrone Verbindungen Schließen Asynchronous Connections am Leben Asynchronous Connections Writing connections Total Duration per Request Idle Workers Load Average (Last 1m) Load Average (Last 15m) Load Average (Last Average (Last 5m) Prozesse Anfragen pro Sekunde Gesamtzugriff Gesamtdauer Gesamtdauer KBytes Scoreboard schließen Scoreboard DNS Lookups Scoreboard abschließen Scoreboard-Idle Cleanup Scoreboard halten am Leben Scoreboard Logging Scoreboard öffnen Scoreboard lesen Scoreboard senden Scoreboard Starting Scoreboard warten

Fehlerbehebung

Weitere Informationen finden Sie im ["Unterstützung"](#) Seite.

Consul Data Collector

Cloud Insights verwendet diesen Datensammler, um Metriken von Consul zu erfassen.

Installation

1. Klicken Sie in **Admin > Data Collectors** auf **+Data Collector**. Wählen Sie unter **Services** die Option **Konsul**.

Wenn Sie keinen Agenten für die Sammlung konfiguriert haben, werden Sie aufgefordert ["Installieren Sie einen Agenten"](#) Ihrer Umgebung zu unterstützen.

Wenn Sie bereits einen Agenten konfiguriert haben, wählen Sie das entsprechende Betriebssystem oder

die entsprechende Plattform aus, und klicken Sie auf **Weiter**.

2. Befolgen Sie die Anweisungen auf dem Bildschirm Consul Configuration, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.

Einrichtung

Informationen finden Sie unter "[Dokumentation für Consul](#)".

Objekte und Zähler für Consul

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Konsul	Namespace-ID-Service-Node prüfen	Node-IP Node OS Node UUID Node Name Service Name Check Name Service Service ID Status	Warnung Bei Kritischem Durchgang

Fehlerbehebung

Weitere Informationen finden Sie im "[Unterstützung](#)" Seite.

Couchbase Data Collector

Cloud Insights verwendet diese Datensammlung, um die Kennzahlen von Couchbase zu erfassen.

Installation

1. Klicken Sie in **Admin > Data Collectors** auf **+Data Collector**. Wählen Sie unter **Services** die Option Couchbase.

Wählen Sie das Betriebssystem oder die Plattform aus, auf dem der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agent für die Sammlung installiert haben oder einen Agent für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das zu erweitern "[Agenten-Installation](#)" Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel für diesen Datensammler aus. Sie können einen neuen Agent-Zugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agent Access Key** klicken. Best Practice: Verwenden Sie einen anderen Agent-Zugriffsschlüssel nur, wenn Sie Datensammler gruppieren möchten, zum Beispiel nach Betriebssystem/Plattform.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.

[Konfiguration von Couchbase]

Einrichtung

Informationen finden Sie unter ["Couchbase Dokumentation"](#).

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Couchbase Node	Namespace Cluster Couchbase Node- Hostname	Node Name Node-IP	Speicher Insgesamt
Couchbase Bucket	Namespace-Bucket- Cluster	Node Name Node-IP	Daten Verwendete Daten Abrufen Verwendete Elemente Anzahl Verwendete Elemente Speicher Verwendete Operationen Pro Sekunde Kontingent Verwendet

Fehlerbehebung

Weitere Informationen finden Sie im ["Unterstützung"](#) Seite.

CouchDB Data Collector

Cloud Insights verwendet diesen Datensammler, um Metriken von CouchDB zu sammeln.

Installation

1. Klicken Sie in **Admin > Data Collectors** auf **+Data Collector**. Wählen Sie unter **Services** CouchDB.

Wählen Sie das Betriebssystem oder die Plattform aus, auf dem der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agent für die Sammlung installiert haben oder einen Agent für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das zu erweitern ["Agenten-Installation"](#) Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel für diesen Datensammler aus. Sie können einen neuen Agent-Zugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agent Access Key** klicken. Best Practice: Verwenden Sie einen anderen Agent-Zugriffsschlüssel nur, wenn Sie Datensammler gruppieren möchten, zum Beispiel nach Betriebssystem/Plattform.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.

[Konfiguration von CouchDB]

Einrichtung

Informationen finden Sie unter ["CouchDB-Dokumentation"](#).

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
CouchDB	Namespace-Server	Node Name Node-IP	Authentifizierung Cache Treffer Authentifizierung Cache Fräulein Datenbank liest Datenbank schreibt Datenbanken Open OS Files Max Anfrageszeit Min Anfrageszeit httpd Request Methoden httpd Request Methoden httpd Request löschen httpd Request Methods Get httpd Request Methods Head httpd Request Methods Post httpd Request Methods Put Status Codes 200 Status Codes 201 Statuscodes 202 Statuscodes 301 Statuscodes 304 Statuscodes 400 Statuscodes 401 Statuscodes 403 Statuscodes 404 Statuscodes 405 Statuscodes 409 Statuscodes 412 Statuscodes 500

Fehlerbehebung

Weitere Informationen finden Sie im ["Unterstützung"](#) Seite.

Docker Data Collector

Cloud Insights verwendet diese Datenerfassung zum Erfassen von Kennzahlen aus Docker.

Installation

1. Klicken Sie in **Admin > Data Collectors** auf **+Data Collector**. Wählen Sie unter **Services** Docker aus.

Wenn Sie keinen Agenten für die Sammlung konfiguriert haben, werden Sie aufgefordert ["Installieren Sie einen Agenten"](#) Ihrer Umgebung zu unterstützen.

Wenn Sie bereits einen Agenten konfiguriert haben, wählen Sie das entsprechende Betriebssystem oder die entsprechende Plattform aus, und klicken Sie auf **Weiter**.

2. Befolgen Sie die Anweisungen im Bildschirm Docker-Konfiguration, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.

[Docker-Konfiguration]

Einrichtung

Das Telegraf-Input-Plug-in für Docker erfasst Kennzahlen über einen bestimmten UNIX-Socket oder einen TCP-Endpunkt.

Kompatibilität

Die Konfiguration wurde mit Docker Version 1.12.6 entwickelt.

Einrichtung

Zugriff auf Docker über einen UNIX-Socket

Wenn der Telegraf-Agent auf bareMetal läuft, fügen Sie den telegraf Unix-Benutzer zur Docker Unix-Gruppe hinzu, indem Sie Folgendes ausführen:

```
sudo usermod -aG docker telegraf
```

Wenn der Telegraf-Agent in einem Kubernetes Pod ausgeführt wird, legen Sie den Docker Unix-Socket offen, indem Sie den Socket als Volume in den POD einbilden und das Volume dann in /var/run/docker.sock mounten. Fügen Sie zum Beispiel der PodSpec Folgendes hinzu:

```
volumes:  
  ...  
  - name: docker-sock  
    hostPath:  
    path: /var/run/docker.sock  
    type: File
```

Fügen Sie dann dem Container Folgendes hinzu:

```
volumeMounts:  
  ...  
  - name: docker-sock  
    mountPath: /var/run/docker.sock
```

Beachten Sie, dass sich das für die Kubernetes-Plattform bereitgestellte Cloud Insights-Installationsprogramm automatisch um diese Zuordnung kümmert.

Zugriff auf Docker über einen TCP-Endpunkt

Docker verwendet standardmäßig Port 2375 für unverschlüsselte Zugriffe und Port 2376 für verschlüsselten Zugriff.

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Docker Engine	Docker Engine Für Namespace	Node Name Node-IP-Node-UUID Node OS Kubernetes Cluster Docker-Versionseinheit	Speichercontainer Container verwendete Container ausgeführt Container gestoppt CPUs Gehroutinen Bilder Listener Ereignisse verwendete Datei Deskriptoren Daten verfügbar Daten insgesamt verwendete Metadaten Verfügbare Metadaten insgesamt verwendete Pool Blocksize

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Docker Container	Namespace Container- Name Docker Engine	Kubernetes-Container- Hash Kubernetes- Container-Ports Kubernetes-Container Restart Anzahl Kubernetes-Container- Ende Meldungspfad Kubernetes Container- Beendigung Meldungsrichtlinie Kubernetes Pod Kulanzzeit Container- Image Container-Status Container-Version Node- Name Kubernetes Container-Log-Pfad Kubernetes Container- Name Kubernetes Docker-Typ Kubernetes Pod Name Kubernetes Namespace Kubernetes Pod UID Kubernetes Sandbox ID Node IP Node UUID Docker Version Kubernetes IO Config Kubernetes IO- Konfiguration gesehen Kubernetes IO- Konfiguration Quelle OpenShift IO SCC Kubernetes Beschreibung Kubernetes Anzeigename OpenShift Tags Kompose Service Pod Vorlage Hash Controller Revision Hash Pod Vorlage Erstellung Lizenz Schema Build Date Schema Lizenz Schema Name Schema URL Schema VCS URL Schema Vendor Schema Version Schema Schema Schema Version Maintainer Customer Pod Kubernetes StatefulSet Pod Name Tenant WebConsole Architektur autoritäre Quelle URL Build Datum RH Build Host RH Component Distribution Scope Installation Release Run Zusammenfassung Uninstall Ref Type Vendor Version Health Status	Speicher Aktiv Anonymer Speicher Aktiv Speicher Cache Hierarchischer Grenzwert Speicher Inaktiver Anonymer Speicher Inaktiver Speicher Speicherlimit Arbeitsspeicher Gemappter Speicher Max Nutzung Speicherseitenfehler Speicherseite Hauptfehler Speicher Im Speicher Ausgepeitet Speicher Resident Set Größe Speicher Resident Set Größe Riesige Speicher Gesamt Aktiv Anonymer Speicher Gesamt Active File Memory Gesamt Cache Speicher Inaktiver Anonymer Speicher Gesamt Inaktiver Speicher Gesamt Mapped File Memory Total Page Fault Memory Total Page Major Fehler Memory Total Paged In Memory Total Paged Out Memory Total Resident Set Größe Speicher Gesamt Resident Set Größe Riesige Speicher Gesamt Nicht entfernen Speicher nicht entfernen Speichernutzung Speichernutzung Prozent Exit Code OOM tötete PID bei fehlender Streak gestartet

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Docker Container Block IO	Namespace Container Name Device Docker Engine	Kubernetes-Container-Hash Kubernetes-Container-Ports Kubernetes-Container-Restart Anzahl Kubernetes-Container-Ende Meldungspfad Kubernetes Container-Beendigung Meldungsrichtlinie Kubernetes Pod Kulanzzzeit Container-Image Container-Status Container-Version Node-Name Kubernetes Container-Log-Pfad Kubernetes Container-Name Kubernetes Docker-Typ Kubernetes Pod Name Kubernetes Namespace Kubernetes Pod UID Node IP Node Sandbox ID Docker Version Kubernetes Config Kubernetes Config gesehen Kubernetes Config Quelle OpenShift SCC Kubernetes Beschreibung OpenShift Anzeigename Schema Tags Schema Version Pod Template Hash Controller Revision Hash Pod Template Kompose Generation Service Schema Build Date Schema Lizenz Schema Name Schema Vendor Customer Pod Kubernetes StatprofSet Pod Name Tenant WebConsole Build Date License Vendor Architecture authorized Source URL RH Build Host RH Component Distribution Scope Install Maintainer Release Run Summary Uninstall VCS Ref VCS Typ Version Schema URL Schema VCS Schema Version Container ID	IO Service Bytes rekursiv Async IO Service Bytes rekursiv IO lesen Service Bytes rekursiv Sync IO Service Bytes rekursiv IO Service Bytes rekursiv Schreib IO Serviced rekursive Async E/A Serviced rekursive Read IO Serviced rekursive Sync IO Serviced rekursive Total IO Serviced rekursive Write

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Docker Container Network	Namespace Container Name Network Docker Engine	Container Image Container Status Container Version Node Name Node IP Node UUID Node OS K8s Cluster Docker Version Container ID	RX-reduzierte RX-Bytes RX-Fehler RX-Pakete TX reduzierte TX-Bytes TX- Fehler TX-Pakete

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Docker Container-CPU	Namespace Container Name CPU Docker Engine	Kubernetes-Container-Hash Kubernetes-Container-Ports Kubernetes-Container Restart Anzahl Kubernetes-Container-Ende Meldungspfad Kubernetes Container-Beendigung Meldungsrichtlinie Kubernetes Pod Kulanzzzeit Kubernetes-Konfiguration Kubernetes-Konfiguration Kubernetes-KonfigurationSCC-Container-Image Container-Status Container-Version Node-Name Kubernetes Container-Log-Pfad Kubernetes-Container-Name Kubernetes Docker Typ Kubernetes Pod Name Kubernetes Pod Namespace Kubernetes Pod UID Node IP Node Sandbox ID Node OS UUID Kubernetes Cluster Docker Version Kubernetes Beschreibung Kubernetes Anzeigename OpenShift Tags Schema Pod Template Version Controller Revision Hash Pod Template Hash Kompose Generation Service Schema Build Schema License Date Schema Name Kubernetes Hersteller-Pod Pod Name StatprofSet Tenant WebConsole Build Date License Vendor Architecture authorized RH Build Source URL Component Host Install Scope Distribution Run Release Maintainer VCS Uninstall Summary Version Typ VCS Ref Schema URL VCS URL VCS Schema Version Schema Container ID	Drosselungszeiträume Drosselung Gedrosselte Perioden Drosselung Gedrosselte Zeitnutzung Nutzung Im Kernel-Modus Nutzung Im Benutzermodus Auslastung Prozent Nutzung Des Systems Gesamt

Fehlerbehebung

Problem:	Versuchen Sie dies:
Nach den Anweisungen auf der Konfigurationsseite sehe ich meine Docker-Metriken in Cloud Insights nicht.	Prüfen Sie die Telegraf-Agentenprotokolle, um zu sehen, ob es folgenden Fehler meldet: E! Fehler im Plugin [inputs.docker]: Berechtigung verweigert beim Versuch, eine Verbindung zum Docker Daemon-Socket herzustellen. Falls dies der Fall ist, ergreifen Sie die erforderlichen Schritte, um den Telegraf-Agent-Zugriff auf den Docker Unix-Socket wie oben angegeben zu ermöglichen.

Weitere Informationen finden Sie im ["Unterstützung"](#) Seite.

Elasticsearch Data Collector

Cloud Insights verwendet diese Datenerfassung zum Erfassen von Metriken aus Elasticsearch.

1. Klicken Sie in **Admin > Data Collectors** auf **+Data Collector**. Wählen Sie unter **Services** Elasticsearch.
Wählen Sie das Betriebssystem oder die Plattform aus, auf dem der Telegraf-Agent installiert ist.
2. Wenn Sie noch keinen Agent für die Sammlung installiert haben oder einen Agent für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das zu erweitern ["Agenten-Installation"](#) Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel für diesen Datensammler aus. Sie können einen neuen Agent-Zugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agent Access Key** klicken. Best Practice: Verwenden Sie einen anderen Agent-Zugriffsschlüssel nur, wenn Sie Datensammler gruppieren möchten, zum Beispiel nach Betriebssystem/Plattform.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.

[Elasticsearch-Konfiguration]

Einrichtung

Informationen finden Sie unter ["Elasticsearch-Dokumentation"](#).

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Elasticsearch-Cluster	Namespace-Cluster	Node-IP Node-Name Cluster-Status	Gesamtknotenanzahl Gesamtknotenanzahl Dateidatenmenge (Bytes) Dateidatenfreiwert (Bytes) Dateisystem-Daten gesamt (Bytes) JVM Threads BS zugewiesene Prozesse Betriebssystem Verfügbare Prozessoren Betriebssystem Mem Free (Bytes) Betriebssystem Mem Free OS Mem Total (Bytes) verwendetes Betriebssystem Mem verwendeter Prozess CPU Indexes Abschlussgröße (Bytes) Indizes Anzahl Indizes Indexen Anzahl Indizes Indizes Docs gelöschte Indizes Feld Datendiktionen Indices Field Data Memory Size (Bytes) Indizes Abfrage Cache-Anzahl Indizes Cache Größe Indizes Anzahl Segmente Anzahl Indizes Segmente Doc Values Speicher (Bytes) Indizes Shards Index Primärarten AVG Indizes Shards Index Primärindizes Indizes Max Indizes Shards Index Primärindizes Index Indizes Min Indizes. Indizes Shards Index Replication Avg Indizes Shards Index Replication Max Indizes Shards Index Replikation Min Indizes Shards durchschn. Indizes Shards Max Indizes Shards Primaries Indizes Indizes Shards Replication Indizes Shards Storage-Größe (Bytes)

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Elasticsearch-Node	Namespace Cluster es Node ID es Node IP es Node	Zone-ID	Machine Learning Enabled Machine Learning Memory Machine Learning Max Open Jobs X-Pack installierte Breakers Accounting Estimated Size (Bytes) Breakers Accounting Limit Size (Bytes) Breakers Accounting Overhead Breakers Accounting Tripped Breakers Field Data Estimated Size (Bytes) Breakers Field Data Overhead Breakers Field Data Tripped Breakers Field Data Breakers Field Data Stimulated Size (Bytes) Breakers in-Flight Limit Size (Bytes) Breakers in-Flight Overhead Breakers in-Flight Dripped Breakers Parent Estimated Size (Bytes) Breakers Parent Limit Size (Bytes) Breakers Parent Overhead Breakers Parent Tripped Breakers Request Estimated Size (Bytes) Breakers Request availed Filesystem Data available (Bytes) Filesystem Data Free (Bytes) Filesystem Data Total (Bytes) Dateisystem IO Stats Devices Ops Filesystem IO Stats Devices (kb) Schreib-I/O- Stats-Geräte Lese-Ops-Filesystem IO Statistik- Geräte EITE (kb) Dateisystem IO Stats Devices Write Ops Dateisystem IO Stats Total Ops Filesystem IO Stats Total Read (kb) Filesystem IO Stats Read Ops-Filesystem – IO- Statistik (KB) Dateisystem-IO-Stats- Write-Ops-Filesystem Least Usage Estimate Available (Bytes)

Fehlerbehebung

Weitere Informationen finden Sie im ["Unterstützung"](#) Seite.

Flik Data Collector

Cloud Insights verwendet diese Datenerfassung zum Erfassen von Kennzahlen aus Flink.

Installation

1. Klicken Sie in **Admin > Data Collectors** auf **+Data Collector**. Wählen Sie unter **Services** die Option Flink.

Wählen Sie das Betriebssystem oder die Plattform aus, auf dem der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agent für die Sammlung installiert haben oder einen Agent für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das zu erweitern ["Agenten-Installation"](#) Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel für diesen Datensammler aus. Sie können einen neuen Agent-Zugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agent Access Key** klicken. Best Practice: Verwenden Sie einen anderen Agent-Zugriffsschlüssel nur, wenn Sie Datensammler gruppieren möchten, zum Beispiel nach Betriebssystem/Plattform.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.

[Flik-Konfiguration]

Einrichtung

Eine vollständige Flink-Implementierung umfasst die folgenden Komponenten:

JobManager: Das Primärsystem Flik. Koordiniert eine Reihe von TaskManagers. In einer Konfiguration mit hoher Verfügbarkeit verfügt das System über mehr als einen JobManager. **Taskmanager:** Hier werden Flik-Operatoren ausgeführt. Das Flink Plugin basiert auf dem telegraf Jolokia Plugin. Als Voraussetzung für die Erfassung von Informationen aus allen Flik-Komponenten muss JMX auf allen Komponenten konfiguriert und über Jolokia freigelegt werden.

Kompatibilität

Die Konfiguration wurde gegen die Version 1.7 von Flink entwickelt.

Einrichtung

Jolokia Agent Jar

Für alle einzelnen Komponenten muss eine Version der Jolokia Agent JAR-Datei heruntergeladen werden. Die gegen getestete Version war ["Jolokia Agent 1.6.0"](#).

Anweisungen unten gehen davon aus, dass die heruntergeladene JAR-Datei (jolokia-jvm-1.6.0-Agent.jar) unter dem Speicherort '/opt/flink/lib/' platziert wird.

JobManager

Um JobManager so zu konfigurieren, dass die Jolokia API freigegeben wird, können Sie die folgende Umgebungsvariable auf Ihren Knoten einrichten und dann den JobManager neu starten:

```
export FLINK_ENV_JAVA_OPTS="-javaagent:/opt/flink/lib/jolokia-jvm-1.6.0-agent.jar=port=8778,host=0.0.0.0"
```

Sie können einen anderen Port für Jolokia (8778) wählen. Wenn Sie eine interne IP haben, um Jolokia zu sperren, können Sie die „Catch all“ 0.0.0.0 durch Ihre eigene IP ersetzen. Beachten Sie, dass diese IP über das telegraf-Plugin zugänglich sein muss.

Taskmanager

So konfigurieren Sie TaskManager(s), um die Jolokia-API zu öffnen, können Sie die folgende Umgebungsvariable auf Ihren Knoten einrichten und dann den TaskManager neu starten:

```
export FLINK_ENV_JAVA_OPTS="-javaagent:/opt/flink/lib/jolokia-jvm-1.6.0-agent.jar=port=8778,host=0.0.0.0"
```

Sie können einen anderen Port für Jolokia (8778) wählen. Wenn Sie eine interne IP haben, um Jolokia zu sperren, können Sie die „Catch all“ 0.0.0.0 durch Ihre eigene IP ersetzen. Beachten Sie, dass diese IP über das telegraf-Plugin zugänglich sein muss.

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Flik Task Manager	Cluster Namespace-Server	Node Name Task-Manager-ID-Knoten-IP	Netzwerk verfügbar Speichersegmente Netzwerk Speichersegmente Speichersegmente Garbage Collection PS MarkSweep Count Garbage Collection PS MarkSweep Time Garbage Collection PS Scavenge Count Garbage Collection PS Scavenge Time Heap Memory Comstived Heap Memory Init Heap Memory Max Heap Memory Used Thread Count Daemon Thread Count Thread Count Spitzenanzahl Thread Count Thread Count Insgesamt Gestartet
Druckauftrag Einflken	Job-ID des Cluster- Namespace-Servers	Node Name Job Name Node-IP Letzte Checkpoint External Path- Neustartzeit	Ausfall Vollneustarts Last Checkpoint Alignment Buffered Last Checkpoint Duration Last Checkpoint Size Anzahl der abgeschlossenen Checkpoints Anzahl der fehlgeschlagenen Checkpoints Anzahl der laufenden Checkpoints Anzahl der Kontrollpunkte Betriebszeit

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Flik Job Manager	Cluster Namespace-Server	Node Name Node-IP	Garbage Collection PS MarkSweep Count Garbage Collection PS MarkSweep Time Garbage Collection PS Scavenge Count Garbage Collection PS Scavenge Time Heap Memory Comstived Heap Memory Init Heap Memory Max Heap Memory Used Number Registrierte Task- Manager Anzahl laufende Jobs Taskleisten verfügbare Task- Steckplätze Gesamt- Thread-Anzahl Daemon- Thread-Anzahl Maximale Anzahl Der Threads Anzahl Der Threads Insgesamt Begonnen

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Flik-Aufgabe	Cluster Namespace Job-ID Task-ID	Server Node Name Job Name Sub Task-Index Task-Versuch-ID Task-Versuch Nummer Task-Name Task-Manager-ID Knoten-IP Aktuelle Eingabe-Wasserzeichen	Puffer in Pool Nutzung Buffers in Warteschlange Länge Buffer Out Pool Nutzung Buffer Out Queue Länge Anzahl Puffer in Lokale Anzahl Buffers in Local per Second Anzahl Puffer in Local per second Rate Anzahl Puffer in Remote Number Buffers in Remote per second Anzahl Puffer in Remote per second Anzahl der Puffer in Remote per Anzahl Der Auspuffer Anzahl Der Auspuffer Pro Sekunde Anzahl Auspuffer Pro Sekunde Anzahl Bytes Pro Sekunde Anzahl Bytes In Lokale Anzahl Bytes Pro Sekunde Anzahl Bytes In Lokal Pro Sekunde Anzahl Bytes In Lokal Pro Sekunde Anzahl Bytes In Remote Number Bytes In Remote Per Second Anzahl Bytes In Remote Pro Sekunde Rate Anzahl Bytes Out Anzahl Bytes Out Pro Sekunde Anzahl Bytes Out Pro Sekunde Anzahl Datensätze In Number Datensätze In Per Second Anzahl Datensätze Pro Sekunde Anzahl Datensätze Pro Sekunde Anzahl Datensätze Pro Sekunde Anzahl Datensätze Aus Anzahl Datensätze Pro Sekunde Anzahl Datensätze Aus Pro Sekunde

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Flik Task Operator	Cluster Namespace Job-ID Operator-ID Task-ID	Server Node Name Job Name Operator Name Sub Task-Index Task-Versuch-ID Task-Versuch-Nummer Task-Name Task-Manager-ID-Knoten-IP	Aktuelle Eingabe Watermark Current Output Watermark Number Records In Number Records In Per Second Count Anzahl Datensätze In Pro Sekunde Anzahl Datensätze Pro Sekunde Anzahl Datensätze Aus Anzahl Datensätze Pro Sekunde Anzahl Anzahl Datensätze Aus Pro Sekunde Anzahl Verspätete Datensätze Verworfen Zugewiesene Partitionen Bytes Verbrauchte Rate Commit Latenz Durchschn. Commit-Latenz Max. Commit Rate Commits faciert fehlgeschlagene Verbindungen Close Rate Verbindungsanzahl Verbindungserzeugung Rate Anzahl Abholen Latenz durchschn. Abholen Max. Abholen Rate Abholen Größe Max. Abholen Drosselzeit durchschn. Abrufdauer Max. Heartbeat Rate Incoming Byte Rate I/O- Zeit durchschn. (Ns) I/O Wartezeit I/O Wartezeit durchschn. (Ns) Verbindungsrate Verbindungszeit durchschn. Letzter Heartbeat ago Netzwerk- I/O-Rate ausgehende Byte-Datensätze verbrauchte Rate Datensätze lag max. Datensätze pro Anforderung durchschn. Anfragemgröße Durchschnittl. Anfragemgröße max. Ansprechrate Wählen Rate Synchronisierungszeit durchschn. Heartbeat Antwort Zeit Max. Verbindungszeit Max. Synchronisierungszeit

Fehlerbehebung

Weitere Informationen finden Sie im "[Unterstützung](#)" Seite.

Hadoop Data Collector

Cloud Insights verwendet diese Datenerfassung zum Erfassen von Kennzahlen aus Hadoop.

Installation

1. Klicken Sie in **Admin > Data Collectors** auf **+Data Collector**. Wählen Sie unter **Services** Hadoop.

Wählen Sie das Betriebssystem oder die Plattform aus, auf dem der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agent für die Sammlung installiert haben oder einen Agent für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das zu erweitern "[Agenten-Installation](#)" Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel für diesen Datensammler aus. Sie können einen neuen Agent-Zugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agent Access Key** klicken. Best Practice: Verwenden Sie einen anderen Agent-Zugriffsschlüssel nur, wenn Sie Datensammler gruppieren möchten, zum Beispiel nach Betriebssystem/Plattform.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.

[Hadoop Konfiguration] [Hadoop Konfiguration]

Einrichtung

Eine vollständige Hadoop Implementierung umfasst die folgenden Komponenten:

- NameNode: Das primäre System Hadoop Distributed File System (HDFS) Koordiniert eine Reihe von DataNodes.
- Sekundärer NameNode: Ein warmer Failover für den NameNode. In Hadoop erfolgt die Heraufstufung auf NameNode nicht automatisch. Secondary NameNode sammelt Informationen von NameNode, damit sie bei Bedarf heraufgestuft werden können.
- DataNode: Tatsächlicher Eigentümer von Daten.
- ResourceManager: Das primäre Computersystem (Yarn). Koordiniert eine Reihe von NodeManagers.
- NodeManager: Die Ressource für Computing. Aktueller Speicherort für das Ausführen von Anwendungen.
- JobHistorieServer: Verantwortlich für die Bearbeitung aller Anfragen im Zusammenhang mit der Jobhistorie.

Das Hadoop Plugin basiert auf dem telegraf Jolokia Plugin. Um Informationen aus allen Hadoop Komponenten zu sammeln, muss JMX auf allen Komponenten konfiguriert und zugänglich gemacht werden.

Kompatibilität

Die Konfiguration wurde mit Hadoop Version 2.9 entwickelt.

Einrichtung

Jolokia Agent Jar

Für alle einzelnen Komponenten muss eine Version der Jolokia Agent JAR-Datei heruntergeladen werden. Die gegen getestete Version war "[Jolokia Agent 1.6.0](#)".

Die nachfolgende Anleitung setzt voraus, dass die heruntergeladene JAR-Datei (jolokia-jvm-1.6.0-Agent.jar) unter der Adresse '/opt/hadoop/lib/' abgelegt wird.

NameNode

Um NameNode zu konfigurieren, um die Jolokia API freizugeben, können Sie unter <HADOOP_HOME>/etc/hadoop/hadoop-env.sh Folgendes einrichten:

```
export HADOOP_NAMENODE_OPTS="$HADOOP_NAMENODE_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7800,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8000
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
```

You can choose a different port for JMX (8000 above) and Jolokia (7800). If you have an internal IP to lock Jolokia onto you can replace the "catch all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from the telegraf plugin. You can use the option '-Dcom.sun.management.jmxremote.authenticate=false' if you don't want to authenticate. Use at your own risk.

Sekundärer NameNode

Um den sekundären NameNode zu konfigurieren, um die Jolokia API freizugeben, können Sie Folgendes in <HADOOP_HOME>/etc/hadoop/hadoop-env.sh einrichten:

```
export HADOOP_SECONDARYNAMENODE_OPTS="$HADOOP_SECONDARYNAMENODE_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7802,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8002
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
```

You can choose a different port for JMX (8002 above) and Jolokia (7802). If you have an internal IP to lock Jolokia onto you can replace the "catch all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from the telegraf plugin. You can use the option '-Dcom.sun.management.jmxremote.authenticate=false' if you don't want to authenticate. Use at your own risk.

DataNode

Um die DataNodes so zu konfigurieren, dass sie die Jolokia API aussetzen, können Sie Folgendes in <HADOOP_HOME>/etc/hadoop/hadoop-env.sh einrichten:

```
export HADOOP_DATANODE_OPTS="$HADOOP_DATANODE_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7801,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8001
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
```

You can choose a different port for JMX (8001 above) and Jolokia (7801). If you have an internal IP to lock Jolokia onto you can replace the "catch all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from the telegraf plugin. You can use the option '-Dcom.sun.management.jmxremote.authenticate=false' if you don't want to authenticate. Use at your own risk.

ResourceManager

Um den ResourceManager so zu konfigurieren, dass die Jolokia API zur Verfügung gestellt wird, können Sie Folgendes in <HADOOP_HOME>/etc/hadoop/hadoop-env.sh einrichten:

```
export YARN_RESOURCEMANAGER_OPTS="$YARN_RESOURCEMANAGER_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7803,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8003
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
```

You can choose a different port for JMX (8003 above) and Jolokia (7803). If you have an internal IP to lock Jolokia onto you can replace the "catch all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from the telegraf plugin. You can use the option '-Dcom.sun.management.jmxremote.authenticate=false' if you don't want to authenticate. Use at your own risk.

NodeManager

Um die NodeManagers so zu konfigurieren, dass sie die Jolokia API aussetzen, können Sie Folgendes in <HADOOP_HOME>/etc/hadoop/hadoop-env.sh einrichten:

```
export YARN_NODEMANAGER_OPTS="$YARN_NODEMANAGER_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7804,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8004
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
```

You can choose a different port for JMX (8004 above) and Jolokia (7804). If you have an internal IP to lock Jolokia onto you can replace the "catch all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from the telegraf plugin. You can use the option '-Dcom.sun.management.jmxremote.authenticate=false' if you don't want to authenticate. Use at your own risk.

JobGeschichteServer

Um den JobHistorieServer so zu konfigurieren, dass die Jolokia API zur Verfügung gestellt wird, können Sie Folgendes in <HADOOP_HOME>/etc/hadoop/hadoop-env.sh einrichten:

```
export HADOOP_JOB_HISTORYSERVER_OPTS="$HADOOP_JOB_HISTORYSERVER_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7805,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8005
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
```

You can choose a different port for JMX (8005 above) and Jolokia (7805). If you have an internal IP to lock Jolokia onto you can replace the "catch all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from the telegraf plugin. You can use the option '-Dcom.sun.management.jmxremote.authenticate=false' if you don't want to authenticate. Use at your own risk.

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Sekundärer Hadoop NameNode	Cluster Namespace- Server	Node Name Node IP Compile Info Version	GC-Anzahl GC-Kopien Anzahl GC-Markierungen Sweep Compact-Anzahl GC-Nummer Info Schwellenwert überschritten GC-Nummer Warnungsschwellenwert überschritten GC-Zeit kopieren GC- Markierungen Sweep Compact-Zeit GC Gesamtdauer Extra Sleep Time Logs Anzahl der Fehler Protokolle Anzahl der fatalen Protokolle Info- Anzahl Warnmeldungen SpeicherHeap-Comstied Speicher Heap Max Speicher Heap Verwendeter Speicher Max Speicher Nicht Heap Speicher Nicht Heap Max Speicher Nicht Heap Verwendete Threads Blockierte Threads Neue Threads Runnable Threads Beendet Threads Timed Waiting Threads

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Hadoop NodeManager	Cluster Namespace-Server	Node Name Node-IP	Container Zugewiesener Speicher Zugewiesener Speicher Zuweisen Opportunistic Virtual Cores Allocchortunistic Virtual Cores Zugeordnete Speichernutzung Verfügbare Kerne Verfügbare Verzeichnisse Bad Lokale Verzeichnisse Bad Log Cache Größe Vor Clean Container Starten Dauer Durchschn. Dauer Container Starten Dauer Anzahl Operationen Container Abgeschlossen Container Container Container Container Container Container Inting Container Killed Containers Started Containers Container Reiniting Container gerollt zurück auf Fehler- Container ausgeführt Plattenauslastung gut Lokale Verzeichnisse Datenträgernutzung gut Log-Verzeichnisse Bytes gelöscht Private Bytes gelöscht Öffentliche Container mit opportunistischen Bytes gelöscht Gesamtanzahl Shuffle Verbindungen Shuffle Ausgabe Bytes Shuffle Outputs fehlgeschlagen Shuffle Outputs OK GC-Anzahl GC-Kopien Anzahl GC- Markierungen Sweep Compact Count GC- Nummer Info Schwellenwert überschritten GC-Nummer Warnungsschwellenwert überschritten GC-Zeit kopieren GC- Markierungen Sweep Compact Time GC Gesamtdauer Extra Sleep Time Logs Anzahl Protokolle Fatal Count Protokolle Warnungszahl Speicher Heap Max

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Hadoop ResourceManager	Cluster Namespace- Server	Node Name Node-IP	AnwendungMaster- Startverzögerung durchschn. AnwendungMaster- Startverzögerung AnwendungMaster- Register Verzögerung durchschn. AnwendungMaster Register Verzögerung Nummer NodeManager Aktive Nummer NodeManager Decommissionierte Nummer NodeManager Decommissioning Nummer NodeManager Lost Number NodeManager neu gestartet Nummer NodeManager Herunterfahren Nummer NodeManager Healthy Number NodeManager Memory Limit NodeManager Virtual Cores Limit used Capacity Active Applications Active Users Aggregierter Container Zugewiesene Aggregatcontainer Freigegebene Aggregate- Speicher Sekunden Ersatz Für Aggregat-Node Lokale Container Zugewiesene Aggregat- Aus Switch-Container Zugewiesenes Aggregat Ack Lokale Container Zugewiesenes Aggregat Virtuelle Kerne Sekunden Vorweggenommen Container Zugewiesener Speicher Zugewiesene Virtuelle Kerne Applikationsversuch Erster Container- Zuweisungsverzögerung Durchschn. Time Application-Versuch Erste Containerzuordnungsverz ögerung Anzahl der Anwendungen Abgeschlossene Anwendungen Anwendungen

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Hadoop DataNode	Cluster Namespace- Server	Node Name Node-IP Cluster-ID-Version	Transceiver-Anzahl überträgt in Bearbeitung Cache Kapazität Cache verwendete Kapazität DFS verwendete geschätzte Kapazität verloren Gesamt Letztes Volume Ausfall Rate Blöcke Anzahl gecachte Blöcke Anzahl fehlgeschlagener Cache- Blöcke Anzahl nicht in Cache-Blöcke Anzahl nicht übertragene Volumes Anzahl Restkapazität GC-Kopien Anzahl GC-Mark Sweep Compact-Anzahl GC- Nummer Info Schwellenwert überschritten GC-Nummer Warnschwellenwert überschritten GC-Zeit Kopieren GC-Zeit GC- Markierungen Sweep Compact Time GC Gesamt Extra Sleep Time Logs Anzahl Protokolle tödliche Anzahl Protokolle Info Anzahl Protokolle Warnungszahl Speicher Heap-Speicher Heap Max Speicher Heap verwendeter Speicher Max Speicher nicht Heap- belegt Speicher Nicht Heap Max Speicher Nicht Heap Verwendet Threads Blockiert Threads Neue Threads Runnable Threads Beendet Threads Timed Waiting Threads Wartend

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Hadoop NameNode	Cluster Namespace-Server	Node Name Node IP Transaktions-ID Letzte geschriebene Zeit seit Letzte geladen Edits HA State File System Status Block Pool ID Cluster ID Compile Info unterschiedliche Version Anzahl Version	Block Kapazität Blöcke Gesamtkapazität genutzte Gesamtkapazität nicht DFS-Blöcke beschädigt geschätzte Kapazität verloren Gesamtblöcke Überschuss Herzschläge abgelaufen Dateien Gesamt File System Lock Queue Länge Blöcke fehlende Blöcke fehlende Replizierung mit Faktor 1 Clients Aktive Daten Knoten Dead Data Nodes Deaktivieren Dead Data Nodes Decommissioning Live Data Nodes Decommissionieren Verschlüsselungszonen Anzahl Daten Knoten, die Wartungsdateien unter Baudaten Knoten eingeben in Wartung Daten Knoten leben in Wartung Daten Knoten Live-Speicher Inches Replikation Ausstehende Timeouts Datenknoten Nachricht Ausstehende Blöcke Ausstehende Löschblöcke ausstehende Replikationsblöcke Ausstehende Replikationsblöcke Ausstehende Replikationsblöcke mehrere verschobene Blöcke geplante Snapshot-Verzeichnisse Daten-Nodes veraltete Dateien Gesamt Last Sync Anzahl der gesamten Transaktionen seit letzten Checkpoint- Transaktionen seit Last Log Roll-Blocks UnderReplicated Volume Failures gesamte Synchronisierungszeiten Gesamtes Objekt Max Operationen hinzufügen Operationen Snapshots zulassen Batched Operations Block Queued Operations Block

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Hadoop JobGeschichteServer	Cluster Namespace- Server	Node Name Node-IP	GC-Anzahl GC-Kopien Anzahl GC-Markierungen Sweep Compact-Anzahl GC-Nummer Info Schwellenwert überschritten GC-Nummer Warnungsschwellenwert überschritten GC-Zeit kopieren GC- Markierungen Sweep Compact-Zeit GC Gesamtdauer Extra Sleep Time Logs Anzahl der Fehler Protokolle Anzahl der fatalen Protokolle Info- Anzahl Warnmeldungen SpeicherHeap-Comstied Speicher Heap Max Speicher Heap Verwendeter Speicher Max Speicher Nicht Heap Speicher Nicht Heap Max Speicher Nicht Heap Verwendete Threads Blockierte Threads Neue Threads Runnable Threads Beendet Threads Timed Waiting Threads

Fehlerbehebung

Weitere Informationen finden Sie im ["Unterstützung"](#) Seite.

HAProxy Data Collector

Cloud Insights verwendet diese Datensammlung, um Kennzahlen von HAProxy zu erfassen.

Installation

1. Klicken Sie in **Admin > Data Collectors** auf **+Data Collector**. Wählen Sie unter **Services** die Option HAProxy.

Wählen Sie das Betriebssystem oder die Plattform aus, auf dem der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agent für die Sammlung installiert haben oder einen Agent für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das zu erweitern ["Agenten-Installation"](#) Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel für diesen Datensammler aus. Sie können einen neuen Agent-Zugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agent Access Key** klicken. Best Practice:

Verwenden Sie einen anderen Agent-Zugriffsschlüssel nur, wenn Sie Datensammler gruppieren möchten, zum Beispiel nach Betriebssystem/Plattform.

4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.

[HAProxy-Konfiguration]

Einrichtung

Telegraf's Plugin für HAProxy setzt auf HAProxy Stats Aktivierung. Diese Konfiguration ist in HAProxy integriert, ist jedoch nicht sofort aktiviert. Wenn HAProxy aktiviert ist, wird ein HTML-Endpunkt angezeigt, der in Ihrem Browser angezeigt werden kann oder für die Extraktion des Status aller HAProxy-Konfigurationen abgekratzt werden kann.

Kompatibilität:

Die Konfiguration wurde gegen HAProxy-Version 1.9.4 entwickelt.

Einrichtung:

Um Statistiken zu aktivieren, bearbeiten Sie Ihre haproxy-Konfigurationsdatei und fügen Sie nach dem Abschnitt 'Standards' die folgenden Zeilen hinzu: Verwenden Sie Ihren eigenen Benutzer/Ihr Passwort und/oder die haproxy-URL:

```
stats enable
stats auth myuser:mypassword
stats uri /haproxy?stats
```

Im Folgenden finden Sie eine vereinfachte Beispiel-Konfigurationsdatei mit aktivierten Statistiken:

```
global
  daemon
  maxconn 256

defaults
  mode http
  stats enable
  stats uri /haproxy?stats
  stats auth myuser:mypassword
  timeout connect 5000ms
  timeout client 50000ms
  timeout server 50000ms

frontend http-in
  bind *:80
  default_backend servers

frontend http-in9080
  bind *:9080
  default_backend servers_2

backend servers
  server server1 10.128.0.55:8080 check ssl verify none
  server server2 10.128.0.56:8080 check ssl verify none

backend servers_2
  server server3 10.128.0.57:8080 check ssl verify none
  server server4 10.128.0.58:8080 check ssl verify none
```

Vollständige und aktuelle Anweisungen finden Sie im ["HAProxy-Dokumentation"](#).

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
HAProxy Frontend	Namespace- Adressenproproxy	Node-IP-Knotenname Proxy-ID-Modus Prozess- id Sitzungen Ratenlimit Server-id Sitzungen Limit Status	Bytes in Bytes Out Cache Hits Cache Lookups Komprimierung Bytes umgangen Komprimierung Bytes in Komprimierung Bytes Out Komprimierung Reaktionen Verbindungsrate Verbindungsrate Max Verbindungen insgesamt Anträge, die von der Verbindung abgelehnt werden Rule Requests verweigert durch Sicherheitsbedenken Antworten verweigert durch Sicherheitsbedenken Anfragen abgelehnt durch Session Rule Requests erfragt Fehler Antworten 1xx Antworten 2xx Antworten 3xx Antworten 4xx Antworten 5xx Antworten andere Anfragen Abfangen Sitzungen Rate Sitzungen Max Anfragen Rate Max Anfragen Rate Max Anforderungen Total Sessions Sitzungen Max Sitzungen Antworten Neuschreibung Total Requests

Objekt:	Kennungen:	Attribute:	Datenpunkte:
HAProxy-Server	Namespace-Adresse-Proxy-Server	Node-IP-Knotenname Check Time to Finish Check Fall Configuration Check Health Value Check RISE Configuration Check Status Proxy ID Last Change Time Last Session Time Mode Process id Server Status Weight	Aktive Server Backup Server Bytes in Bytes Out Downs Check Downs Check Fails Client abgebrochen Verbindungen Verbindung Verbindung Durchschnittliche Zeit Ausfallzeit Gesamt Denied Responses Verbindungsfehler Antwort 1xx Antworten 2xx Antworten 3xx Antworten 4xx Antworten 5xx Antworten anderer Server ausgewählt Total Queue Current Queue Max. Durchschnittliche Zeit Sitzungen pro Zweite Sitzungen pro Sekunde Max. Wiederverwendbarkeit der Verbindung Reaktionszeit Durchschnittliche Sitzungen Sitzungen Max Server Transfer bricht Sitzungen gesamte Sitzungen Gesamtzeit Durchschnittliche Anforderungen Redispatches Anfragen Wiederholungen Anfragen Neuschreibung Anfragen

Objekt:	Kennungen:	Attribute:	Datenpunkte:
HAProxy-Back-End	Namespace-Adressenproproxy	Node-IP-Node-Name Proxy-ID Letzte Änderung Zeit Letzte Sitzung Zeitmodus Prozess-id Server-id Sitzungen Limit Status Gewicht	Aktive Server Backup Server Bytes in Bytes Out Cache Aufrufe Cache Lookups überprüfen Downs Client abbricht Komprimierung Bytes umgangen Komprimierung Bytes in Komprimierung Bytes out Komprimierungsantworten Verbindung Durchschnittliche Zeit Ausfallzeit Total Requests verweigert durch Sicherheitsbedenken Antworten verweigert durch Sicherheit Bedenken Verbindungsfehler Antworten Reaktion 1xx Antworten 2xx Antworten 3xx Antworten 4xx Antworten 5xx Antworten anderer Server ausgewählt Total Queue Current Queue Max. Warteschlange Durchschnittliche Zeit Sitzungen pro Sekunde Sitzungen pro Sekunde Max. Anfragen Gesamt Verbindungswiederverwen- dung Reaktionszeit Durchschnittliche Sitzungen Sitzungen Max. Serverübertragung Abreibungen Sitzungen Gesamtzeit Durchschnittliche Anfragen Neuzuweisen Wiederholungsanfragen Wiederholungsanfragen Wiederholungsanfragen Wiederholungsanfragen Anträge Neu Schreiben

Fehlerbehebung

Weitere Informationen finden Sie im ["Unterstützung"](#) Seite.

JVM Data Collector

Cloud Insights verwendet diese Datenerfassung zum Erfassen von Kennzahlen aus JVM.

Installation

1. Klicken Sie in **Admin > Data Collectors** auf **+Data Collector**. Wählen Sie unter **Services** JVM.

Wählen Sie das Betriebssystem oder die Plattform aus, auf dem der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agent für die Sammlung installiert haben oder einen Agent für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das zu erweitern "[Agenten-Installation](#)" Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel für diesen Datensammler aus. Sie können einen neuen Agent-Zugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agent Access Key** klicken. Best Practice: Verwenden Sie einen anderen Agent-Zugriffsschlüssel nur, wenn Sie Datensammler gruppieren möchten, zum Beispiel nach Betriebssystem/Plattform.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.

[JVM-Konfiguration]

Einrichtung

Informationen finden Sie unter "[JVM-Dokumentation](#)".

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
JVM	Namespace-JVM	OS Architektur OS Name OS Version Laufzeit Spezifikation Laufzeit Spezifikation Hersteller Laufzeit Spezifikation Version Uptime Laufzeit VM Name Laufzeit VM Anbieter Laufzeit VM Version Node Name Node IP	Class Loaded Class Loaded Class Memory Unloaded Memory Heap Init Memory Heap used Max Memory Heap Used Memory Non Heap Innit Memory Non Heap Max Memory nicht Heap Used Memory Objects Ausstehende Fertigstellung von Betriebssystemprozessoren verfügbar Betriebssystem engagierte virtuelle Speichergröße OS Kostenlos Physikalische Speichergröße OS Freier Swap Speicherplatz Größe OS Max Datei Descriptor Anzahl OS Open File Descriptors Anzahl Betriebssystem Prozessor CPU Load OS CPU Time OS System CPU Load OS System Load Average OS Gesamt Physical Memory Size OS Gesamt Swap Space Size Thread Daemon Anzahl der Threads Spitzenanzahl Thread Count Thread Total Started Count Garbage Collector Copy Collection Count Garbage Collector Copy Collection Time Garbage Collector Sammlung von Mark- Sweep Sammlungszeit Zeitabfälle Collector G1 Sammlung der Alten Generation Speicherbage Collector G1 Zeitabbage der Jungen Generation Sammlungsähler Garbage Collector G1 Young Generation Collection Time Garbage Collector Zeitabfälle Sammlung der aktuellen Mark-Sweep Sammlung Zeitgarage Collector Parallel Collection Count Garbage Collector Parallel

Fehlerbehebung

Weitere Informationen finden Sie im ["Unterstützung"](#) Seite.

Kafka Data Collector

Cloud Insights verwendet diese Datensammler, um Metriken aus Kafka zu sammeln.

Installation

1. Klicken Sie in **Admin > Data Collectors** auf **+Data Collector**. Wählen Sie unter **Services** Kafka.

Wählen Sie das Betriebssystem oder die Plattform aus, auf dem der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agent für die Sammlung installiert haben oder einen Agent für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das zu erweitern ["Agenten-Installation"](#) Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel für diesen Datensammler aus. Sie können einen neuen Agent-Zugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agent Access Key** klicken. Best Practice: Verwenden Sie einen anderen Agent-Zugriffsschlüssel nur, wenn Sie Datensammler gruppieren möchten, zum Beispiel nach Betriebssystem/Plattform.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.

[Konfiguration von Kafka]

Einrichtung

Das Kafka Plugin basiert auf dem telegraf's Jolokia Plugin. Um Informationen aus allen Kafka-Brokern zu sammeln, muss JMX über Jolokia auf allen Komponenten konfiguriert und zugänglich gemacht werden.

Kompatibilität

Konfiguration wurde gegen Kafka Version 0.11.0 entwickelt.

Einrichtung

Alle Anweisungen unten Nehmen wir an, dass Ihr Installationsort für kafka '/opt/kafka' ist. Sie können die nachfolgenden Anweisungen an Ihren Installationsort anpassen.

Jolokia Agent Jar

Eine Version die Jolokia Agent jar-Datei muss sein ["Heruntergeladen"](#). Die gegen die Version getestetete war Jolokia Agent 1.6.0.

Anweisungen unten gehen davon aus, dass die heruntergeladene JAR-Datei (jolokia-jvm-1.6.0-Agent.jar) unter dem Speicherort '/opt/kafka/libs/' abgelegt wird.

Kafka Brokers

Um Kafka Brokers so zu konfigurieren, dass sie die Jolokia API aussetzen, können Sie in `<KAFKA_HOME>/bin/kafka-Server-Start.sh` kurz vor dem Anruf „kafka-run-class.sh“ Folgendes hinzufügen:

```
export JMX_PORT=9999
export RMI_HOSTNAME=`hostname -I`
export KAFKA_JMX_OPTS="-javaagent:/opt/kafka/libs/jolokia-jvm-1.6.0-
agent.jar=port=8778,host=0.0.0.0
-Dcom.sun.management.jmxremote.password.file=/opt/kafka/config/jmxremote.p
assword -Dcom.sun.management.jmxremote.ssl=false
-Djava.rmi.server.hostname=$RMI_HOSTNAME
-Dcom.sun.management.jmxremote.rmi.port=$JMX_PORT"
```

Beachten Sie, dass das obige Beispiel 'Hostname -i' verwendet, um die Umgebungsvariable 'RMI_HOSTNAME' einzurichten. In mehreren IP-Maschinen muss dies optimiert werden, um die IP, die Sie für RMI-Verbindungen interessieren, zu erfassen.

Sie können einen anderen Port für JMX (9999 oben) und Jolokia (8778) wählen. Wenn Sie eine interne IP haben, um Jolokia zu sperren, können Sie die „Catch all“ 0.0.0.0 durch Ihre eigene IP ersetzen. Beachten Sie, dass diese IP über das telegraf-Plugin zugänglich sein muss. Sie können die Option '-Dcom.sun.management.jmxremote.authenticate=false' verwenden, wenn Sie nicht authentifizieren möchten. Nutzung auf eigenes Risiko.

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Kafka Broker	Cluster Namespace Broker	Node Name Node-IP	Replikatmanager Fetcher Max Lag Zookeeper Client-Verbindungen Zookeeper Client-Verbindungen (15 m Rate) Zookeeper Client-Verbindungen (5 m Rate) Zookeeper Client-Verbindungen (mittlere Rate) Zookeeper Client-Verbindungen (1 m Rate) Anzahl der Threads des Replikatmanagers Anzahl der Threads Anzahl der Threads Anzahl der Threads Anzahl der aktuellen Lesevorgänge Anzahl der insgesamt gestarteten Offline-Partitionen Anfragen Gesamtzeit (50. Perzentil) Anfragen produzieren Gesamtzeit (75. Perzentil) Anfragen produzieren Gesamtzeit (98 Perzentil) Anfragen produzieren Gesamtzeit (999. Perzentil) Erstellen von Anfragen Gesamtzeit (9th Perzentil) Erstellen von Anfragen Gesamtzeit produzieren Anfragen Gesamtzeit produzieren Anfragen Max produzieren Anfragen Gesamtzeit Mittelwert produzieren Anfragen Gesamtzeit Min Erzeugungsanforderungen Totalzeit Max Gesamtzeit Gesamtzeit Stddev Replica Manager ISR reduziert Replikatmanager verkleinert ISR (15 m Rate) Replica Manager ISR reduziert (5 m Rate) Replica Manager ISR reduziert (Mittlere Rate) Replica Manager ISR-Shrink (1-m-Rate) Anforderung Handler durchschn. Leerlaufanfrage (15-m-Rate) Anforderung

Fehlerbehebung

Weitere Informationen finden Sie im ["Unterstützung"](#) Seite.

Kibana Data Collector

Cloud Insights verwendet diesen Datensammler, um Kennzahlen von Kibana zu sammeln.

Installation

1. Klicken Sie in **Admin > Data Collectors** auf **+Data Collector**. Wählen Sie unter **Services** die Option Kibana.

Wählen Sie das Betriebssystem oder die Plattform aus, auf dem der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agent für die Sammlung installiert haben oder einen Agent für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das zu erweitern ["Agenten-Installation"](#) Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel für diesen Datensammler aus. Sie können einen neuen Agent-Zugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agent Access Key** klicken. Best Practice: Verwenden Sie einen anderen Agent-Zugriffsschlüssel nur, wenn Sie Datensammler gruppieren möchten, zum Beispiel nach Betriebssystem/Plattform.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.

[Kibana-Konfiguration]

Einrichtung

Informationen finden Sie unter ["Kibana Dokumentation"](#).

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Kibana	Namespace-Adresse	Versionsstatus des Node- IP-Node-Namens	Gleichzeitige Verbindungen Heap Max Heap verwendete Anforderungen pro Sekunde Antwortzeit Max. Betriebszeit

Fehlerbehebung

Weitere Informationen finden Sie im ["Unterstützung"](#) Seite.

Memcached Data Collector

Cloud Insights verwendet diese Datensammlung, um Kennzahlen aus Memcached zu erfassen.

Installation

1. Klicken Sie in **Admin > Data Collectors** auf **+Data Collector**. Wählen Sie unter **Services** Memcached.

Wählen Sie das Betriebssystem oder die Plattform aus, auf dem der Telegraf-Agent installiert ist.
2. Wenn Sie noch keinen Agent für die Sammlung installiert haben oder einen Agent für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das zu erweitern "[Agenten-Installation](#)" Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel für diesen Datensammler aus. Sie können einen neuen Agent-Zugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agent Access Key** klicken. Best Practice: Verwenden Sie einen anderen Agent-Zugriffsschlüssel nur, wenn Sie Datensammler gruppieren möchten, zum Beispiel nach Betriebssystem/Plattform.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.

[Konfiguration mit Memcached]

Einrichtung

Informationen finden Sie unter "[Wiki mit Memcached](#)".

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Gememcachte	Namespace-Server	Node-IP-Node-Name	Akzeptieren von Verbindungen verarbeitet Authentifizierungsanforderungen fehlgeschlagene Authentifizierungen verwendete Bytes (pro Sekunde) geschriebene Bytes (pro Sek.) CAS Badval CAS Hits CAS Misses Flush Reqs (pro Sek.) Get Reqs (pro Sek.) Set Reqs (pro Sek.) Touch Reqs (pro Sek.) Verbindungserträge (pro Sek.) Verbindungsstrukturen Verbindungen öffnen Aktuelle gespeicherte Objekte Decr fordert Zugriffe (pro Sek.) Decr fordert Fehlschläge (pro Sek.) Löschen von Anfragen Treffer (pro Sek.) Löschen von Anfragen Fehlschläge (pro Sek.) entfernte Objekte gültige Abreibungen abgelaufene Objekte Get Hits (pro Sek.) Get Misses (pro Sek.) Gebrauchte Hash Bytes Hash-Bytes erweitert Hash Power Level Inc. Hash Power Level Inc. Zugriffe (pro Sek.) Infr Anfragen Misses (pro Sek.) Server Max Bytes anhören deaktiviert Num zurückgewonnener Mitarbeiter Threads Anzahl geöffnete Verbindungen Gesamtzahl der gespeicherten Elemente Touch Hits Touch Misses Server Uptime

Fehlerbehebung

Weitere Informationen finden Sie im ["Unterstützung"](#) Seite.

MongoDB Data Collector

Cloud Insights verwendet diesen Datensammler, um Metriken von MongoDB zu erfassen.

Installation

1. Klicken Sie in **Admin > Data Collectors** auf **+Data Collector**. Wählen Sie unter **Services** die Option MongoDB aus.

Wählen Sie das Betriebssystem oder die Plattform aus, auf dem der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agent für die Sammlung installiert haben oder einen Agent für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das zu erweitern "[Agenten-Installation](#)" Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel für diesen Datensammler aus. Sie können einen neuen Agent-Zugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agent Access Key** klicken. Best Practice: Verwenden Sie einen anderen Agent-Zugriffsschlüssel nur, wenn Sie Datensammler gruppieren möchten, zum Beispiel nach Betriebssystem/Plattform.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.

[MongoDB Konfiguration]

Einrichtung

Informationen finden Sie unter "[MongoDB Dokumentation](#)".

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
MongoDB	Namespace-Hostname		
MongoDB Datenbank	Name der Namespace-Hostname-Datenbank		

Fehlerbehebung

Informationen können im gefunden werden "[Unterstützung](#)" Seite.

MySQL Data Collector

Cloud Insights verwendet diese Datensammlung, um Kennzahlen von MySQL zu sammeln.

Installation

1. Klicken Sie in **Admin > Data Collectors** auf **+Data Collector**. Wählen Sie unter **Services** MySQL.

Wählen Sie das Betriebssystem oder die Plattform aus, auf dem der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agent für die Sammlung installiert haben oder einen Agent für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das zu erweitern "[Agenten-Installation](#)" Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel für diesen Datensammler aus. Sie können einen neuen Agent-Zugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agent Access Key** klicken. Best Practice: Verwenden Sie einen anderen Agent-Zugriffsschlüssel nur, wenn Sie Datensammler gruppieren möchten, zum Beispiel nach Betriebssystem/Plattform.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.

[MySQL-Konfiguration]

Einrichtung

Informationen finden Sie unter "[MySQL-Dokumentation](#)".

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
MySQL	Namespace für MySQL Server	Node-IP-Node-Name	Abgebrochene Clients (pro s) abgebrochene Verbindungen (pro s) RX Byte (pro s) TX Bytes (pro Sek.) Befehle Admin (pro Sek.) Befehle Alter Ereignisbefehle Alter Funktion Befehle Alter Instanz Befehle Alter Prozedur Befehle Alter Server Befehle Alter Tabelle Befehle Alter Tablespace Befehle Alter Benutzer Befehle Analyse Befehle Zuweisen zu Keycache-Befehlen Begin-Befehle Binlog-Befehle Aufruf Procedure-Befehle DB-Befehle Change Master befiehlt Change Repl Filter Befehle Check Commands Prüfsummenbefehle Befehle Commit-Befehle DB-Befehle erstellen Ereignisbefehle erstellen Befehle erstellen Index-Befehle erstellen Maßnahmen-Befehle erstellen Serverbefehle erstellen Trigger-Befehle erstellen UDF-Befehle erstellen Benutzerbefehle erstellen Befehle anzeigen erstellen Dealloc SQL-Verbindungsfehler akzeptieren erstellte tmp-Disk-Tabellen verzögerte Fehler Flush-Befehle Handler Commit Innodb Buffer Pool Bytes Daten Schlüsselblöcke Nicht Gespült Schlüssel Leseanforderungen Schlüssel Schreib Schlüssel Schreibvorgänge Max Ausführungszeit Überschritten Max Verwendete Verbindungen Open Files Performance Schema Konten Lost Prepared Stmt Count Qcache Freie Blöcke

Fehlerbehebung

Weitere Informationen finden Sie im ["Unterstützung"](#) Seite.

Netstat Data Collector

Cloud Insights verwendet diese Datensammlung, um netstat-Kennzahlen zu sammeln.

Installation

1. Klicken Sie in **Admin > Data Collectors** auf **+Data Collector**. Wählen Sie unter **Services** netstat aus.

Wählen Sie das Betriebssystem oder die Plattform aus, auf dem der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agent für die Sammlung installiert haben oder einen Agent für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das zu erweitern ["Agenten-Installation"](#) Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel für diesen Datensammler aus. Sie können einen neuen Agent-Zugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agent Access Key** klicken. Best Practice: Verwenden Sie einen anderen Agent-Zugriffsschlüssel nur, wenn Sie Datensammler gruppieren möchten, zum Beispiel nach Betriebssystem/Plattform.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.

[Windows Netstat-Konfiguration]

Einrichtung

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Netstat	Node-UUID	Node-IP-Node-Name	

Fehlerbehebung

Weitere Informationen finden Sie im ["Unterstützung"](#) Seite.

Nginx Data Collector

Cloud Insights verwendet diesen Datensammler, um Metriken von Nginx zu erfassen.

Installation

1. Klicken Sie in **Admin > Data Collectors** auf **+Data Collector**. Wählen Sie unter **Services** Nginx.

Wählen Sie das Betriebssystem oder die Plattform aus, auf dem der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agent für die Sammlung installiert haben oder einen Agent für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das zu erweitern "[Agenten-Installation](#)" Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel für diesen Datensammler aus. Sie können einen neuen Agent-Zugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agent Access Key** klicken. Best Practice: Verwenden Sie einen anderen Agent-Zugriffsschlüssel nur, wenn Sie Datensammler gruppieren möchten, zum Beispiel nach Betriebssystem/Plattform.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.

[Linux-Nginx-Konfiguration] [Linux-Nginx-Konfiguration]

Einrichtung

Für die nginx-metrische Sammlung ist Nginx erforderlich "[http_stub_Status_Module](#)" Aktiviert sein.

Weitere Informationen finden Sie im "[Nginx-Dokumentation](#)".

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Nginx	Namespace-Server	Node-IP-Node-Name-Port	Akzeptiert Aktive Bearbeitet Leseanforderungen, Die Auf Das Schreiben Warten

Fehlerbehebung

Weitere Informationen finden Sie im "[Unterstützung](#)" Seite.

PostgreSQL Data Collector

Cloud Insights verwendet diesen Datensammler, um Metriken aus PostgreSQL zu sammeln.

Installation

1. Klicken Sie in **Admin > Data Collectors** auf **+Data Collector**. Wählen Sie unter **Services** die Option PostgreSQL.

Wählen Sie das Betriebssystem oder die Plattform aus, auf dem der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agent für die Sammlung installiert haben oder einen Agent für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das zu erweitern "[Agenten-Installation](#)" Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel für diesen Datensammler aus. Sie können einen neuen Agent-Zugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agent Access Key** klicken. Best Practice: Verwenden Sie einen anderen Agent-Zugriffsschlüssel nur, wenn Sie Datensammler gruppieren möchten,

zum Beispiel nach Betriebssystem/Plattform.

4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.

[PostgreSQL-Konfiguration]

Einrichtung

Informationen finden Sie unter ["PostgreSQL-Dokumentation"](#).

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
PostgreSQL Server	Namespace-Datenbankserver	Node Name Node-IP	Puffer Zugeordnete Buffers Back-End-Puffer Dateisynchronisation Buffers Checkpoint Puffer Clean Checkpoints Sync Time Checkpoints Write Time Checkpoints Requests Checkpoints Timed Max Geschrieben Sauber
PostgreSQL Datenbank	Namespace-Datenbankserver	Datenbank OID Node Name Node IP	Blöcke Lesezeit Blöcke Write Time Blocks Treffer Blöcke Liest Konflikte Deadlocks Client-Nummer Temp-Dateien Bytes Temp-Dateien Anzahl Zeilen Gelöschte Zeilen Abgeholt Zeilen Zeilenanzahl Zeilenanzahl Zeilenanzahl Zeilenumfügen Letzte Transaktionen Letzte Transaktionen Übertragen Rollbacks

Fehlerbehebung

Weitere Informationen finden Sie im ["Unterstützung"](#) Seite.

Puppet Agent Data Collector

Cloud Insights verwendet diesen Datensammler, um Metriken vom Puppet Agent zu erfassen.

Installation

1. Klicken Sie in **Admin > Data Collectors** auf **+Data Collector**. Wählen Sie unter **Services** Puppet.

Wählen Sie das Betriebssystem oder die Plattform aus, auf dem der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agent für die Sammlung installiert haben oder einen Agent für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das zu erweitern "[Agenten-Installation](#)" Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel für diesen Datensammler aus. Sie können einen neuen Agent-Zugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agent Access Key** klicken. Best Practice: Verwenden Sie einen anderen Agent-Zugriffsschlüssel nur, wenn Sie Datensammler gruppieren möchten, zum Beispiel nach Betriebssystem/Plattform.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.

[Puppet-Konfiguration]

Einrichtung

Informationen finden Sie unter "[Puppet-Dokumentation](#)"

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Puppet Agent	Namespace-Node-UUID	Node Name Ort Node-IP- Version Konfigstring Version Puppet	Änderungen Total Events Failure Ereignisse Success Events Summe Ressourcen Geänderte Ressourcen Fehlgeschlagen Ressourcen Konnten Nicht Neu Starten Ressourcen Outofsync Ressourcen Neustart Ressourcen Geplante Ressourcen Übersprungene Ressourcen Gesamtzeit Ankerzeit Abruf Configtime Cron Time Exec Time File Time Filebucket Time Lastrun Time Package Time Zeitplanzeit Service Time Sshauthorizedkey Time Total Time User

Fehlerbehebung

Weitere Informationen finden Sie im ["Unterstützung"](#) Seite.

Redis Data Collector

Cloud Insights verwendet diesen Datensammler, um Kennzahlen von Redis zu sammeln. Redis ist ein Open Source, in-Memory Data Structure Store, der als Datenbank-, Cache- und Nachrichten-Broker verwendet wird und die folgenden Datenstrukturen unterstützt: Strings, Hash-Funktionen, Listen, Sätze und mehr.

Installation

1. Klicken Sie in **Admin > Data Collectors** auf **+Data Collector**. Wählen Sie unter **Services** Redis.

Wählen Sie das Betriebssystem oder die Plattform aus, auf dem der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agent für die Sammlung installiert haben oder einen Agent für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das zu erweitern ["Agenten-Installation"](#) Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel für diesen Datensammler aus. Sie können einen neuen Agent-Zugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agent Access Key** klicken. Best Practice: Verwenden Sie einen anderen Agent-Zugriffsschlüssel nur, wenn Sie Datensammler gruppieren möchten, zum Beispiel nach Betriebssystem/Plattform.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.

[Redis Data Collector Konfiguration]

Einrichtung

Informationen finden Sie unter ["Redis-Dokumentation"](#).

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Redis	Namespace-Server		

Fehlerbehebung

Weitere Informationen finden Sie im ["Unterstützung"](#) Seite.

Copyright-Informationen

Copyright © 2023 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFT SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.