Data Infrastructure Insights -Dokumentation

Data Infrastructure Insights

NetApp
October 16, 2025

This PDF was generated from https://docs.netapp.com/de-de/data-infrastructure-insights/index.html on October 16, 2025. Always check docs.netapp.com for the latest.

Inhalt

Data Infrastructure Insights -Dokumentation . . . 1
Was kann Data Infrastructure Insights für mich tun? . . . 1
Erste Schritte . . . 1
Neuigkeiten bei Data Infrastructure Insights . . . 2
Oktober 2025 . . . 2
Infrastrukturzustand: Sofortige Transparenz bei Speicher- und Fabric-Risiken . . . 2
Multi-Condition-Monitore für präzise Alarmierung . . . 3
Abfrageverbesserungen: Objektdetails auf einen Blick . . . 3
Verbesserungen der Workload-Sicherheit . . . 4
August 2025 . . . 4
Fokussierte Widget-Daten immer zur Hand . . . 4
Dashboards exportieren und importieren . . . 5
Verbesserte Cloud-Integration: Unterstützung für Google Cloud NetApp Volumes (GCNV) . . . 5
Verbesserte StorageGRID -Überwachung . . . 6
Betriebssystemunterstützung . . . 6
Juni 2025 . . . 6
VM Analyzer: Ganzheitliche VM-to-Storage-Transparenz und Fehlerbehebung . . . 6
Betriebssystemunterstützung . . . 7
Mai 2025 . . . 7
Neue Landingpages halten Sie im Flow . . . 7
Verbesserungen der Workload-Sicherheit . . . 7
Asynchroner CSV-Export . . . 9
April 2025 . . . 9
ML-gestützte Anomaliegrenzen in Zeilen-Widgets zur proaktiven Problemlösung . . . 9
Optimieren Sie VMware-Kosten mit VSAN-Speicherunterstützung . . . 10
Alarmdetails immer zur Hand . . . 11
Asynchroner Export der Workload-Sicherheitsforensik . . . 11
In Regeln gruppierte Datensammlerbenachrichtigungen . . . 11
März 2025 . . . 12
Verbesserte Kontextnavigation für effizientes Infrastrukturmanagement . . . 12
Bewahren Sie den Verlauf entfernter Assets auf . . . 12
Kubernetes Operator Push-Button-Upgrade . . . 13
Testen der Konnektivität für Storage Workload Security-Datenkollektoren . . . 14
Betriebssystemunterstützung . . . 14
Februar 2025 . . . 15
DII API-Nutzungsverfolgung: Verbessern Sie Sicherheit und Effizienz . . . 15
Workload Security API zum Einschränken von Benutzern . . . 16
Januar 2025 . . . 16
Proaktives Risikomanagement mit Forensics Grouping . . . 16
Dashboard-Zugriffskontrolle . . . 17
Dezember 2024 . . . 18
Einführung von SAN Analyzer: Verbesserte Sichtbarkeit für Block-Workloads . . . 18
Optimieren Sie VM-Kosten mit intelligenter Host-Stilllegung und VM-Rückgewinnung . . . 19

Entdecken Sie Log-Einblicke mit Zeitdiagrammen und Tabellen-Widget-Unterstützung . . . 20
November 2024 . . . 21
Neue API für Workload-Sicherheitswarnungen . . . 21
Analysieren Sie Konfigurationsänderungen in Ihrer Umgebung . . . 21
KubeVirt-Support: Überwachen Sie die Workloads virtueller Maschinen, die in Ihrem Kubernetes-Cluster ausgeführt werden . . . 21
Oktober 2024 . . . 22
Gewinnen Sie neue Erkenntnisse mit benutzerdefinierten Ausdrücken in Monitoren . . . 22
Minimieren Sie Alarmunterbrechungen während der Wartungszeit . . . 22
Optimieren Sie das Alarmmanagement mit neuen Alarmbenachrichtigungsregeln . . . 23
Log Analytics in Dashboards . . . 24
Bessere VMware-Beobachtbarkeit mit VMware Events . . . 24
Aktualisierungen des Datensammlers: . . . 25
September 2024 . . . 25
Einführung von Data Infrastructure Insights, ehemals Cloud Insights . . . 25
August 2024 . . . 25
Anzeigen spezifischer Daten für Ihren Zeitraum . . . 25
Analyse von Veränderungen und Veränderungsverhältnissen (%) . . . 25
Exportieren Sie die Ergebnisse der Protokollabfrage in eine CSV-Datei . . . 26
Beheben Sie Warnungen nach Zeit . . . 26
Juli 2024 . . . 27
AIOps: Anomalieerkennung . . . 27
Verbesserungen der Workload-Sicherheit . . . 27
Einfachere Dashboard-Navigation . . . 27
Juni 2024 . . . 28
Betriebssystemunterstützung . . . 28
Mai 2024 . . . 28
Automatisches Lösen von Warnmeldungen basierend auf der Zeit . . . 28
April 2024 . . . 29
iSCSI-Unterstützung für Kubernetes . . . 29
Betriebssystemunterstützung . . . 30
März 2024 . . . 30
Details zum Workload Security Agent . . . 30
Schnelleres Darstellen größerer Datenmengen . . . 30
Februar 2024 . . . 31
Verbesserungen der Benutzerfreundlichkeit . . . 31
Alle Änderungen in Ihrem Namespace anzeigen . . . 32
Zugehörige Protokolle für Warnungen . . . 33
Erfassen Sie ONTAP Switch-Daten . . . 33
Workload Security Data Collector-API . . . 33
Januar 2024 . . . 34
Testen Sie Cloud Insights -Funktionen, die Sie noch nicht verwendet haben . . . 34
Wie gesund ist meine Arbeitsbelastung? . . . 34
Datensammler-Updates . . . 34
Verbesserter ML-Algorithmus zur Ransomware-Erkennung . . . 34

Veraltete Funktionalität . . . 35
Dezember 2023 . . . 36
Change Analytics auf einen Blick . . . 36
Kubernetes-Workload-Leistungs-Dashboard . . . 36
Abfragedetails auf einem Bildschirm . . . 37
Aktualisierungen des Datensammlers: . . . 38
November 2023 . . . 38
Workload-Sicherheit: Einen Collector anhalten/fortsetzen . . . 38
Informationen zum Storage Node-Support . . . 39
VMWare-Tags zu Cloud Insights -Anmerkungen zuordnen . . . 39
Verbesserungen der Brocade CLI-Collector-Zuverlässigkeit für FOS 9.1.1c und höhere Firmware . . . 39
Oktober 2023 . . . 39
Verbesserte Workload-Sicherheit . . . 39
Modulversuche . . . 40
Beschränken Sie den Zugriff auf bestimmte Domänen . . . 40
Datensammler-Updates . . . 40
September 2023 . . . 41
Finden Sie ganz einfach, was Sie in den Protokollen suchen . . . 41
„Floating“-Log-Detailbereich . . . 42
Menü einklappen . . . 43
Verbesserungen beim Datensammler . . . 44
August 2023 . . . 44
Sammeln von Isilon/PowerScale-Protokollen und erweiterten Analysedaten . . . 45
Verbesserte Workload-Karte . . . 45
Anpassung der Kubernetes Managed Unit-Nutzung . . . 45
Änderungen beim Sammler/Erwerb: . . . 46
Verbesserte Menüs . . . 46
Juli 2023 . . . 48
Letzte Änderungen anzeigen . . . 48
Verbesserungen für den Operator . . . 48
Einblick: Kühllager zurückgewinnen . . . 49
Bildsignatur des Bedieners . . . 49
Aggregation, bedingte Formatierung und mehr für Abfragen . . . 49
API für Audit . . . 50
Datensammler: Trident Economy . . . 51
Juni 2023 . . . 51
Überprüfen Sie Ihre Nutzung . . . 51
Kubernetes Network Monitoring und Map ist für alle verfügbar . . . 51
Änderungen beim Sammler/Erwerb: . . . 51
Neue ONTAP Essentials Dashboards . . . 52
Zusätzliche Systemmonitore . . . 52
Mai 2023 . . . 52
Verbesserte Installation des Kubernetes-Überwachungsoperators . . . 52
Speichervirtualisierung . . . 52
Neue Webhook-Parameter . . . 53

Berichterstellung zu Kubernetes-Daten . . . 53
Standardmäßige ONTAP -Systemmonitore für Neukunden aktiviert . . . 53
April 2023 . . . 53
Kubernetes-Leistungsüberwachung und -Karte . . . 53
ONTAP Essentials Sicherheits-Dashboard . . . 54
ONTAP Cold Storage zurückgewinnen . . . 55
Die Abonnementbenachrichtigung steuert auch Bannernachrichten . . . 56
Reporting im neuen Look . . . 56
Monitore standardmäßig angehalten . . . 56
Suchen Sie nach der Registerkarte „API-Messung“? . . . 56
März 2023 . . . 57
Cloud Connection für ONTAP 9.9+ veraltet . . . 57
Januar 2023 . . . 57
Neue Protokollmonitore . . . 57
.CSV-Export für alle Dashboard-Tabellen-Widgets . . . 57
Dezember 2022 . . . 57
Entdecken Sie Ransomware-Schutz und andere Sicherheitsfunktionen während der Cloud Insights -Testversion . . . 57
Kubernetes Workloads haben eine eigene Landingpage . . . 58
Überprüfen Sie Ihre Prüfsummen . . . 58
Verbesserungen bei der Protokollwarnung . . . 58
11 neue Standard ONTAP -Monitore für SnapMirror zur Gewährleistung der Geschäftskontinuität . . . 59
November 2022 . . . 59
Mehr als 40 neue Sicherheits-, Datenerfassungs- und CVO-Monitore! . . . 59
Oktober 2022 . . . 59
Bessere und genauere Ransomware-Erkennung mit der ONTAP Autonomous Ransomware Protection-Integration . . . 60
September 2022 . . . 60
Monitore in der Basic Edition verfügbar . . . 60
ONTAP Power- und StorageGRID Dashboards . . . 60
Schwellenwertsichtbarkeit in Tabellen auf einen Blick . . . 60
Sicherheitsmonitor . . . 60
Chatten Sie von überall . . . 61
Mehr sichtbare Einblicke . . . 61
Neue Datensammler . . . 61
Weitere Updates des Datensammlers . . . 61
Betriebssystemunterstützung . . . 61
August 2022 . . . 62
Cloud Insights hat ein neues Aussehen! . . . 62
Sie wissen nicht, wo Sie anfangen sollen? Schauen Sie sich ONTAP Essentials an! . . . 62
Speicherdatenfamilien werden zusammengeführt . . . 63
Wie viel Strom verbraucht mein Speicher? . . . 64
Aus der Vorschau entfernte Funktionen . . . 65
Wie steht es um die Gesundheit meiner Datenerfassung? . . . 65
Automatisch erneuernde API-Token . . . 65

Die Basic Edition bietet Ihnen mehr als je zuvor . . . 66
Möchten Sie mehr erfahren? . . . 66
Betriebssystemunterstützung . . . 66
Juni 2022 . . . 66
Kubernetes-Clustersättigung und andere Details . . . 66
Wie alt ist Ihr Kubernetes-Cluster? . . . 67
Kapazitätsprognose bis zur vollständigen Auslastung . . . 67
Was hat sich in meiner Umgebung geändert? . . . 68
Betriebssystemunterstützung . . . 68
Aktualisierter Telegraf-Agent . . . 68
Vorschaufunktionen . . . 68
Mai 2022 . . . 69
Chatten Sie live mit dem NetApp Support . . . 69
Kubernetes-Operator . . . 69
Verwalten Sie Benutzer und Einladungen mit der API . . . 70
Datenerfassungswarnungen . . . 70
Warnmeldung zu Änderungen am ONTAP -Speicher . . . 70
Vorschaufunktionen . . . 70
April 2022 . . . 71
Teile dein Feedback! . . . 71
Aktualisierter Dashboard-Editor . . . 71
Verbesserte Überwachung Ihrer Kubernetes-Infrastruktur . . . 72
Vorschaufunktionen . . . 72
Neuer Datensammler . . . 73
Weitere Updates des Datensammlers . . . 73
März 2022 . . . 73
Cloud-Verbindung für ONTAP 9.9+ . . . 73
Neue FSx für NetApp ONTAP -Monitore . . . 73
Neue Cloud Secure -Funktionen für alle verfügbar . . . 74
Aktualisierter Telegraf-Agent . . . 74
Datensammler-Updates . . . 74
Februar 2022 . . . 74
Cloud Insights behebt Apache Log4j-Schwachstellen . . . 74
Kubernetes-Namespace-Detailseite . . . 74
Dezember 2021 . . . 75
Tiefere Integration für ONTAP -Systeme . . . 75
Abfragen von Protokollen . . . 75
Benachrichtigungen auf Datensammlerebene. . . . 76
Größere Flexibilität der Cloud Secure -Rollen . . . 76
Betriebssystemunterstützung . . . 76
Datensammler-Updates . . . 76
November 2021 . . . 77
Adaptive Dashboards . . . 77
Zugriff auf die Berichtsdatenbank über die API . . . 78
Pod-Tabellen auf der VM-Landingpage . . . 78

Datensammler-Updates . . . 78
Weitere unterstützte Betriebssysteme . . . 79
Oktober 2021 . . . 79
Filter auf K8S Explorer-Seiten . . . 79
K8s-Daten für die Berichterstattung . . . 79
Das dunkle Design ist da . . . 80
Datensammler-Unterstützung . . . 80
September 2021 . . . 80
Leistungsrichtlinien sind jetzt Monitore . . . 80
Autovervollständigungsvorschläge, Platzhalter und Ausdrücke in Monitoren . . . 80
Aktualisierter Telegraf-Agent . . . 81
Datensammler-Unterstützung . . . 81
August 2021 . . . 82
Neue Benutzeroberfläche der Audit-Seite . . . 82
Verbesserte Benutzerrollenverwaltung . . . 82
Juni 2021 . . . 82
Autovervollständigungsvorschläge, Platzhalter und Ausdrücke in Filtern . . . 82
Verfügbare APIs nach Edition . . . 83
Kubernetes PV und Pod-Sichtbarkeit . . . 83
Kubernetes-Knoten-zu-VM-Links . . . 83
Alert-Monitore ersetzen Leistungsrichtlinien . . . 84
Cloud Secure unterstützt NFS . . . 85
Cloud Secure -Snapshot-Bereinigung . . . 85
Geschwindigkeit der Cloud Secure Datenerfassung . . . 85
Juni 2021 . . . 85
Aktualisierter Telegraf-Agent . . . 85
Hinzufügen von Korrekturmaßnahmen zu einer Warnung . . . 86
Cloud Insights -APIs für alle Editionen . . . 86
April 2021 . . . 86
Einfachere Verwaltung von Monitoren . . . 87
Erweiterte Warnoptionen durch Webhooks . . . 87
Verbesserte Geräteidentifikation . . . 87
Sie haben nach mehr gefragt! . . . 88
Mehrere Abonnements in einer Cloud Insights Umgebung . . . 88
Wähle deinen Weg . . . 88
Einfacheres, Cloud Secure -Onboarding . . . 88
Februar 2021 . . . 89
Aktualisierter Telegraf-Agent . . . 89
Cloud-Kostenanalysator . . . 89
Abfragen von Objekten mit Nullwerten mithilfe von Filtern . . . 90
Unterstützung mehrerer Regionen . . . 90
Januar 2021 . . . 90
Zusätzliche ONTAP -Metriken umbenannt . . . 90
Neuer Kubernetes Explorer . . . 92
Dezember 2020 . . . 93

Einfachere Kubernetes-Installation . . . 93
November 2020 . . . 93
Zusätzliche Dashboards . . . 93
Spaltenumbenennung in Tabellen-Widgets . . . 93
Oktober 2020 . . . 94
Standarderweiterung von Integrationsdaten . . . 94
Technischer Support für die Basic Edition . . . 94
Cloud Secure -API . . . 94
September 2020 . . . 94
Abfrageseite mit Integrationsdaten . . . 94
Formatierung der Einheitenanzeige im Tabellen-Widget . . . 95
Detailseite der Erfassungseinheit . . . 95
Cloud Secure Docker-Abhängigkeit entfernt . . . 95
Berichterstellung für Benutzerrollen . . . 95
Neue API-Kategorie für die Datenaufnahme . . . 96
August 2020 . . . 96
Überwachung und Alarmierung . . . 96
Juli 2020 . . . 97
Cloud Secure *Snapshot erstellen* Aktion . . . 97
Metrik-/Zähleraktualisierungen . . . 98
Cloud Secure – Erkennung potenzieller Angriffe . . . 99
Abonnieren Sie die Premium Edition über AWS . . . 100
Erweitertes Tabellen-Widget . . . 100
Metrikfilterung . . . 102
ONTAP Advanced Counter-Daten . . . 102
Erweiterte Zähler-Dashboards . . . 104
Weitere Informationen . . . 104
Menü „Richtlinien und Verstöße“ . . . 104
Aktualisierter Telegraf-Agent . . . 104
Juni 2020 . . . 105
Vereinfachte Fehlerberichterstattung des Datensammlers . . . 105
Widget-Verbesserungen . . . 105
Mai 2020 . . . 106
Berichterstellung für Benutzerrollen . . . 106
Cloud Secure -Sicherheitsupdates . . . 107
Dashboard-Gruppierung . . . 107
Dashboard-Pinnung . . . 108
TV-Modus und automatische Aktualisierung . . . 108
April 2020 . . . 109
Neue Zeitbereichsauswahl im Dashboard . . . 109
Cloud Secure -Sicherheitsupdates . . . 109
Standard-Dashboard-Zeit . . . 109
Optimierte Aggregationszeiten . . . 109
Automatische Formatierung der Anzeigeeinheit . . . 109
Anmerkungen mithilfe der API importieren . . . 110

Einfacherer Widget-Selektor . . . 110
Februar 2020 . . . 111
API mit Premium Edition . . . 111
Erste Abfrage nach dem Hinzufügen eines Datensammlers . . . 111
Einfachere Widget-Duplizierung . . . 112
Einmaliges Anmelden (SSO) . . . 112
Januar 2020 . . . 112
Swagger-Dokumentation für REST-API . . . 113
Fortschrittsbalken für Feature-Tutorials . . . 113
Änderungen an der Erfassungseinheit . . . 113
Optimierte Zeitaggregation in Widgets . . . 113
Vereinfachter Prozess „Erste Schritte mit Cloud Insights“ . . . 113
Onboarding von Data Infrastructure Insights . . . 115
Erstellen Ihres NetApp Console . . . 115
Was ist, wenn ich bereits über eine NetApp Console verfüge? . . . 115
Starten Sie Ihre kostenlose Testversion von Data Infrastructure Insights . . . 115
Sign in und los gehts . . . 116
Abmelden . . . 116
Inaktivitäts-Timeout . . . 116
Sicherheit . . . 117
Data Infrastructure Insights Sicherheit . . . 117
Sicherheitsübersicht . . . 117
Informationen und Region . . . 119
Welche Informationen speichert Data Infrastructure Insights ? . . . 119
Wo werden meine Informationen gespeichert? . . . 120
Weitere Informationen . . . 121
SecurityAdmin-Tool . . . 121
Überlegungen zu Upgrades und Installationen . . . 122
Verwalten der Sicherheit auf der Erfassungseinheit . . . 122
Bevor Sie beginnen . . . 122
Verwenden des SecurityAdmin-Tools . . . 122
Festlegen eines Benutzers zum Ausführen des Tools . . . 124
Aktualisieren oder Entfernen des Proxys . . . 125
Externer Schlüsselabruf . . . 127
Verschlüsseln eines Passworts zur Verwendung in der API . . . 127
Erste Schritte . . . 131
Daten sammeln . . . 131
Erste Schritte beim Sammeln von Daten . . . 131
Anforderungen an die Erfassungseinheit . . . 133
Konfigurieren von Erfassungseinheiten . . . 136
Konfigurieren eines Agenten zum Sammeln von Daten (Windows/Linux) . . . 143
Konfigurieren von Datenkollektoren . . . 155
Ermitteln des Erfassungsstatus des Datensammlers . . . 155
Verwalten konfigurierter Datenkollektoren . . . 156
Untersuchung eines gescheiterten Datensammlers . . . 158

Dashboards importieren . . . 159
Importieren aus der Dashboard-Galerie . . . 159
Importieren eines exportierten Dashboards . . . 159
Benutzerkonten und Rollen . . . 159
Berechtigungsstufen . . . 160
Erstellen von Konten durch Einladen von Benutzern . . . 163
Ändern der Rolle eines vorhandenen Benutzers . . . 164
Löschen von Benutzern . . . 165
Single Sign-On (SSO) und Identitätsföderation . . . 165
Zugriffsbeschränkung nach Domäne . . . 168
Data Infrastructure Insights Datensammlerliste . . . 170
Abonnieren von Data Infrastructure Insights . . . 174
Testversion . . . 174
Testversion über AWS Marketplace . . . 175
Was ist, wenn meine Testversion abgelaufen ist? . . . 175
Was ist, wenn mein **Abonnement** abgelaufen ist? . . . 175
Modulbewertung . . . 175
Schätzer . . . 176
Abonnementoptionen . . . 177
Beobachtbarkeitsmessung . . . 177
Workload-Sicherheitsmessung . . . 178
Wie abonniere ich? . . . 178
Abonnieren Sie direkt über den NetApp Vertrieb . . . 178
Selbstabonnement über AWS Marketplace . . . 178
Zeigen Sie Ihren Abonnementstatus an . . . 179
Zeigen Sie Ihr Nutzungsmanagement an . . . 180
Was passiert, wenn ich meinen abonnierten Verbrauch überschreite? . . . 180
Direkt abonnieren und die Testphase überspringen . . . 181
Hinzufügen einer Berechtigungs-ID . . . 181
Beobachtbarkeit . . . 182
Dashboards erstellen . . . 182
Dashboards – Übersicht . . . 182
Dashboard-Funktionen . . . 186
Beispiel-Dashboards . . . 220
Best Practices für Dashboards und Widgets . . . 225
Arbeiten mit Abfragen . . . 228
In Abfragen verwendete Assets . . . 228
Erstellen von Abfragen . . . 230
Anzeigen von Abfragen . . . 237
Exportieren von Abfrageergebnissen in eine CSV-Datei . . . 238
Ändern oder Löschen einer Abfrage . . . 239
Zuweisen mehrerer Anwendungen zu oder Entfernen mehrerer Anwendungen von Assets . . . 240
Tabellenwerte kopieren . . . 241
Protokoll-Explorer . . . 241
Identifizieren inaktiver Geräte . . . 247

Einblicke . . . 248
Einblicke . . . 248
Einblicke: Gemeinsam genutzte Ressourcen unter Druck . . . 248
Einblicke: Kubernetes-Namespaces haben nicht mehr genügend Speicherplatz . . . 251
Einblicke: ONTAP Cold Storage zurückgewinnen . . . 252
Monitore und Warnungen . . . 255
Alarmierung mit Monitoren . . . 255
Anzeigen und Verwalten von Warnungen von Monitoren . . . 265
Konfigurieren von E-Mail-Benachrichtigungen . . . 268
Anomalieerkennungsmonitore . . . 271
Systemmonitore . . . 275
Konfigurieren von E-Mail-Benachrichtigungen . . . 363
Webhook-Benachrichtigungen . . . 366
Arbeiten mit Anmerkungen . . . 380
Anmerkungen definieren . . . 380
Verwenden von Anmerkungen . . . 383
Erstellen von Anmerkungsregeln . . . 385
Anmerkungen importieren . . . 387
Arbeiten mit Anwendungen . . . 390
Nachverfolgen der Asset-Nutzung nach Anwendung . . . 390
Erstellen von Anwendungen . . . 390
Automatische Geräteauflösung . . . 391
Übersicht über die automatische Geräteauflösung . . . 392
Regeln zur Geräteauflösung . . . 394
Fibre Channel-Geräteauflösung . . . 397
IP-Geräteauflösung . . . 399
Einstelloptionen auf der Registerkarte „Einstellungen“ . . . 401
Beispiele für reguläre Ausdrücke . . . 402
Informationen zur Asset-Seite . . . 409
Übersicht über die Asset-Seite . . . 409
Filtern nach Objekten im Kontext . . . 415
Speichervirtualisierung . . . 416
Hinweise und Tipps zur Suche nach Assets und Warnungen . . . 418
Daten analysieren . . . 420
SAN Analyzer – Übersicht . . . 420
VM Analyzer – Übersicht . . . 423
Überwachen des Infrastrukturzustands . . . 425
Berichterstattung . . . 427
Übersicht über die Data Infrastructure Insights . . . 427
Benutzerrollen für Data Infrastructure Insights Reporting . . . 428
Vordefinierte Berichte leicht gemacht . . . 430
Storage Manager-Dashboard . . . 433
Erstellen eines Berichts (Beispiel) . . . 437
Berichte verwalten . . . 440
Erstellen benutzerdefinierter Berichte . . . 444

Zugriff auf die Berichtsdatenbank über die API . . . 451
So werden historische Daten für die Berichterstellung aufbewahrt . . . 455
Schemadiagramme für die Data Infrastructure Insights -Berichterstattung . . . 456
Data Infrastructure Insights Schemas für die Berichterstellung . . . 508
Kubernetes . . . 510
Übersicht über Kubernetes-Cluster . . . 510
Verfeinern des Filters . . . 510
Vor der Installation oder Aktualisierung des NetApp Kubernetes Monitoring Operator . . . 511
Wichtige Hinweise vor dem Start . . . 512
Installation und Konfiguration des Kubernetes Monitoring Operators . . . 515
Vor der Installation des Kubernetes Monitoring Operator . . . 515
Installieren des Kubernetes Monitoring Operators . . . 516
Kubernetes-Überwachungskomponenten . . . 518
Upgrade auf den neuesten Kubernetes Monitoring Operator . . . 519
Stoppen und Starten des Kubernetes-Überwachungsoperators . . . 520
Deinstallation . . . 521
Über Kube-State-Metrics . . . 522
Konfigurieren/Anpassen des Operators . . . 522
Eine Anmerkung zu Geheimnissen . . . 526
Überprüfen der Bildsignaturen des Kubernetes-Überwachungsoperators . . . 527
Fehlerbehebung . . . 527
Konfigurationsoptionen für den Kubernetes-Überwachungsoperator . . . 536
Beispieldatei für AgentConfiguration . . . 540
Kubernetes-Cluster-Detailseite . . . 549
Anzahl der Namespaces, Knoten und Pods . . . 550
Gemeinsam genutzte Ressourcen und Sättigung . . . 550
Namensräume . . . 550
Arbeitslasten . . . 551
Das Cluster-„Rad“ . . . 551
Ein Hinweis zu den Messgeräten . . . 554
Überwachung und Zuordnung der Kubernetes-Netzwerkleistung . . . 554
Voraussetzungen . . . 555
Monitore . . . 556
Die Karte . . . 556
Arbeitslastdetails und Warnungen . . . 558
Suchen und Filtern . . . 558
Arbeitslastbezeichnungen . . . 559
Tauchen Sie tief ein . . . 560
Kubernetes-Änderungsanalyse . . . 562
Filtern . . . 563
Schnellstatus . . . 564
Detailbereich . . . 565
ONTAP Essentials . . . 567
Überblick . . . 567
Datensicherung . . . 568

Sicherheit . . . 569
Warnungen . . . 573
Infrastruktur . . . 574
Vernetzung . . . 575
Arbeitslasten . . . 575
Admin und andere Aufgaben . . . 577
API für Data Infrastructure Insights . . . 577
Voraussetzungen für den API-Zugriff . . . 577
API-Dokumentation (Swagger) . . . 577
API-Zugriffstoken . . . 578
API-Typ . . . 579
Bestandsdurchlauf . . . 580
Erweitert . . . 580
Leistungsdaten . . . 582
Objektleistungsmetriken . . . 584
Leistungsverlaufsdaten . . . 584
Objekte mit Kapazitätsattributen . . . 585
Verwenden der Suche zum Nachschlagen von Objekten . . . 586
Deaktivieren oder Widerrufen eines API-Tokens . . . 586
Rotieren abgelaufener API-Zugriffstoken . . . 587
Überwachung Ihrer Umgebung . . . 588
Wirtschaftsprüfung . . . 588
Active IQ Digital Advisor . . . 591
Workload-Sicherheit . . . 594
Informationen zur Speicher-Workload-Sicherheit . . . 594
Sichtweite . . . 594
Schutz . . . 594
Einhaltung . . . 594
Erste Schritte . . . 594
Erste Schritte mit Workload-Sicherheit . . . 594
Anforderungen für den Workload Security Agent . . . 595
Installation des Workload Security Agent . . . 599
Löschen eines Workload Security Agent . . . 607
Konfigurieren eines Active Directory (AD)-Benutzerverzeichnis-Collectors . . . 607
Konfigurieren eines LDAP-Verzeichnisserver-Collectors . . . 613
Konfigurieren des ONTAP SVM-Datenkollektors . . . 619
Fehlerbehebung beim ONTAP SVM Data Collector . . . 629
Konfigurieren des Cloud Volumes ONTAP und Amazon FSx for NetApp ONTAP . . . 637
Benutzerverwaltung . . . 639
SVM-Ereignisratenprüfer (Leitfaden zur Agentendimensionierung) . . . 640
Warnungen . . . 644
Alarm . . . 644
Filteroptionen . . . 646
Die Seite „Warnungsdetails“ . . . 646
Aktion „Schnappschuss machen“ . . . 648

Warnmeldungen . . . 649
Aufbewahrungsrichtlinie . . . 649
Fehlerbehebung . . . 650
Forensik . . . 650
Forensik – Alle Aktivitäten . . . 650
Forensische Benutzerübersicht . . . 661
Richtlinien für automatisierte Antworten . . . 662
Richtlinien für zulässige Dateitypen . . . 664
Integration mit ONTAP Autonomous Ransomware Protection . . . 665
Voraussetzungen . . . 666
Erforderliche Benutzerberechtigungen . . . 666
Beispielwarnung . . . 666
Einschränkungen . . . 667
Fehlerbehebung . . . 667
Integration mit ONTAP Access Denied . . . 668
Voraussetzungen . . . 668
Erforderliche Benutzerberechtigungen . . . 669
Ereignisse vom Typ „Zugriff verweigert“ . . . 669
Blockieren des Benutzerzugriffs . . . 670
Voraussetzungen für die Benutzerzugriffssperre . . . 670
Wie aktiviere ich die Funktion? . . . 671
Wie richte ich die automatische Sperrung des Benutzerzugriffs ein? . . . 671
Wie kann ich feststellen, ob es im System blockierte Benutzer gibt? . . . 671
Manuelles Einschränken und Verwalten des Benutzerzugriffs . . . 671
Verlauf der Benutzerzugriffsbeschränkungen . . . 672
Wie deaktiviere ich die Funktion? . . . 672
Manuelles Wiederherstellen von IPs für NFS . . . 672
Manuelles Wiederherstellen von Benutzern für SMB . . . 673
Fehlerbehebung . . . 674
Workload-Sicherheit: Simulation eines Angriffs . . . 675
Dinge, die Sie vor dem Beginn beachten sollten . . . 676
Richtlinien: . . . 676
Schritte: . . . 676
Generieren Sie die Beispieldateien programmgesteuert: . . . 677
Fortsetzen des Collectors . . . 678
Generieren Sie die Beispieldateien programmgesteuert: . . . 678
Generieren einer Warnung in Workload Security . . . 679
Alarm wird mehrmals ausgelöst . . . 680
Konfigurieren von E-Mail-Benachrichtigungen für Alarme, Warnungen und den Zustand von Agenten/Datenquellen-Sammlern . . . 680
Alarme und Warnungen vor potenziellen Angriffen . . . 680
Integritätsüberwachung für Agenten und Datensammler . . . 680
Empfangen von Agent- und Data Collector-Upgrade-Benachrichtigungen . . . 681
Fehlerbehebung . . . 681
Webhook-Benachrichtigungen . . . 681

Workload-Sicherheitsbenachrichtigungen mithilfe von Webhooks . . . 681
Workload Security Webhook-Beispiel für Discord . . . 687
Workload Security Webhook-Beispiel für PagerDuty . . . 690
Workload Security Webhook-Beispiel für Slack . . . 695
Beispiel für einen Workload-Sicherheits-Webhook für Microsoft Teams . . . 699
Workload-Sicherheits-API . . . 703
API-Dokumentation (Swagger) . . . 704
API-Zugriffstoken . . . 704
Skript zum Extrahieren von Daten über die API . . . 705
Fehlerbehebung beim ONTAP SVM Data Collector . . . 705
Fehlerbehebung . . . 714
Fehlerbehebung bei allgemeinen Problemen mit Data Infrastructure Insights . . . 714
Anmeldeprobleme . . . 714
Andere Probleme . . . 715
Ressourcen . . . 716
Fehlerbehebung bei Problemen mit der Erfassungseinheit unter Linux . . . 716
Überlegungen zu Proxys und Firewalls . . . 718
Ressourcen . . . 719
Fehlerbehebung bei Problemen mit der Erfassungseinheit unter Windows . . . 720
Überlegungen zu Proxys und Firewalls . . . 722
Ressourcen . . . 722
Untersuchung eines gescheiterten Datensammlers . . . 723
Data Infrastructure Insights Datensammler-Supportmatrix . . . 724
HP Enterprise 3PAR / Alletra 9000 / Primera StoreServ Storage . . . 724
Amazon AWS EC2 . . . 743
Amazon AWS S3 . . . 749
Microsoft Azure NetApp Files . . . 753
Brocade Fibre Channel Switches . . . 762
Brocade Network Advisor HTTP . . . 773
Brocade FOS REST . . . 777
Cisco MDS- und Nexus Fabric-Switches . . . 785
Zusammenhalt . . . 793
EMC Celerra (SSH) . . . 802
EMC CLARiiON (NaviCLI) . . . 811
EMC-Datendomäne (SSH) . . . 828
EMV ECS . . . 837
Dell EMC Isilon und PowerScale Rest . . . 847
Dell EMC Isilon / PowerScale (CLI) . . . 866
EMC PowerStore REST . . . 882
EMC RecoverPoint (HTTP) . . . 898
EMC ScaleIO und PowerFlex REST . . . 901
EMC Symmetrix-CLI . . . 907
Dell Unisphere REST . . . 927
EMC VNX (SSH) . . . 944
EMC VNXe und Unity Unisphere (CLI) . . . 964

EMC VPLEX 978
EMC XtremIO (HTTP) 987
NetApp E-Serie 1001
Pure Storage FlashBlade REST 1016
Google Cloud Compute 1026
Google Cloud Netapp Volumes 1031
HDS HCP (HTTPS) 1042
HiCommand-Gerätemanager 1047
Hitachi Ops Center 1061
HDS HNAS (CLI) 1077
HPE Nimble / Alletra 6000 Storage 1086
Huawei OceanStor (REST/HTTPS) 1098
IBM Cleversafe 1117
IBM DS 8K (DSCLI) 1122
IBM PowerVM (SSH) 1135
IBM SVC (CLI) 1138
IBM XIV und A9000 (XIVCLI) 1155
Infinidat Infinibox (HTTP) 1160
Microsoft Azure Compute 1169
Microsoft Hyper-V 1175
NetApp 7-Modus 1185
NetApp E-Serie REST 1212
Amazon FSx for NetApp ONTAP 1221
NetApp Clustered Data ONTAP 8.1.1+ 1243
ASA 1284
NetApp ONTAP REST 1298
NetApp SolidFire 8.1+ 1320
NetApp StorageGRID (HTTPS) 1337
Nutanix-Speicher (REST) 1347
OpenStack (REST-API / SSH) 1360
Oracle ZFS (HTTPS) 1364
Pure Storage FlashArray (HTTP) 1378
Red Hat RHV (REST) 1392
Rubrik Storage 1396
VAST DataStore 1407
NetApp HCI Virtual Center 1418
VMware Cloud auf AWS 1428
VMware vSphere (Webdienste) 1434
Referenz & Support 1448
Support anfordern 1448
Supportanspruch aktivieren 1448
Supportinformationen erhalten 1451
Data Infrastructure Insights Datensammler-Supportmatrix 1452
Datensammlerreferenz – Infrastruktur 1453
Anbieterspezifische Referenz 1453

Konfigurieren des Amazon EC2-Datensammlers . . . 1453
Amazon FSx for NetApp ONTAP Datenkollektor . . . 1456
Konfigurieren des Azure-Compute-Datensammlers . . . 1459
Broadcom . . . 1460
Cisco MDS Fabric Switches Datensammler . . . 1468
Cohesity SmartFiles-Datensammler . . . 1471
Dell . . . 1472
Dell EMC . . . 1472
Fujitsu Eternus Datensammler . . . 1499
NetApp Google Compute-Datenkollektor . . . 1500
Google Cloud NetApp Volumes Datensammler . . . 1501
HP Unternehmen . . . 1503
Hitachi-Datensysteme . . . 1511
Infinidat InfiniBox Datensammler . . . 1519
Huawei OceanStor Datensammler . . . 1521
IBM . . . 1522
Lenovo Datensammler . . . 1531
Microsoft . . . 1532
NetApp . . . 1534
Nutanix NX-Datensammler . . . 1570
Oracle ZFS Storage Appliance-Datenkollektor . . . 1571
Pure Storage FlashArray-Datensammler . . . 1574
Red Hat Virtualization-Datenkollektor . . . 1575
Rubrik CDM-Datensammler . . . 1576
Konfigurieren des VMware VSphere-Datenkollektors . . . 1578
Datensammlerreferenz – Dienste . . . 1581
Knotendatenerfassung . . . 1581
ActiveMQ-Datensammler . . . 1584
Apache-Datensammler . . . 1586
Konsul-Datensammler . . . 1589
Couchbase-Datensammler . . . 1590
CouchDB-Datensammler . . . 1592
Docker-Datensammler . . . 1594
Elasticsearch-Datensammler . . . 1602
Flink-Datensammler . . . 1604
Hadoop-Datensammler . . . 1611
HAProxy-Datensammler . . . 1616
JVM-Datensammler . . . 1624
Kafka-Datensammler . . . 1628
Kibana-Datensammler . . . 1631
Installation und Konfiguration des Kubernetes Monitoring Operators . . . 1633
Memcached-Datensammler . . . 1654
MongoDB-Datensammler . . . 1657
MySQL-Datensammler . . . 1659
Netstat-Datensammler . . . 1664

Nginx-Datensammler . . . 1665
PostgreSQL-Datensammler . . . 1668
Puppet Agent-Datensammler . . . 1670
Redis-Datensammler . . . 1672
Objektsymbolreferenz . . . 1674
Infrastruktursymbole: . . . 1674
Kubernetes-Symbole: . . . 1674
Überwachung der Netzwerkleistung von Kubernetes und Kartensymbole: . . . 1675
Rechtliche Hinweise . . . 1676
Copyright . . . 1676
Marken . . . 1676
Patente . . . 1676
Datenschutzrichtlinie . . . 1676
Open Source . . . 1676

Data Infrastructure Insights -Dokumentation

NetApp Data Infrastructure Insights (ehemals Cloud Insights) ist ein Tool zur Überwachung der Cloud-Infrastruktur, das Ihnen Einblick in Ihre gesamte Infrastruktur bietet. Mit Data Infrastructure Insights können Sie alle Ihre Ressourcen, einschließlich Ihrer öffentlichen Clouds und Ihrer privaten Rechenzentren, überwachen, Fehler beheben und optimieren.

Was kann Data Infrastructure Insights für mich tun?

Data Infrastructure Insights bietet hybrides Multicloud-Monitoring und verschafft Ihnen so vollständige Transparenz über Infrastruktur und Workloads.

- Datensammler für heterogene Infrastrukturen und Workloads, einschließlich Kubernetes
- Offener Telegraf-Collector und offene APIs für einfache Integration
- Umfassende Alarmierung und Benachrichtigungen
- Maschinelles Lernen für intelligente Erkenntnisse
- Optimieren Sie die Ressourcennutzung
- Integrierte oder anpassbare Dashboards mit erweiterten Filtern zur Minimierung von Anzeigestörungen bei der Beantwortung von Fragen
- Ermitteln Sie den Zustand Ihrer ONTAP Speichervorgänge
- Schützen Sie Ihr wertvollstes Geschäftsgut – Ihre Daten – vor Ransomware oder Datenzerstörungsangriffen

---

Erste Schritte

- Wie kann ich**loslegen** mit Data Infrastructure Insights?
- Ich bin angemeldet. Was mache ich jetzt?"Datenerfassung" "Einrichten von Benutzern"
- Eindrucksvoll! Was kommt als Nächstes?"Vorbereiten von Assets: Kommentieren" "Die gewünschten Assets finden: Abfragen" "Die gewünschten Daten anzeigen: Dashboards" "Überwachung und Warnungen" "Daten sichern"
- Das ist tolles Zeug! Ich bin bereit**abonnieren** .

Neuigkeiten bei Data Infrastructure Insights

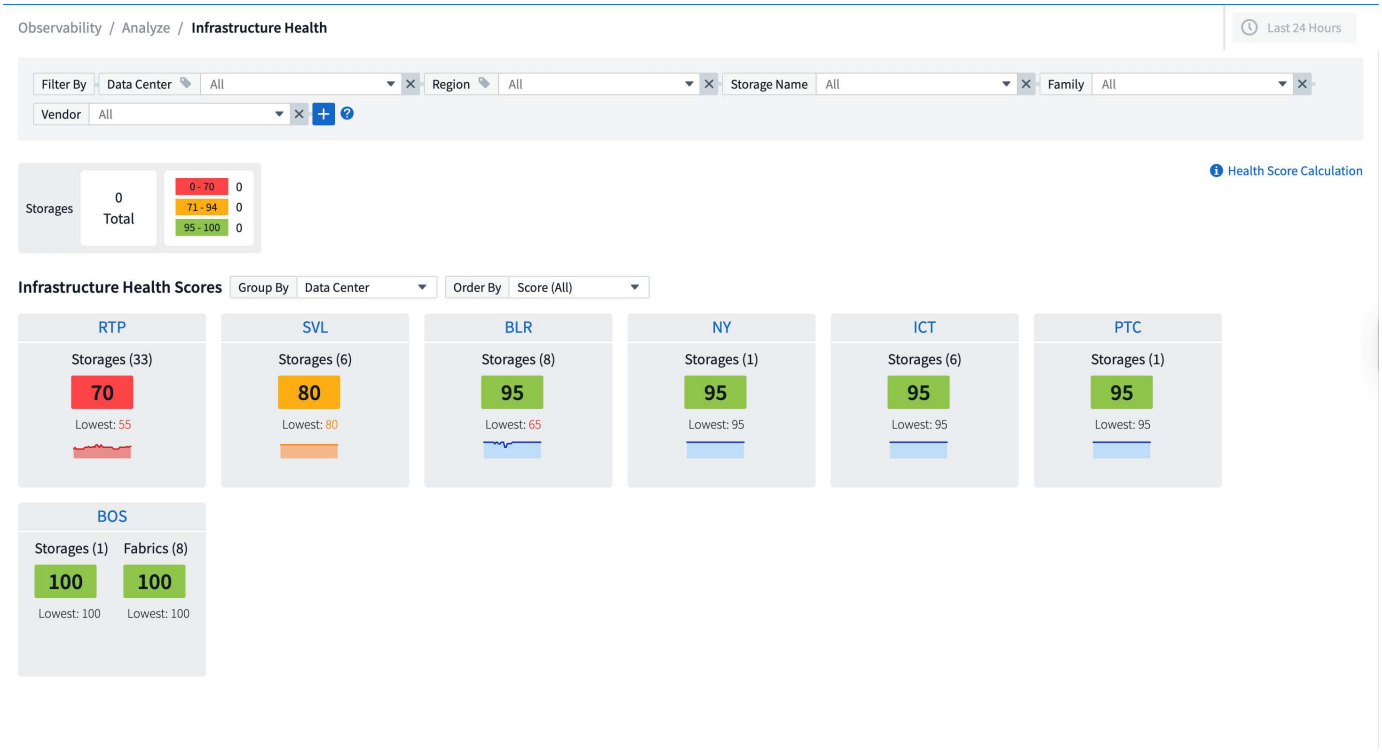
NetApp verbessert und erweitert seine Produkte und Services kontinuierlich. Hier sind einige der neuesten Features und Funktionen, die in Data Infrastructure Insights (ehemals Cloud Insights) verfügbar sind.

Oktober 2025

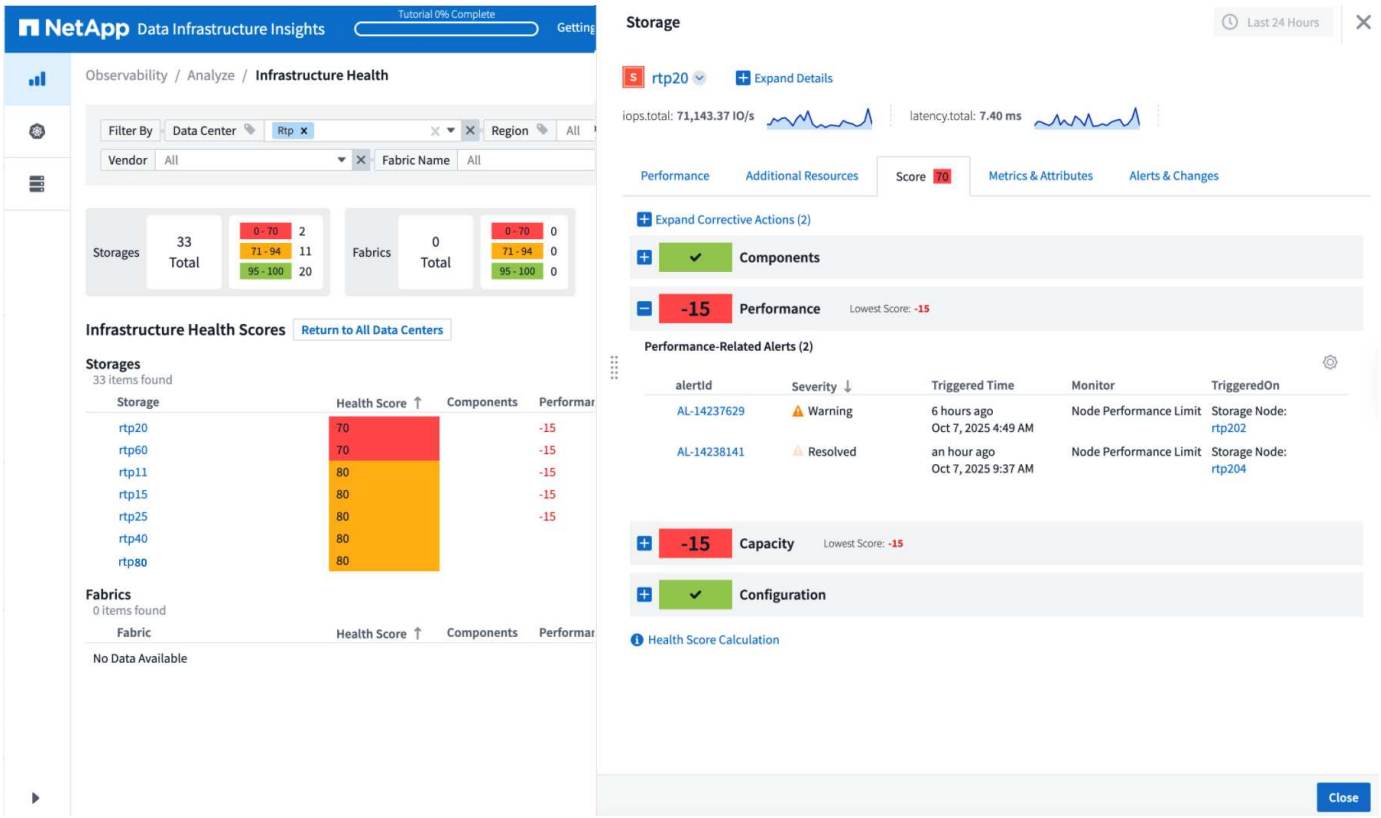
Infrastrukturzustand: Sofortige Transparenz bei Speicher- und Fabric-Risiken

Erhalten Sie mit unserer neuen Funktion „Infrastructure Health“ sofortigen Einblick in potenzielle Risiken in Ihrem Speicher und Ihren Fabrics. Ein einziges, farbcodiertes Dashboard bietet Ihnen eine einheitliche Risikotransparenz und hilft Ihnen, Ausfallzeiten zu minimieren und Umsatzeinbußen schnell zu vermeiden.

Werte unter 100 weisen auf potenzielle Probleme hin; je niedriger der Wert, desto instabiler sind die Ressourcen. Durch die Gruppierung von Ressourcen nach Rechenzentrum oder Region für intuitive, konsolidierte Integritätsbewertungen können Sie kritische Bereiche einfach priorisieren und Fehler beheben.

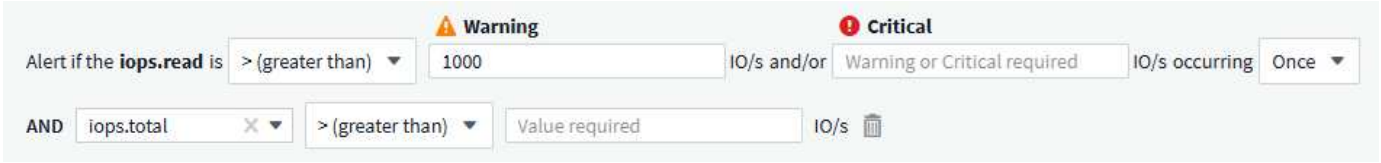


Zeigen Sie mit einem Mausklick detaillierte Informationen in einem ausziehbaren Bildschirmfenster an, um Probleme, die Aufmerksamkeit erfordern, schnell zu erkennen und die Sicherheit und Belastbarkeit Ihrer Systeme zu gewährleisten.



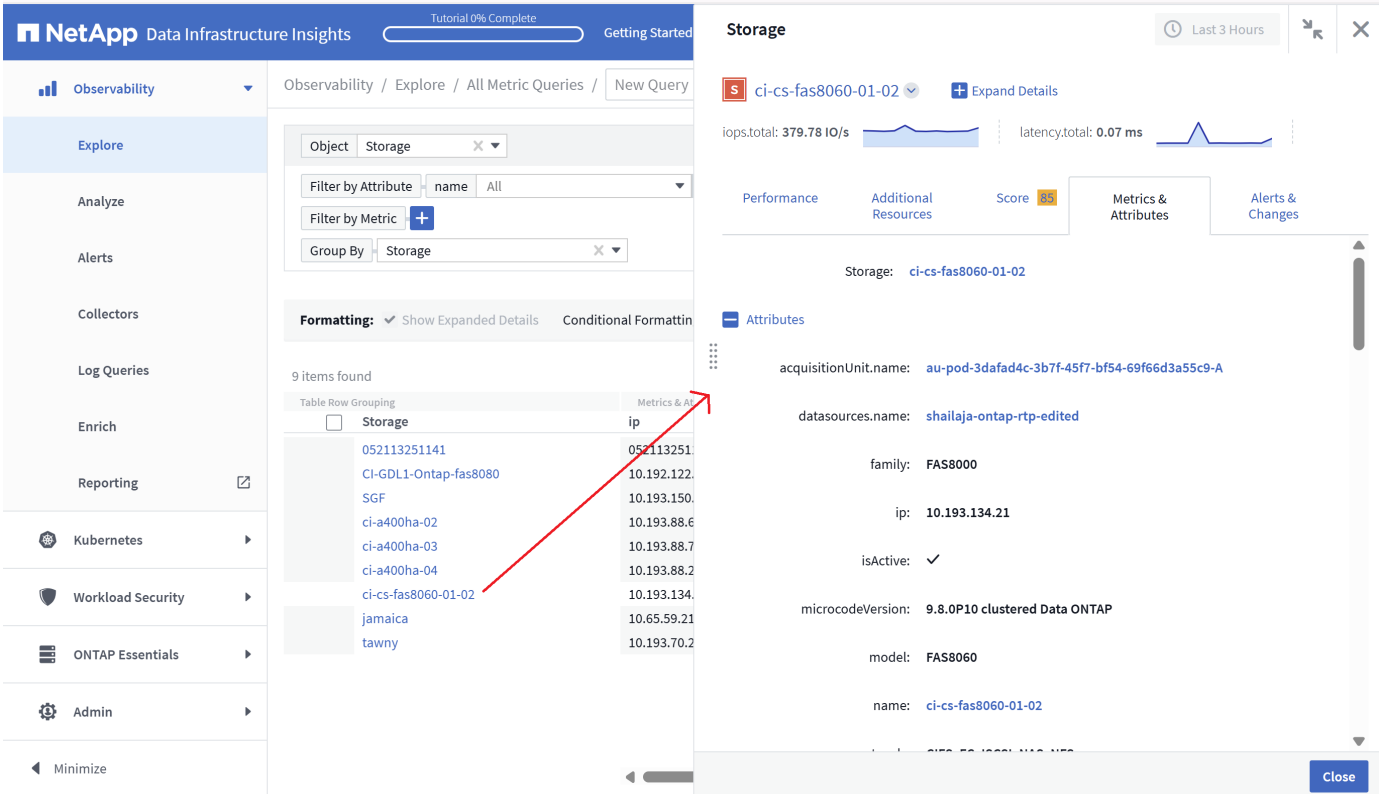
Multi-Condition-Monitore für präzise Alarmierung

Reduzieren Sie Alarmgeräusche und verbessern Sie die Überwachungspräzision, indem Sie jedem Metrikmonitor eine optionale zweite Bedingung hinzufügen. Warnungen werden nur ausgelöst, wenn beide Bedingungen erfüllt sind. So erhalten Sie gezieltere Benachrichtigungen, die sich auf die Szenarien konzentrieren, die für Sie am wichtigsten sind.



Abfrageverbesserungen: Objektdetails auf einen Blick

Durch Auswählen einer Zeile in einer Objektabfrage-Ergebnisliste wird ein Detailbereich für das ausgewählte Objekt geöffnet. Zeigen Sie schnell Metriken und Attribute (die Standardansicht für Objektabfragen), Warnungen und Änderungen, Leistungs- und Integritätswerte an oder erkunden Sie verwandte Ressourcen. Alle relevanten Objektinformationen stehen Ihnen zur Verfügung.



Verbesserungen der Workload-Sicherheit

Zwei neue APIs geben Ihnen mehr Kontrolle über Ihre Workload Security-Umgebung:

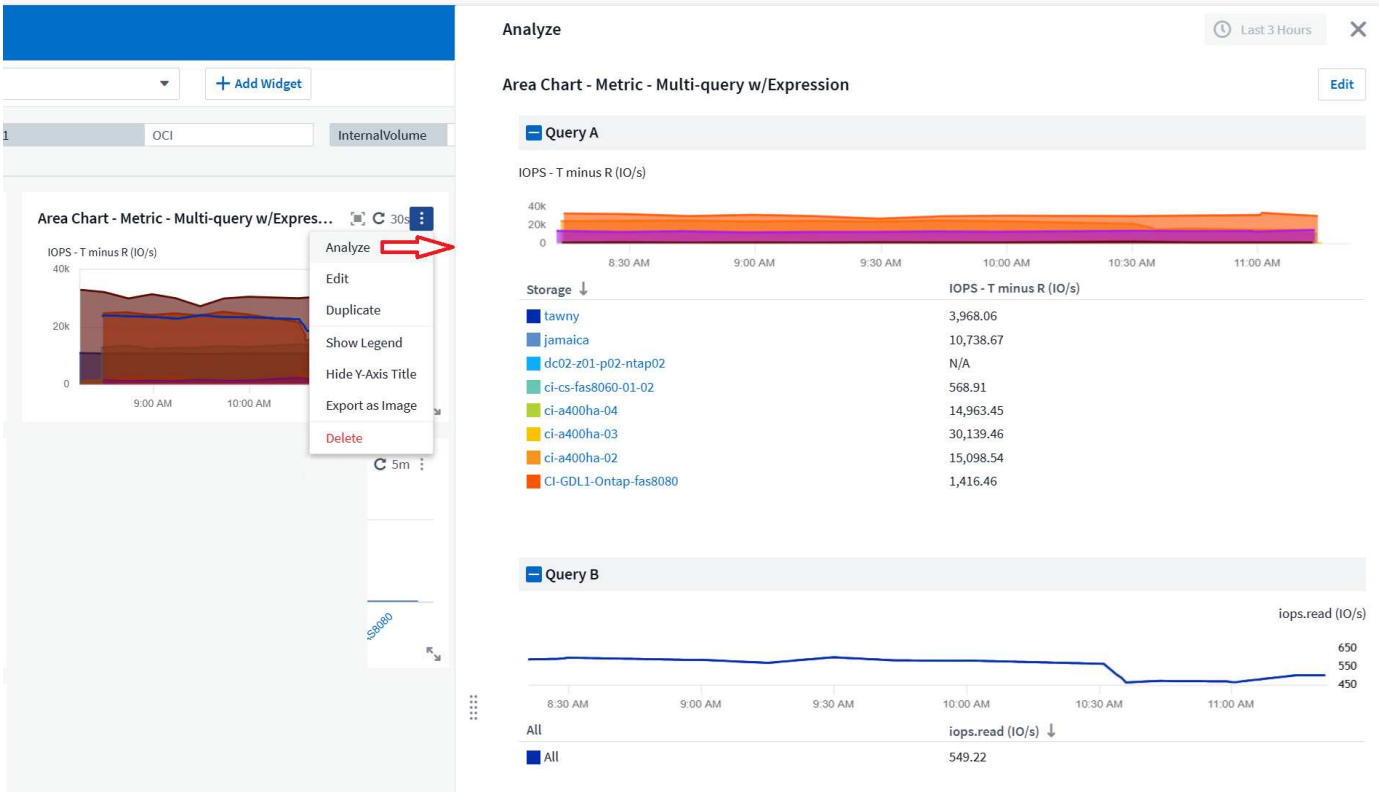
1. Zeigen Sie Gruppen mit *GET /rest/v1/cloudsecure/activities/groups* an und verwalten Sie sie.
2. Datensammler mit *POST /rest/v1/cloudsecure/collectors/{collector-uuid}/status* anhalten und fortsetzen

Darüber hinaus sind die Berechtigungsprüfungen für Workload Security-Rollen jetzt noch sicherer. Aufgrund der verbesserten Sicherheit können bei einigen vorhandenen Benutzern beim Hinzufügen eines Collectors Berechtigungsprobleme auftreten. Bestätigen Sie die Benutzerberechtigungen, indem Sie den Anweisungen im"Dokumentation" .

August 2025

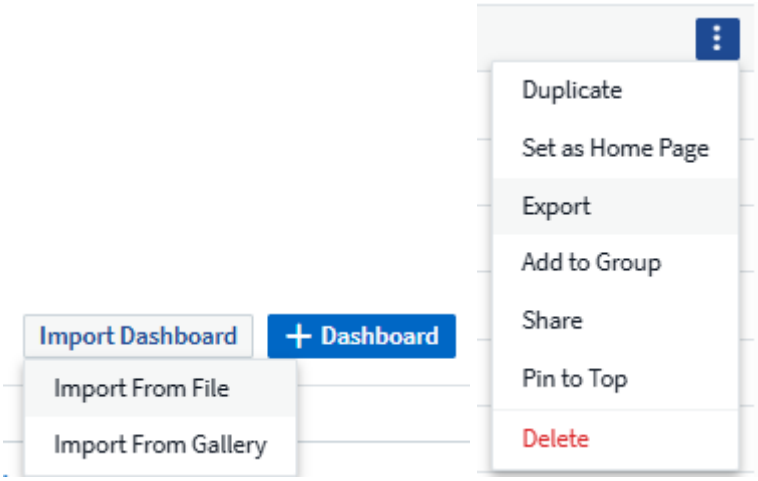
Fokussierte Widget-Daten immer zur Hand

Mit der neuen **Analysieren**-Funktion in den meisten Widgets können Sie die Daten in jeweils einem Widget genauer betrachten. Klicken Sie einfach auf die Schaltfläche „Analysieren“ in einem Widget, um eine Detailansicht zu öffnen, in der Sie die zugrunde liegenden Daten interaktiv erkunden und für tiefere Einblicke hineinzoomen können – ohne den Kontext Ihres Dashboards zu verlassen.



Dashboards exportieren und importieren

Wenn Sie mehrere Mandanten verwalten und ein nützliches Dashboard entwickelt haben, können Sie das Dashboard exportieren und in einen anderen Mandanten importieren.



Verbesserte Cloud-Integration: Unterstützung für Google Cloud NetApp Volumes (GCNV)

- Google Cloud NetApp Volumes* (GCNV) wird jetzt als Datensammler in DII vollständig unterstützt und vervollständigt unser Ökosystem für die Hybrid-Cloud-Überwachung. Erhalten Sie Einblick in kritische Speicherobjekte wie Organisationen, Pools und Volumes in der gesamten Infrastruktur. Jetzt können Sie alle Ihre Speicherumgebungen – vor Ort oder in der Cloud – von einer einzigen Plattform aus verfolgen.

Verbesserte StorageGRID -Überwachung

Die StorageGRID Protokollsammlung ist jetzt standardmäßig aktiviert und stellt DII Ereignisverfolgungsdaten bereit. Außerdem haben wir die StorageGrid-Überwachung um über 50 Standardwarnungen, Echtzeit-Ereignisverfolgung und neue Dashboards erweitert, um komplexe Speichernetzvorgänge zu vereinfachen. Bleiben Sie Problemen immer einen Schritt voraus, indem Sie tiefere Einblicke in Verkehrsrichtlinien und Bucket-Leistung erhalten.

Betriebssystemunterstützung

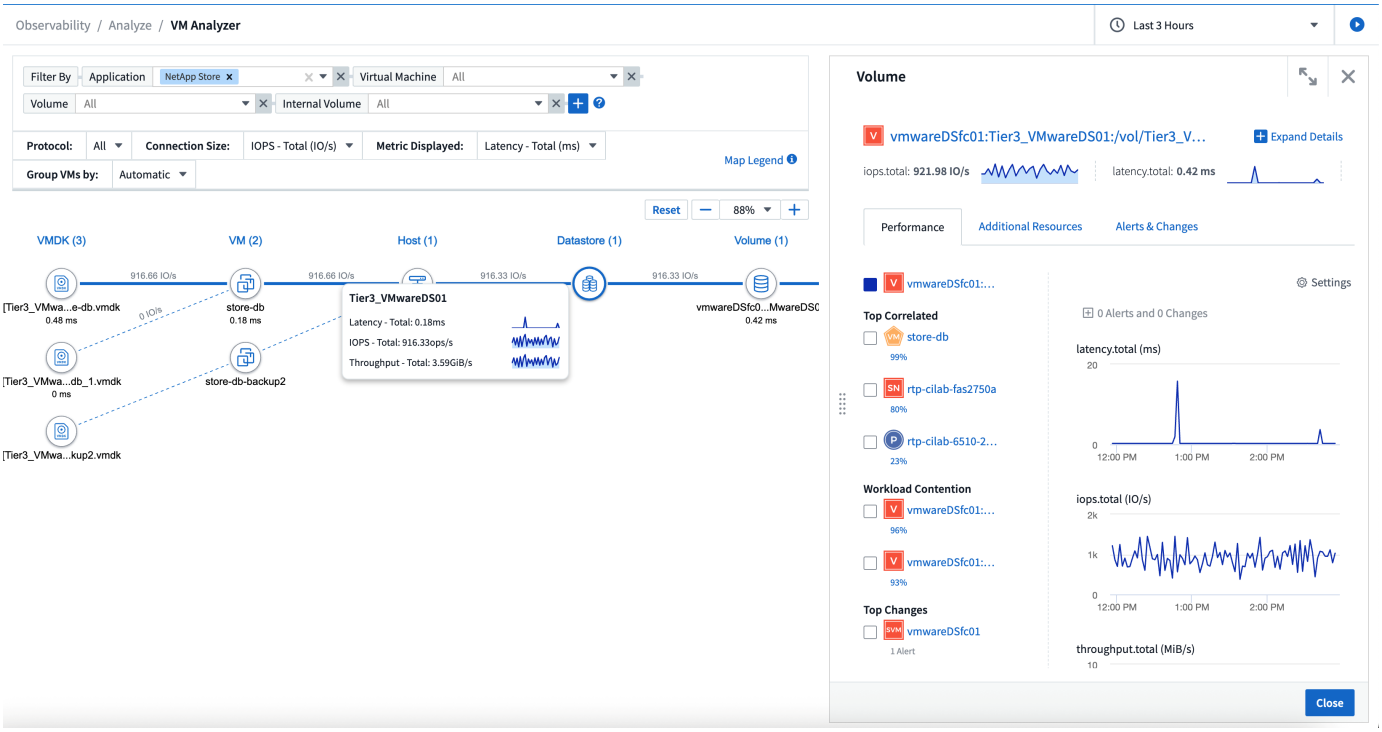
Die folgenden Betriebssysteme werden jetzt mit Data Infrastructure Insights Acquisition Units unterstützt, zusätzlich zu denen"bereits unterstützt" :

- AlmaLinux (64-Bit) 10
- Red Hat (64-Bit) 10
- Rocky (64-Bit) 9.6

Juni 2025

VM Analyzer: Ganzheitliche VM-to-Storage-Transparenz und Fehlerbehebung

Die **VM Analyzer**-Funktion von DII bietet eine umfassende End-to-End-Ansicht Ihrer virtualisierten Umgebungen. Der VM Analyzer vereinfacht die Fehlerbehebung, indem er den gesamten Pfad von virtuellen Maschinen zum Speicher abbildet. So können Benutzer Leistungsprobleme bei virtuellen Datenträgern, VMs, Hosts, Datenspeichern, Volumes und Speichern schnell lokalisieren. Mit einer intuitiven Topologieansicht, Filterung und detaillierten Leistungsmetriken können Administratoren Engpässe leicht erkennen, Verkehrsungleichgewichte analysieren und die Gesamtspeicherleistung optimieren.



Betriebssystemunterstützung

Die folgenden Betriebssysteme werden jetzt mit Data Infrastructure Insights Acquisition Units unterstützt, zusätzlich zu denen"bereits unterstützt" :

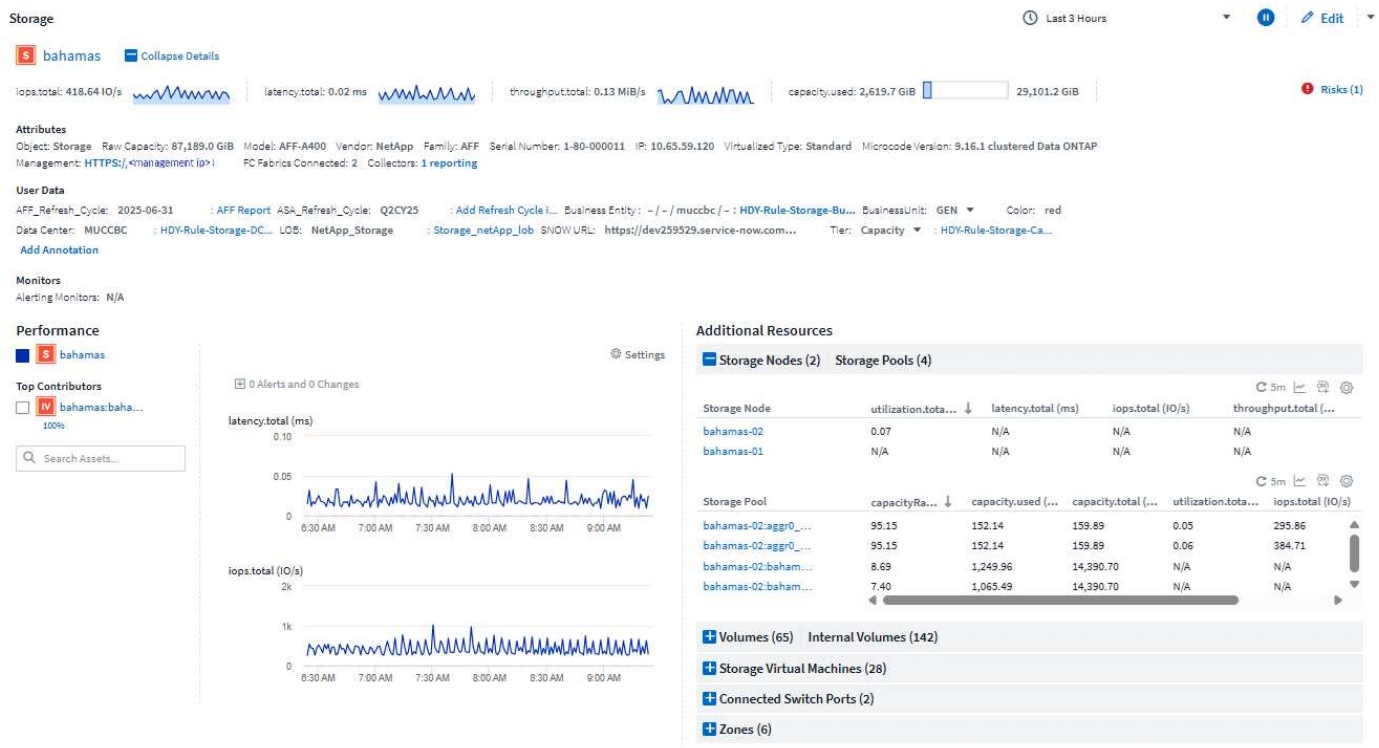
- Debian (64-Bit) 12
- Oracle Enterprise Linux (64-Bit) 9.6
- Red Hat (64-Bit) 9,6

Mai 2025

Neue Landingpages halten Sie im Flow

Die neu gestalteten Zielseiten zeigen alles, was Sie brauchen – zusammenfassende Daten, Leistungsdiagramme, Korrelationen, Warnungen und Änderungen sowie wichtige Ressourcen – in einer Ansicht.

Jetzt können Sie Fehler schneller beheben und im Fluss bleiben, ohne zwischen Registerkarten zu springen oder den Kontext zu verlieren.

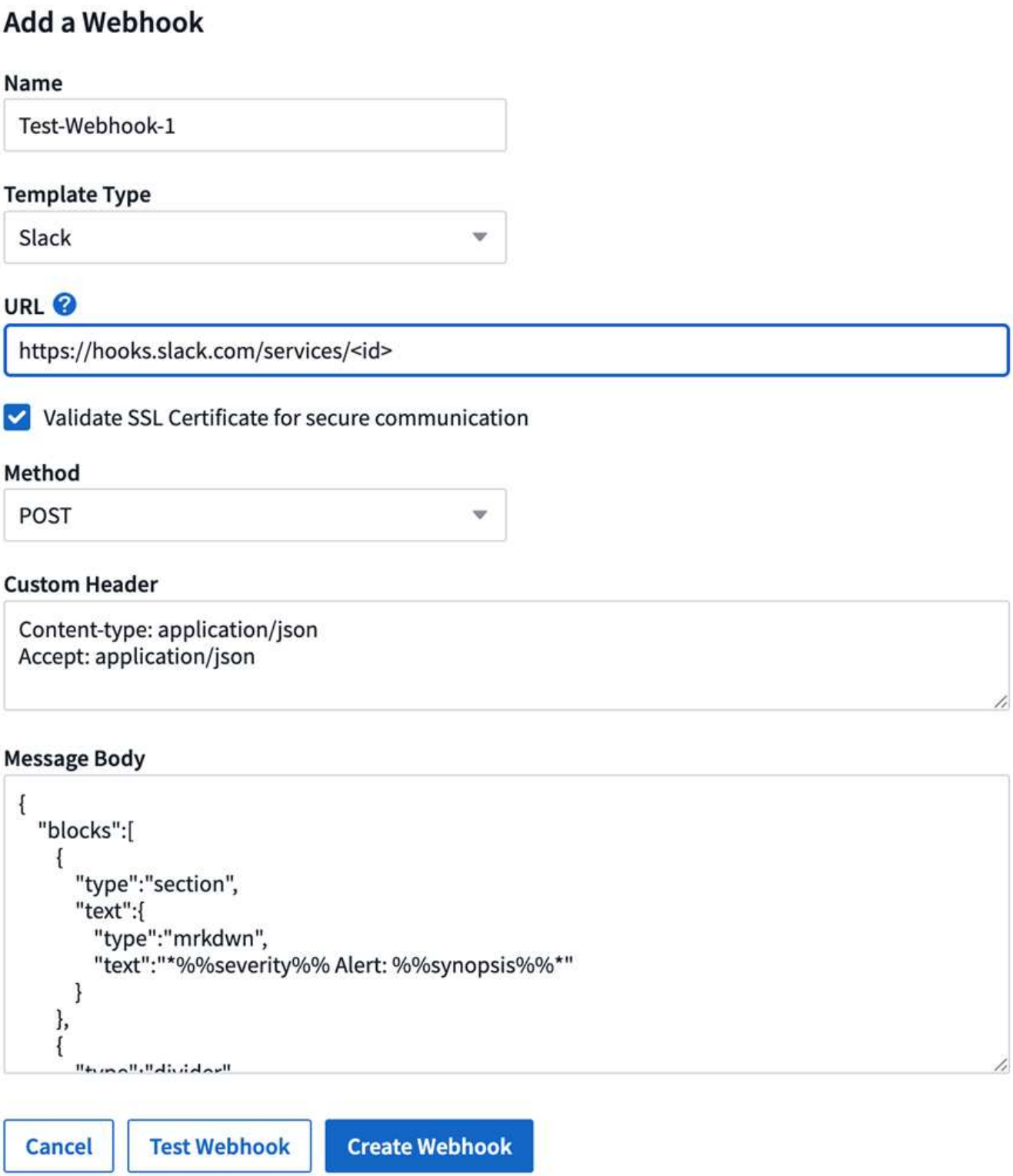


Verbesserungen der Workload-Sicherheit

Webhooks jetzt für Workload-Sicherheitswarnungen verfügbar

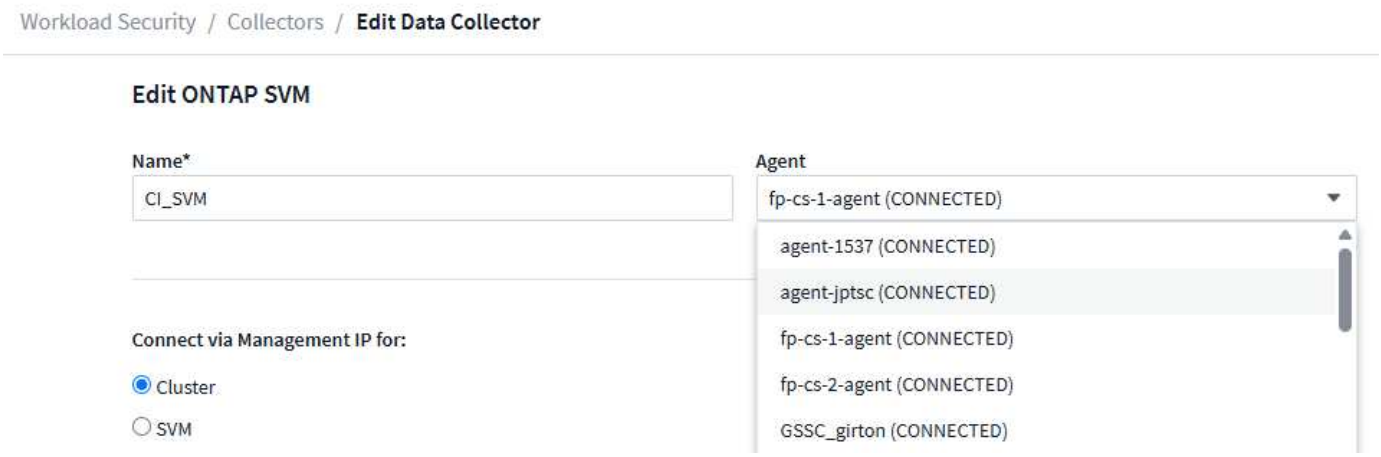
Workload Security unterstützt jetzt sofort einsatzbereite Webhook-Benachrichtigungen an Tools wie Slack, PagerDuty, Teams und mehr. Darüber hinaus bieten wir anpassbare Vorlagen, mit denen Sie die Nachricht anpassen oder in jede andere SIEM- oder Drittanbieteranwendung integrieren können. Leiten Sie kritische Warnungen direkt in Ihre vorhandenen Sicherheits-Workflows weiter, damit Ihr Team schneller

Nachforschungen anstellen und reagieren kann.



Migration von Workload Security-Sammlern zwischen Agenten

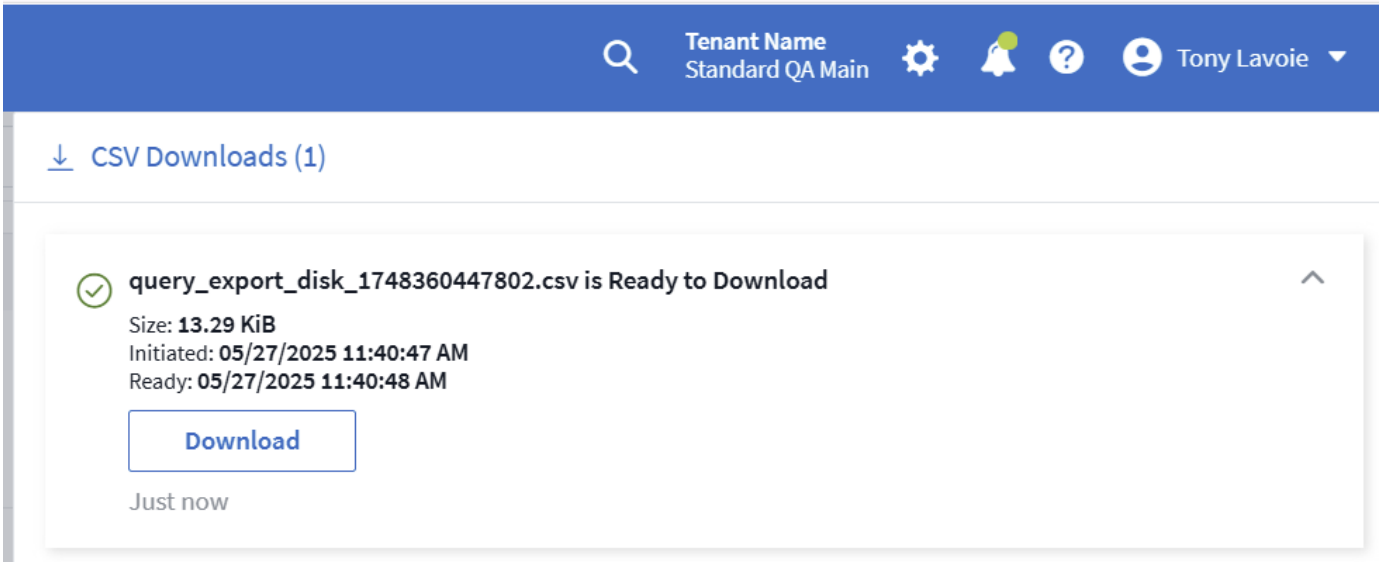
Sie können einen Workload Security-Collector problemlos von einem Agenten auf einen anderen migrieren und so einen effizienten Lastenausgleich der Collector-Instanzen zwischen den Agenten ermöglichen. Die Migration ist so einfach wie das Bearbeiten des Collectors und das Auswählen des Zielagenten aus der Liste.



Asynchroner CSV-Export

Das Exportieren von Daten in das CSV-Format kann je nach der zu exportierenden Datenmenge einige Sekunden bis mehrere Stunden dauern. Data Infrastructure Insights exportiert diese Daten jetzt asynchron, sodass Sie weiterarbeiten können, während die CSV-Datei kompiliert wird.

Zeigen Sie Ihre CSV-Exporte an, indem Sie in der oberen rechten Symbolleiste das Glockensymbol auswählen.



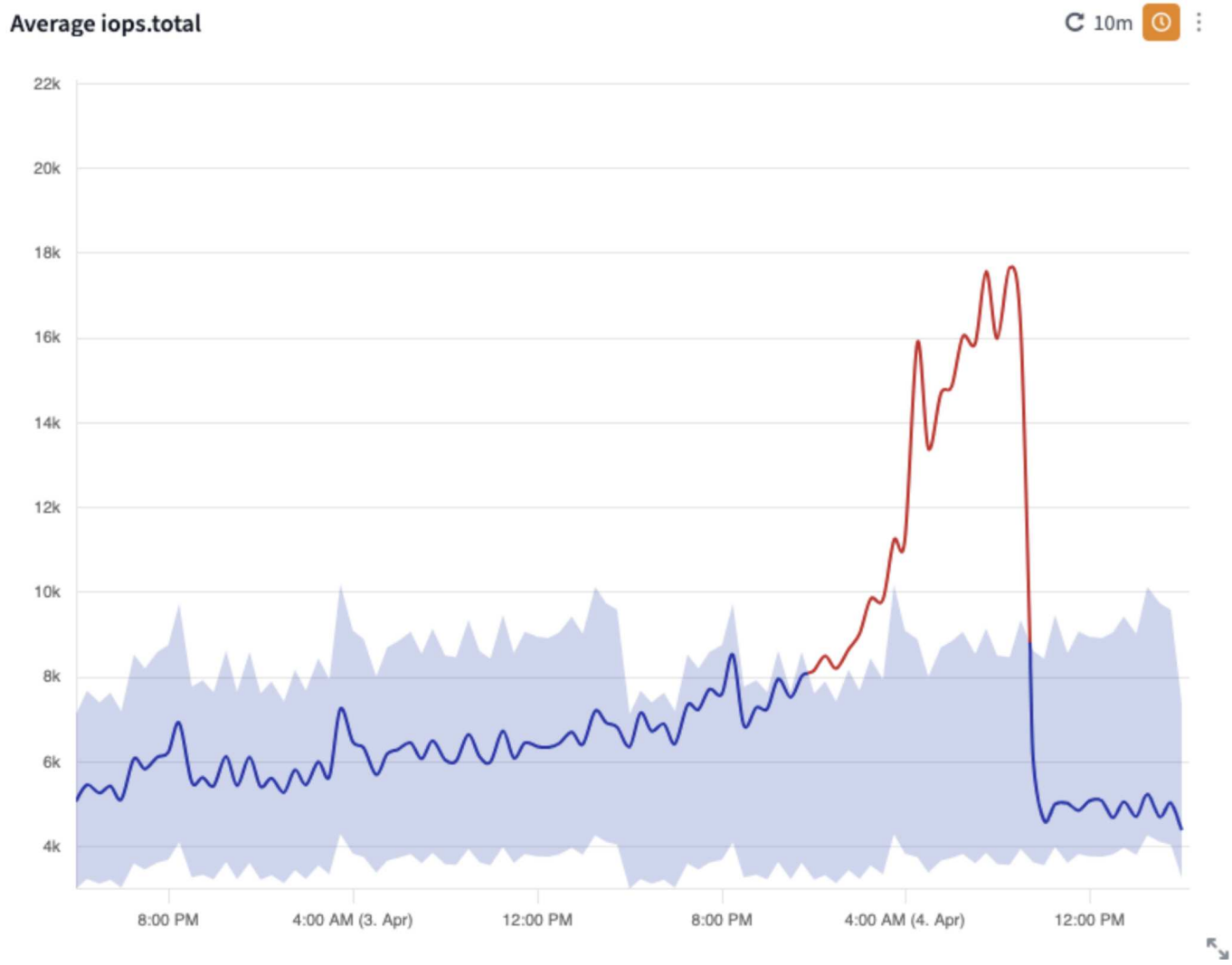
April 2025

ML-gestützte Anomaliegrenzen in Zeilen-Widgets zur proaktiven Problemlösung

Um Leistungsprobleme mit Linien- oder Spline-Diagramm-Widgets zu beheben, können Sie jetzt erwartete Verhaltensgrenzen neben tatsächlichen Messwerten anzeigen, sodass Sie zwischen normalen und abnormalen Messwerttrends unterscheiden können.

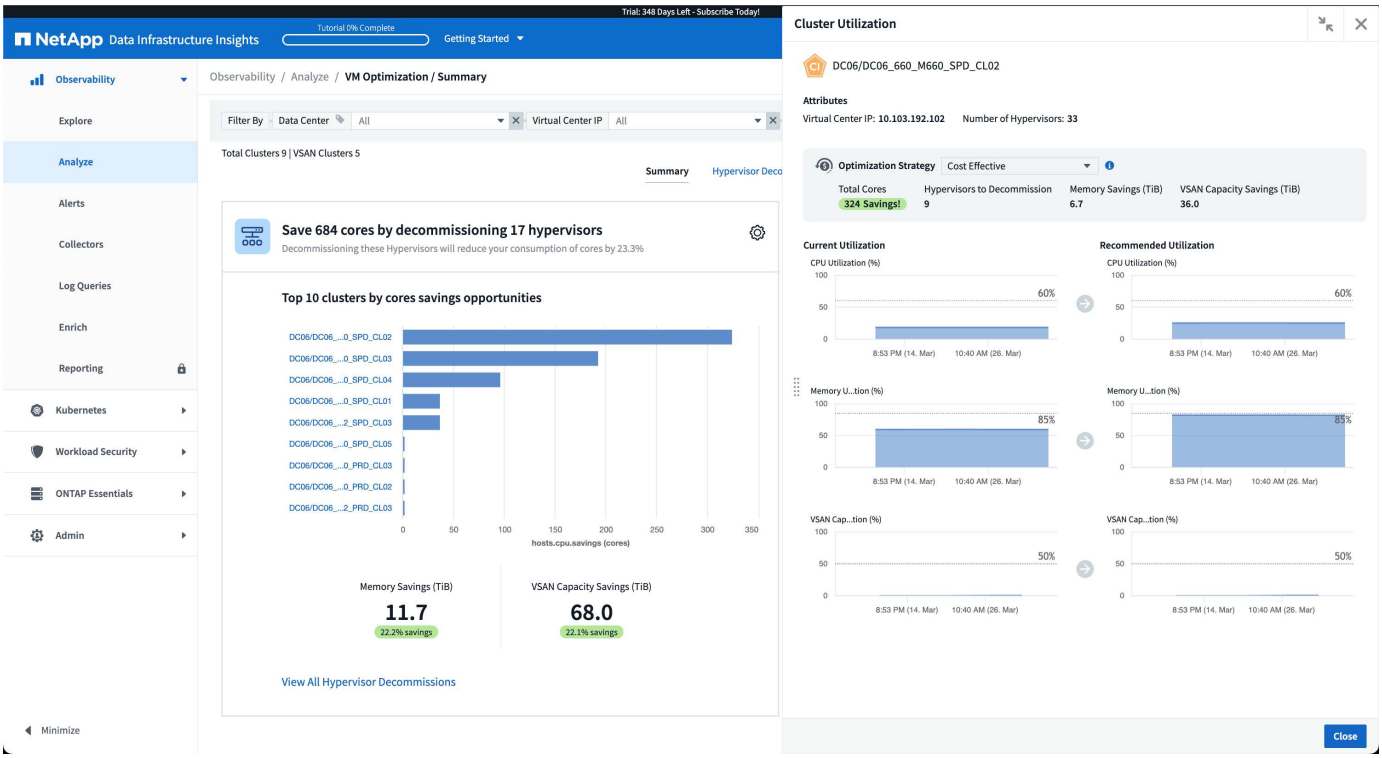
DII-Maschinelles Lernen mit saisonaler Datenanalyse legt intelligente Schwellenwerte basierend auf historischen Mustern fest. Wenn die Messwerte von den erwarteten Bereichen abweichen, hebt das System diese als Anomalien hervor. Dies ermöglicht eine schnelle Problemidentifizierung, verkürzt die

durchschnittliche Zeit bis zur Lösung und behebt Probleme, bevor sie sich auf den Betrieb auswirken.



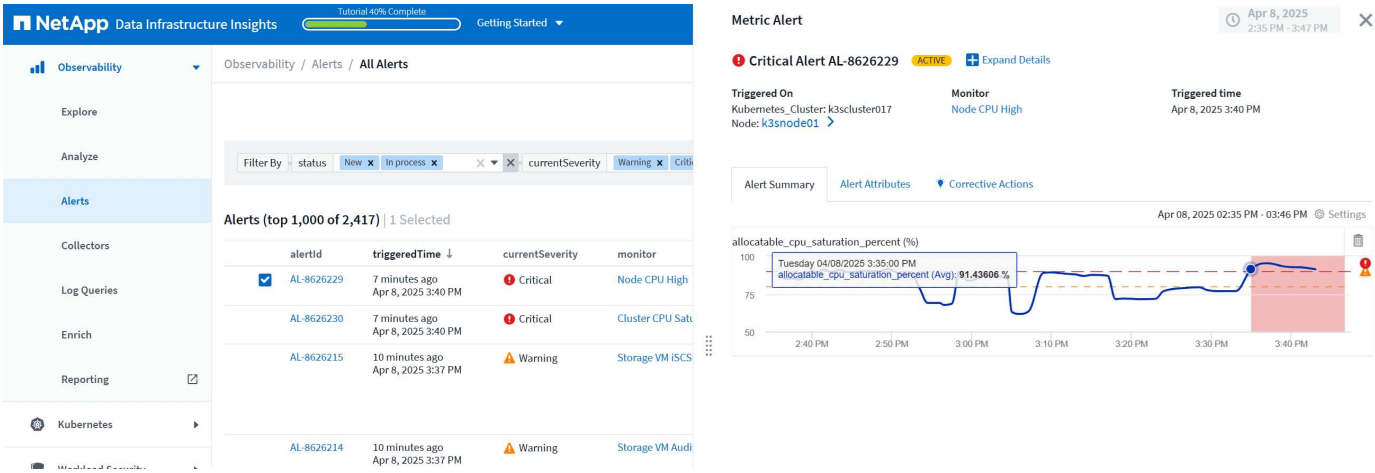
Optimieren Sie VMware-Kosten mit VSAN-Speicherunterstützung

Unsere VM-Optimierungsfunktion umfasst jetzt Unterstützung für VMWare-Umgebungen mit VSAN-Speicher. Zusätzlich zur CPU- und Speichernutzung berücksichtigt die Analyse jetzt auch den lokalen VSAN-Speicher für Rückgewinnungsempfehlungen und hilft Ihnen so, die Lizenzkosten weiter zu senken.



Alarmdetails immer zur Hand

Mit dem neuen Slideout-Panel ist die Untersuchung von Warnungen einfacher als je zuvor. Wählen Sie eine Warnung aus, um Details zu dieser Warnung anzuzeigen, und wechseln Sie einfach zwischen Warnungen, ohne beim Untersuchen von Problemen die Übersicht zu verlieren.



Asynchroner Export der Workload-Sicherheitsforensik

Das Exportieren forensischer Daten kann je nach der Menge der zu exportierenden Daten zwischen einigen Sekunden und mehreren Stunden dauern. Workload Security exportiert diese Daten asynchron, sodass Sie weiterarbeiten können, während die CSV-Datei kompiliert wird.

In Regeln gruppierte Datensammlerbenachrichtigungen

Wenn Sie Benachrichtigungen für Datensammler konfiguriert haben, werden diese Benachrichtigungen ab dem 15. April in Benachrichtigungsregeln behandelt, mit einer einzigen Regel für Sammler mit identischen

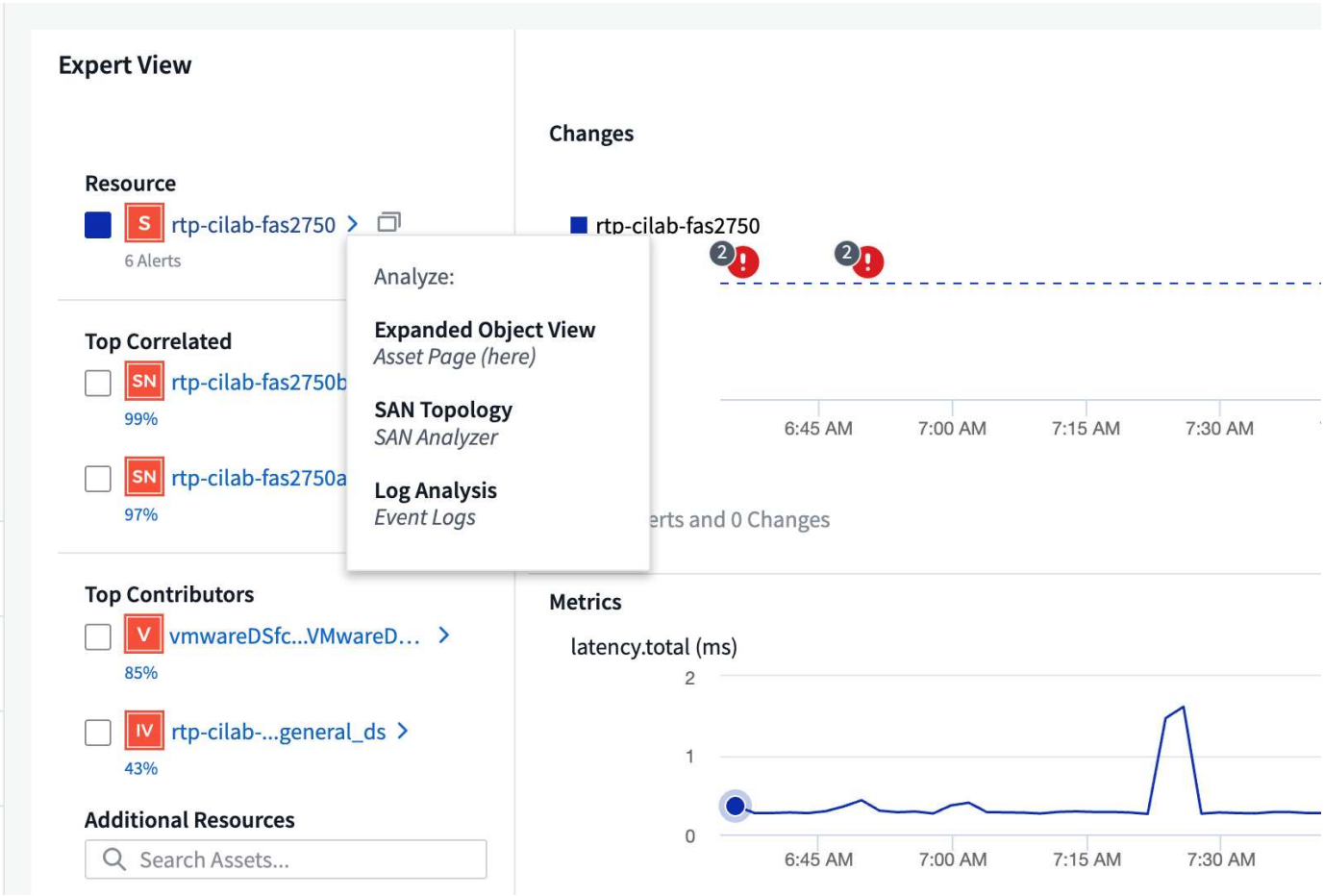
Empfängern. Für Sammler mit unterschiedlichen Empfängern gelten separate Regeln. Vorhandene Collector-Benachrichtigungen werden in Benachrichtigungsregeln migriert.

März 2025

Verbesserte Kontextnavigation für effizientes Infrastrukturmanagement

Sparen Sie Zeit, indem Sie Data Infrastructure Insights für operative Exzellenz nutzen. Wir fügen jetzt Kontextmenü-Links hinzu, mit denen Sie von jedem Objekt direkt zur Asset-Landingpage springen können, um Einblicke in die Geräteleistung zu erhalten, zum SAN Analyzer zur Visualisierung der Netzwerktopologie, zu Protokollen für Betriebsbewusstsein oder zum Change Analyzer für das Konfigurationsmanagement.

Durch den sofortigen Zugriff auf wichtige Daten über mehrere Ansichten hinweg erhalten Sie schneller ein klareres Verständnis der Objektbeziehungen. Dieser optimierte Arbeitsablauf beschleunigt die Entscheidungsfindung und Problemlösung, spart Ihnen letztendlich Zeit und verbessert Ihre gesamten Analysefunktionen.



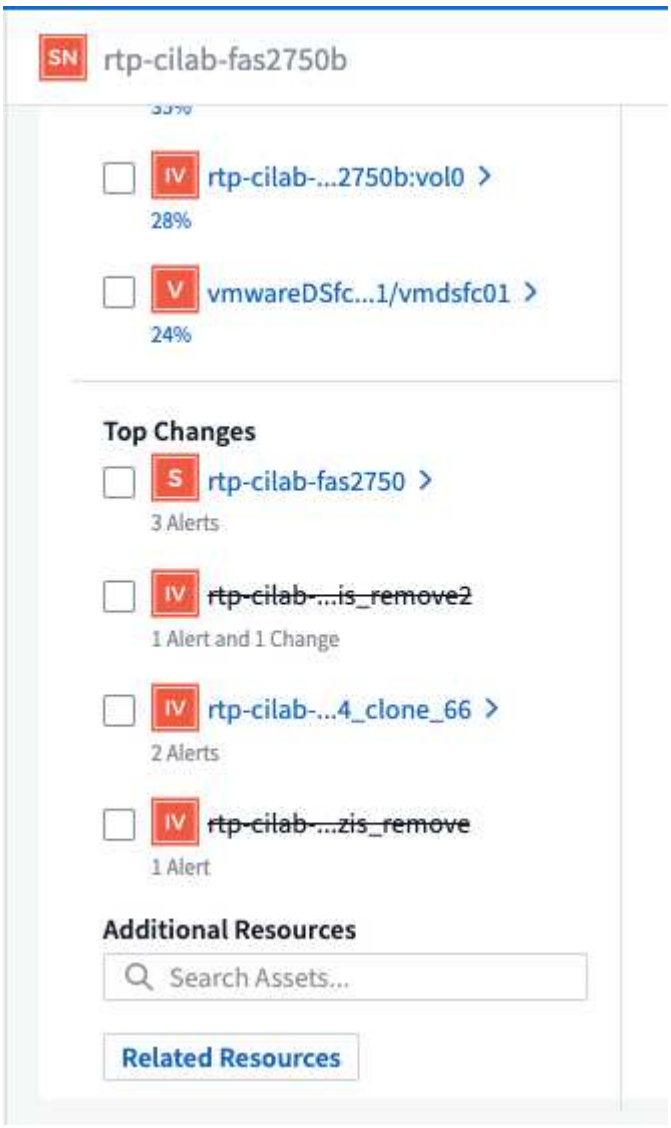
Bewahren Sie den Verlauf entfernter Assets auf

Unsere erweiterte Infra Change-Funktion bewahrt jetzt den Verlauf entfernter Assets wie Qtrees und Volumes auf, die verschoben wurden und nicht mehr verfügbar sind.

Fehlt bei Ihrem Fehlerbehebungsrätsel etwas? Nicht mehr! Sie sehen alles – einschließlich der durchgestrichenen gelöschten Objekte – und haben so auch nach dem Entfernen von Assets den

vollständigen Kontext im Blick. So wird sichergestellt, dass Sie im gesamten Pfad keine wichtigen Elemente aus früheren Änderungen oder Warnungen verpassen.

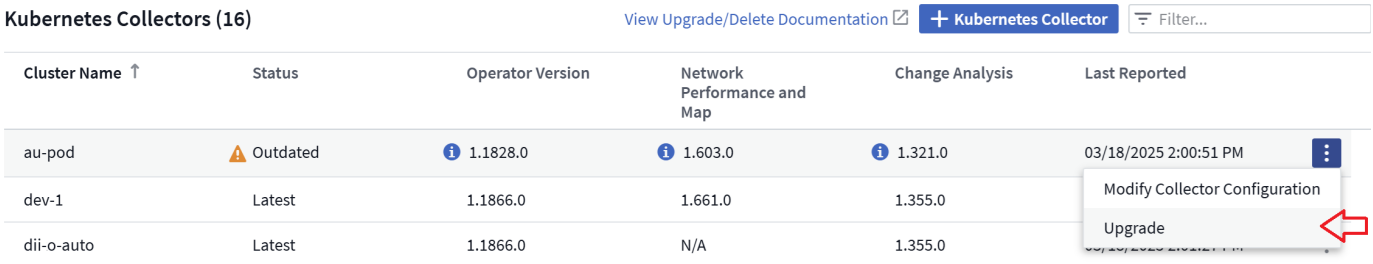
Das Ergebnis? Schnellere Lösungszeiten und sicherere Infrastrukturentscheidungen, selbst wenn die betreffenden Anlagen nicht mehr vorhanden sind.



Kubernetes Operator Push-Button-Upgrade

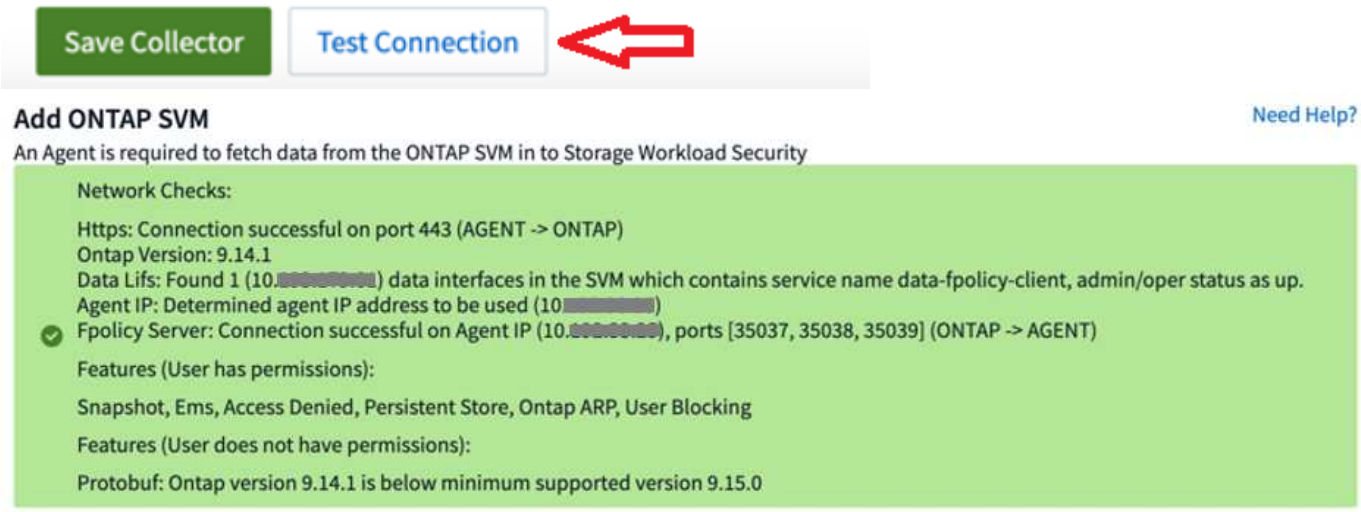
Möchten Sie sicher sein, dass Sie den neuesten Kubernetes Operator haben? Aktualisieren Sie den Operator bei Bedarf über das Clustermenü von DII Kubernetes Collectors. Wählen Sie einfach „Upgrade“ aus dem Menü aus. Der Operator überprüft die Bildsignaturen, erfasst einen Schnappschuss Ihrer aktuellen Installation und führt das Upgrade durch.

Das Push-Button-Upgrade ist eine optionale Funktion und seine Aktivierung kann pro Cluster verwaltet werden.



Testen der Konnektivität für Storage Workload Security-Datenkollektoren

Die Funktion zum Testen der Konnektivität soll Endbenutzern dabei helfen, die spezifischen Ursachen von Fehlern beim Einrichten von Datensammlern in Data Infrastructure Insights (DII) Workload Security zu identifizieren. Dadurch können die Benutzer Probleme im Zusammenhang mit der Netzwerkkommunikation oder fehlenden Rollen selbst beheben.



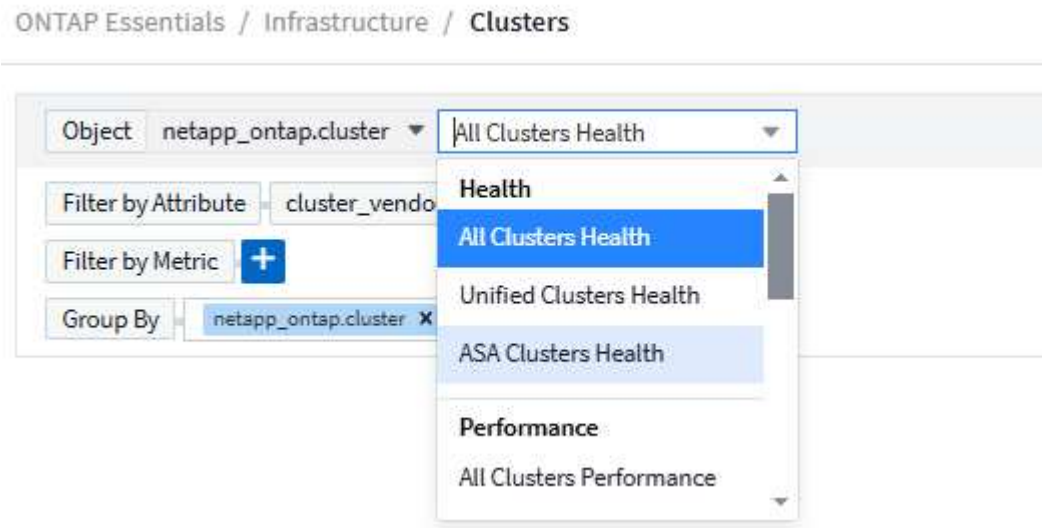
Betriebssystemunterstützung

Die folgenden Betriebssysteme werden jetzt mit Data Infrastructure Insights Acquisition Units unterstützt, zusätzlich zu denen"bereits unterstützt" :

- AlmaLinux 9.5
- Debian (64-Bit) 11
- OpenSUSE Leap 15.6
- Oracle Enterprise Linux (64-Bit) 8.9, 8.10, 9.5
- Red Hat (64-Bit) 8.9, 8.10, 9.5
- Rocky 9.5
- SUSE Linux Enterprise Server 15 SP6
- Ubuntu Server 24.04 LTS

Februar 2025

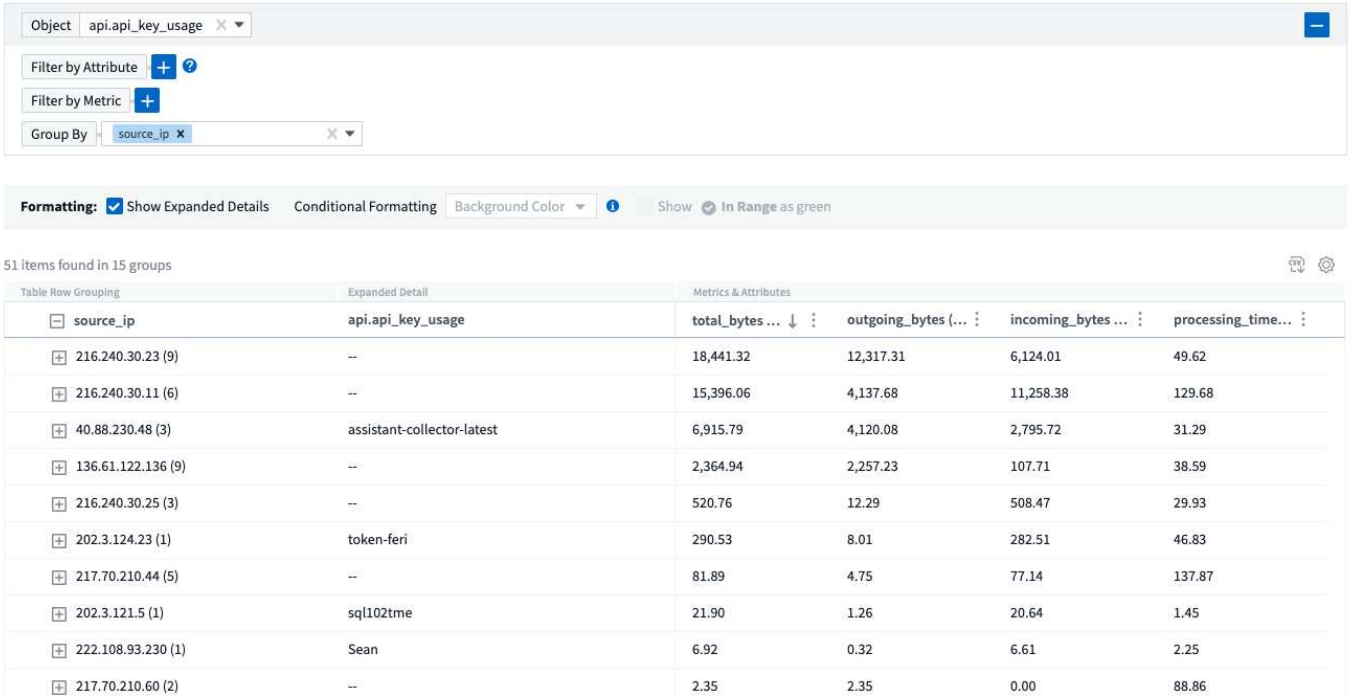
ONTAP essentials umfasst jetzt sofort einsatzbereite Verwaltbarkeit für die neueste Generation von"ASA" Geräte. Dazu gehört SAN Analyzer für VM-zu-LUN-Topologien von Workloads, die auf ONTAP ausgeführt werden, jetzt auch mit NetApp Unterstützung als Teil der Data Infrastructure Insights Basic Edition verfügbar.



DII API-Nutzungsverfolgung: Verbessern Sie Sicherheit und Effizienz

Stärken Sie Ihre Sicherheitslage und optimieren Sie die Ressourcenverwaltung mit der erweiterten REST-API-Nutzungsverfolgung, die für Administratorbenutzer verfügbar ist. Mit der API-Nutzungsverfolgung können Sie sehen, welche API-Token von welchen IP-Adressen verwendet werden und welches Datenverkehrsvolumen sie generieren. Durch die Verknüpfung von Token mit bestimmten IP-Adressen und Nutzungsstufen erhalten Sie aussagekräftige Einblicke in Systemzugriffs- und Nutzungstrends und haben so die Kontrolle, die Sie benötigen, um eine sichere, effiziente Umgebung aufrechtzuerhalten und einen reibungslosen Betrieb zu gewährleisten.

Um die API-Nutzung anzuzeigen, navigieren Sie zu **Observability > Admin > API-Zugriff** und wählen Sie *API-Nutzung anzeigen*. Beachten Sie, dass diese API nur für DII Observability-APIs verfügbar ist. Sie gilt nicht für Workload Security.



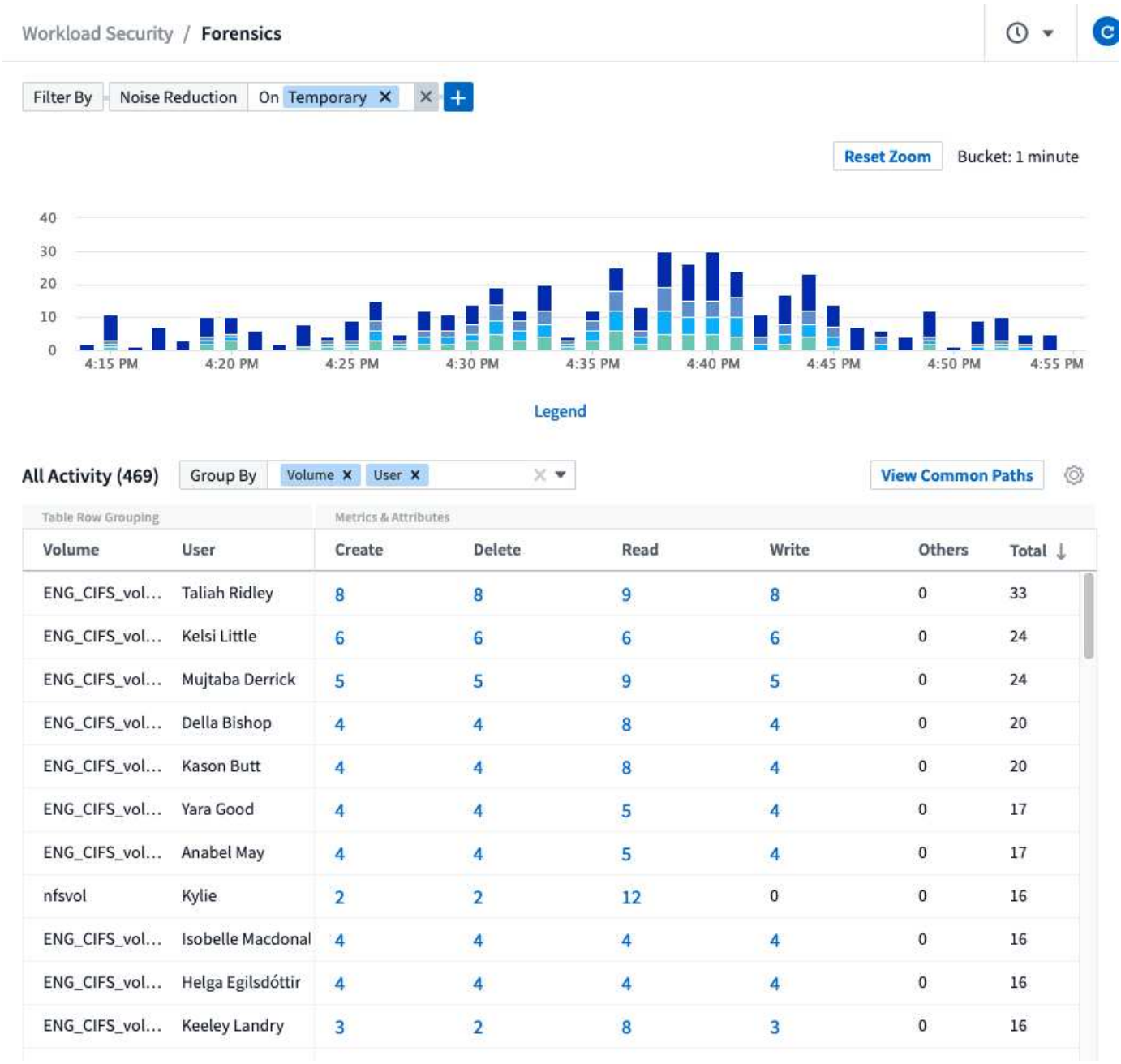
Workload Security API zum Einschränken von Benutzern

Zur Verwaltung von Benutzerbeschränkungen in Workload Security wurde eine neue API hinzugefügt. Mit der API können Sie einen Benutzer sperren oder entsperren oder die Dauer seines eingeschränkten Zugriffs ändern. Weitere Informationen zur API *cloudsecure_actions.block* finden Sie auf der Seite „Admin > API-Zugriff > API-Dokumentation“.

Januar 2025

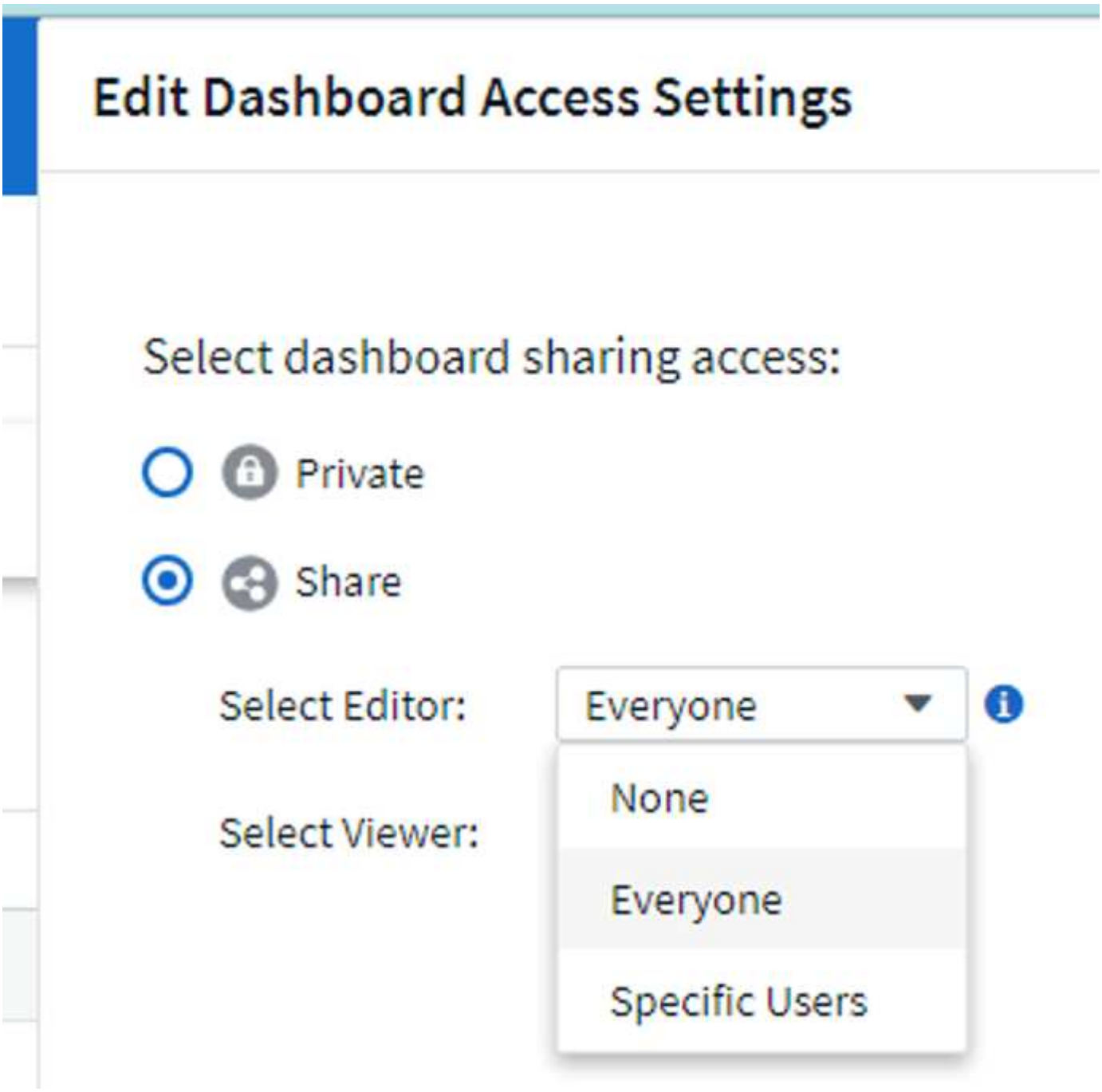
Proaktives Risikomanagement mit Forensics Grouping

Wir stellen unsere neueste Funktion vor, die Ihre Sicherheits- und Ressourcenverwaltungsfunktionen verbessern soll! Mit der erweiterten Gruppierungsfunktion und der Unterstützung für hierarchisches Mehrfachgruppieren können Sie jetzt problemlos Benutzer identifizieren, die auf bestimmte Ordner zugegriffen haben, die aktivsten Benutzer und Freigaben ermitteln und Risiken proaktiv verwalten, indem Sie aktive Client-IP-Adressen verfolgen. Optimieren Sie Ihre Speicher- und Bandbreitennutzung, indem Sie die am häufigsten aufgerufenen Dateien und Ordner ermitteln und durch die Identifizierung von Benutzern eine bessere Kontrolle über den Systemzugriff erlangen.



Dashboard-Zugriffskontrolle

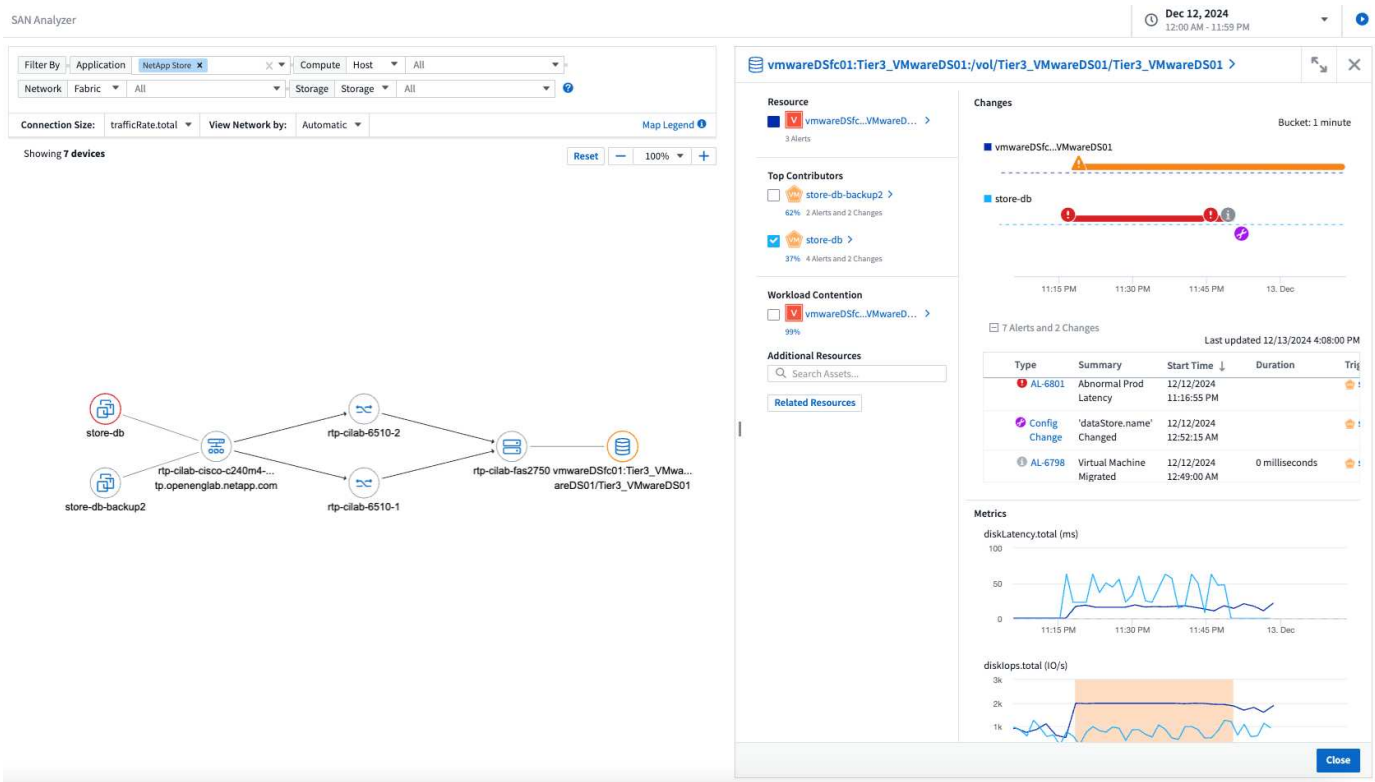
Data Infrastructure Insights gibt Ihnen jetzt mehr Kontrolle über den Zugriff auf die von Ihnen erstellten Dashboards. Sie entscheiden, wer Ihre Diagramme ändern kann. Sie kontrollieren die Offenlegung potenziell sensibler Informationen. Arbeiten Sie noch an einem Dashboard, das noch nicht für die allgemeine Sichtbarkeit bereit ist? Sie können es privat halten, bis Sie bereit sind, es freizugeben.



Dezember 2024

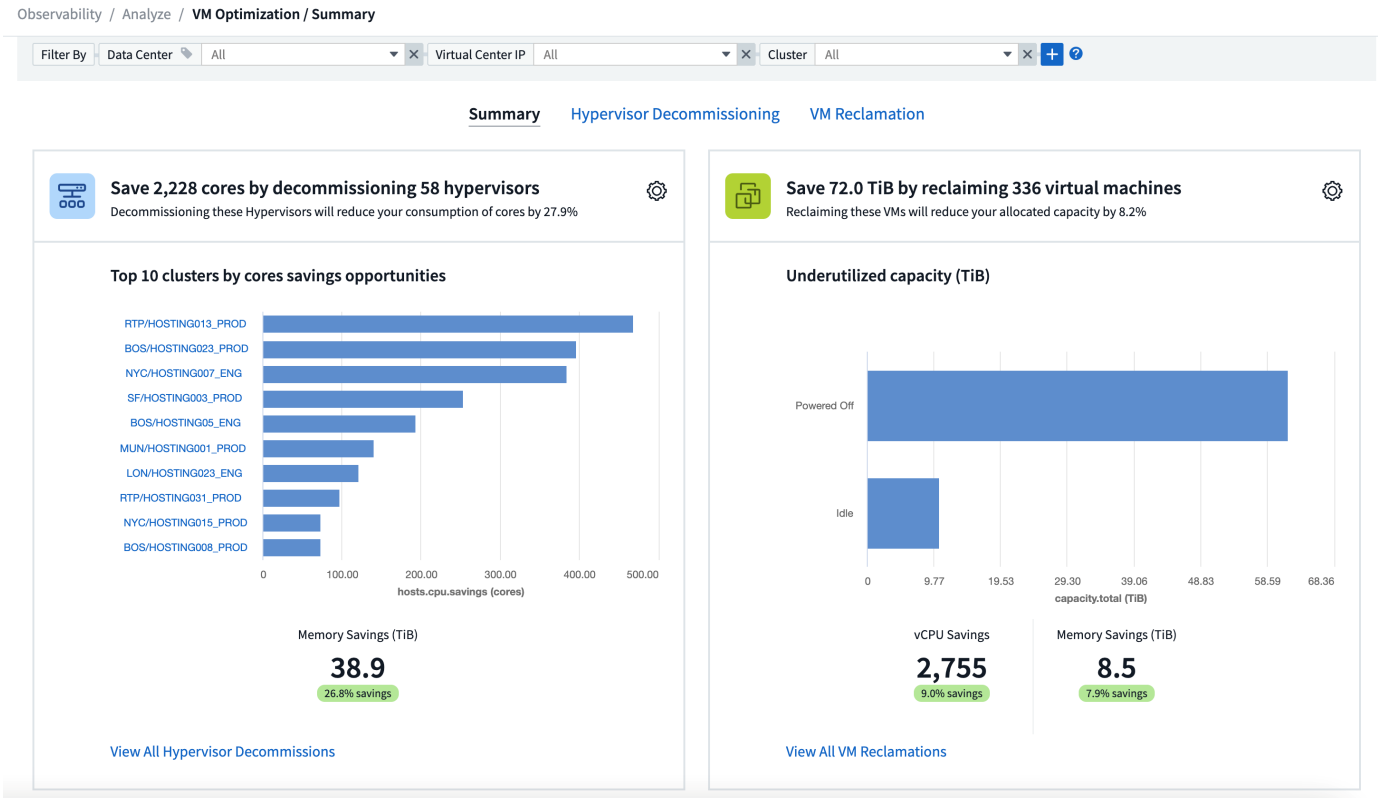
Einführung von SAN Analyzer: Verbesserte Sichtbarkeit für Block-Workloads

SAN spielt eine entscheidende Rolle bei der Bewältigung wichtiger Arbeitslasten, seine Komplexität kann jedoch zu erheblichen Ausfällen und Störungen für die Kunden führen. Mit dem **SAN Analyzer** von DII wird die SAN-Verwaltung einfacher und effizienter. Dieses leistungsstarke Tool bietet End-to-End-Sichtbarkeit und bildet Abhängigkeiten von VM/Host über Netzwerk bis hin zu LUN und Speicher ab. Durch die Bereitstellung einer interaktiven Topologiekarte ermöglicht Ihnen SAN Analyzer, Probleme zu lokalisieren, Änderungen zu verstehen und das Verständnis des Datenflusses zu verbessern. Optimieren Sie die SAN-Verwaltung in komplexen IT-Umgebungen mit SAN Analyzer und erhöhen Sie Ihre Transparenz bei Block-Workloads.



Optimieren Sie VM-Kosten mit intelligenter Host-Stilllegung und VM-Rückgewinnung

Data Infrastructure Insights unterstützt Sie bei der Verwaltung der Infrastruktur- und Lizenzkosten, indem es das historische Verhalten der Umgebung analysiert und kurz- und langfristige Prognosen erstellt und detaillierte Empfehlungen für die Außerbetriebnahme von Hosts und die Wiederherstellung ausgeschalteter und inaktiver VMs generiert. Diese Empfehlungen helfen Ihnen, die Leistungsstabilität sicherzustellen, ungenutzte Kapazitäten freizugeben und die Speicher- und CPU-Zuweisung zu reduzieren.



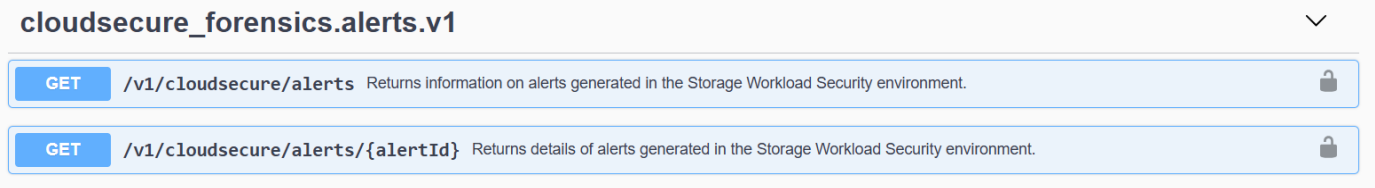
Entdecken Sie Log-Einblicke mit Zeitdiagrammen und Tabellen-Widget-Unterstützung

Jetzt können Sie Zeitdiagramme (Balken, Linien, Flächen) nutzen, um Trends und Muster in Protokolldaten zu erkennen, z. B. wiederkehrende Fehler oder Aktivitätsspitzen, und so wertvolle Einblicke in das Systemverhalten im Zeitverlauf gewinnen. Darüber hinaus können Sie jetzt mithilfe von Tabellen Protokollmeldungen direkt in das Dashboard einbinden und so eine umfassendere Ansicht der Protokolldetails erhalten.

November 2024

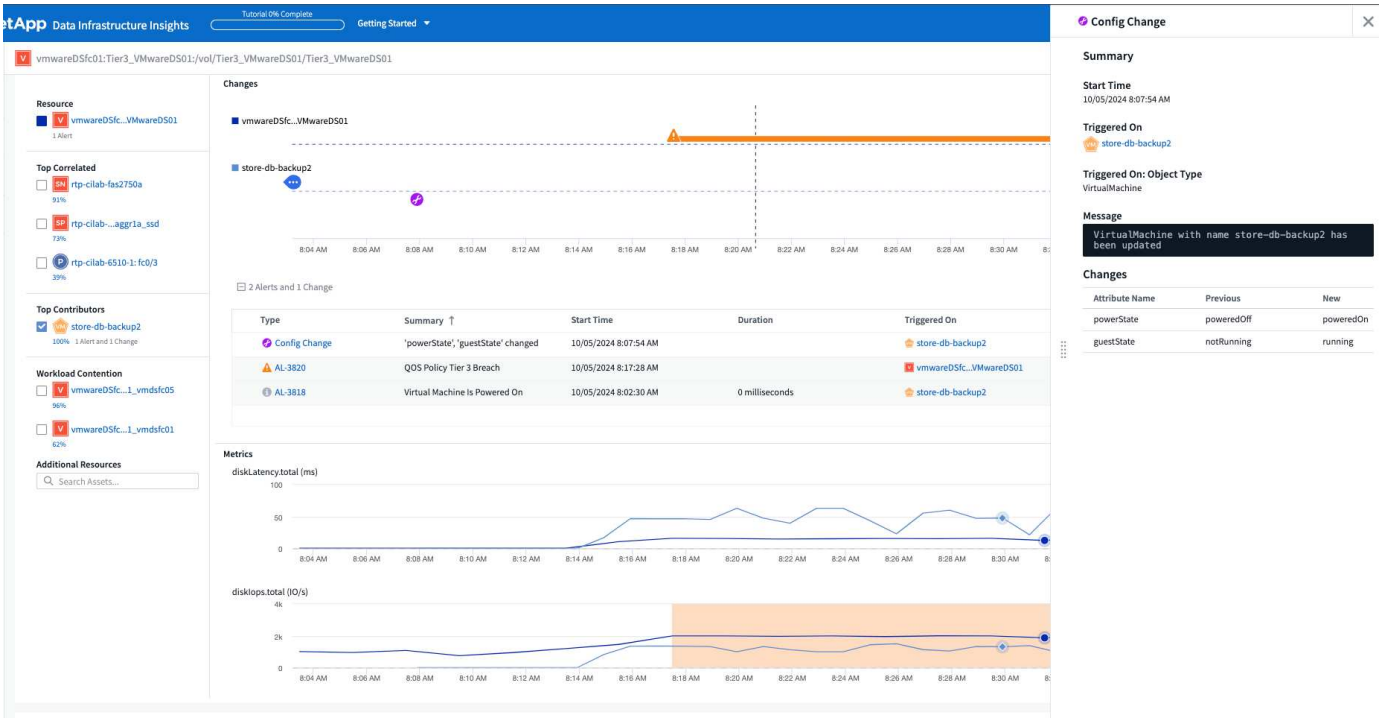
Neue API für Workload-Sicherheitswarnungen

Forensische Warnmeldungen mit der neuen Workload Security abrufen**"cloudsecure_forensics.alerts** API" .



Analysieren Sie Konfigurationsänderungen in Ihrer Umgebung

Konfigurationsänderungen sind eine der häufigsten Ursachen für Probleme in der modernen IT. Data Infrastructure Insights(DII) neu"Änderungsanalyse" Mithilfe dieser Funktion können Sie Änderungen, die in Ihrer Umgebung Probleme verursachen, klar erkennen. Beschleunigen Sie die Fehlerbehebung, indem Sie alle Änderungen an Geräten und zugehörigen Infrastrukturkomponenten anzeigen, die möglicherweise zu einem Problem geführt haben. Wenn Sie oder Ihr Team geplante Änderungen durchführen, können Sie diese außerdem schnell validieren und sicherstellen, dass es keine unerwarteten Auswirkungen gibt, bevor die Service-Level beeinträchtigt werden.



KubeVirt-Support: Überwachen Sie die Workloads virtueller Maschinen, die in Ihrem Kubernetes-Cluster ausgeführt werden

DII unterstützt jetzt vollständig KubeVirt, die Kubernetes-native Virtualisierungslösung, die von Plattformen wie OpenShift Virtualization und Harvester verwendet wird. Erhalten Sie vollständige Transparenz über die Metriken, Ereignisse, Konfigurationsänderungen und den Netzwerkverkehr sowohl der virtuellen Maschinen als auch der Container-Workloads innerhalb Ihrer Kubernetes-Cluster.

Oktober 2024

Gewinnen Sie neue Erkenntnisse mit benutzerdefinierten Ausdrücken in Monitoren

Mithilfe von Ausdrücken können Sie arithmetische Operationen in Metrik- und Anomalieerkennungsmonitoren durchführen. Hier sind einige Beispiele:

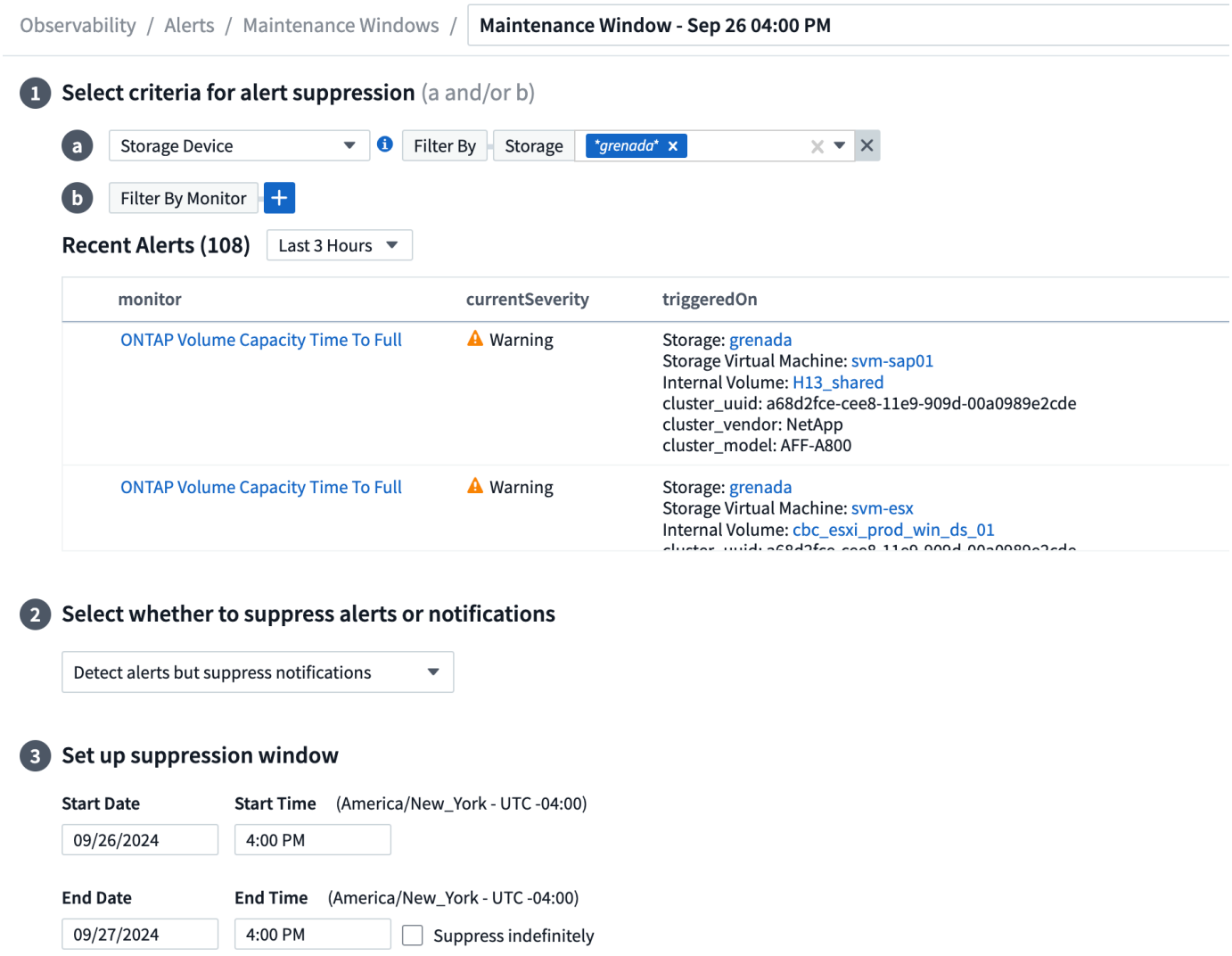
- Verhältnis: IOPS/TB, um zu erkennen, wo bei Cloud-Speicheranbietern Service-Level-Grenzen erreicht werden.
- Prozentsatz: Verwendet/Verfügbar zur Berechnung der Auslastung
- Aggregation: Kombinieren Sie mehrere Arten von physischen Portfehlern in einem Monitor
- Vergleich: Vergleichen Sie die aktuelle Auslastung der Ressourcenreserve mit dem optimalen Reservepunkt, um Ressourcen zu identifizieren, die nicht mit voller Kapazität laufen.

Minimieren Sie Alarmunterbrechungen während der Wartungszeit

Mithilfe von Wartungsfenstern können Sie Warnmeldungen während geplanter Wartungszeiträume unterdrücken und so unnötige Unterbrechungen vermeiden.

Mit Wartungsfenstern können Sie für die von Ihnen ausgewählten Objekte und Metriken bestimmte Wartungszeiträume planen, in denen Warnbenachrichtigungen unterdrückt werden. Sie können beispielsweise Warnmeldungen unterdrücken, die von bestimmten Speichersystemen ausgelöst werden, wenn sich diese Speichersysteme in einer geplanten Upgrade-Phase befinden.

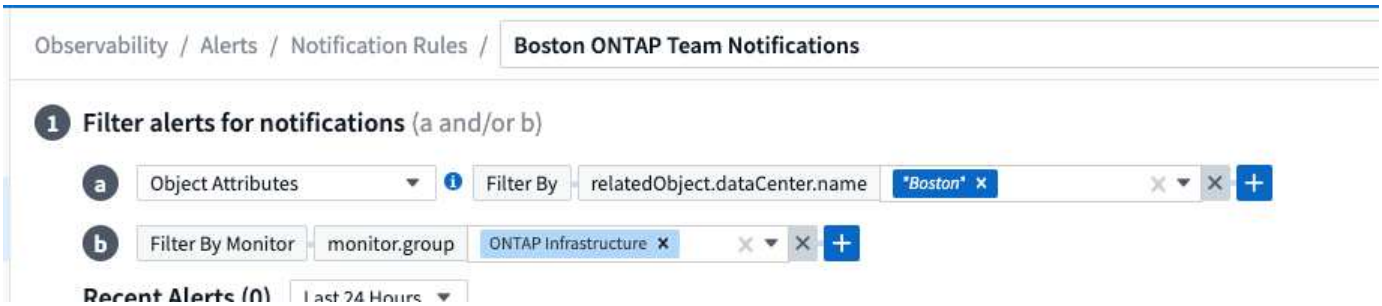
Beachten Sie, dass nur Warnmeldungen unterdrückt werden (E-Mail, Webhook). Die Warnmeldungen selbst werden weiterhin auf der Seite „Beobachtbarkeit > Warnmeldungen > Alle Warnmeldungen“ angezeigt.



Optimieren Sie das Alarmmanagement mit neuen Alarmbenachrichtigungsregeln

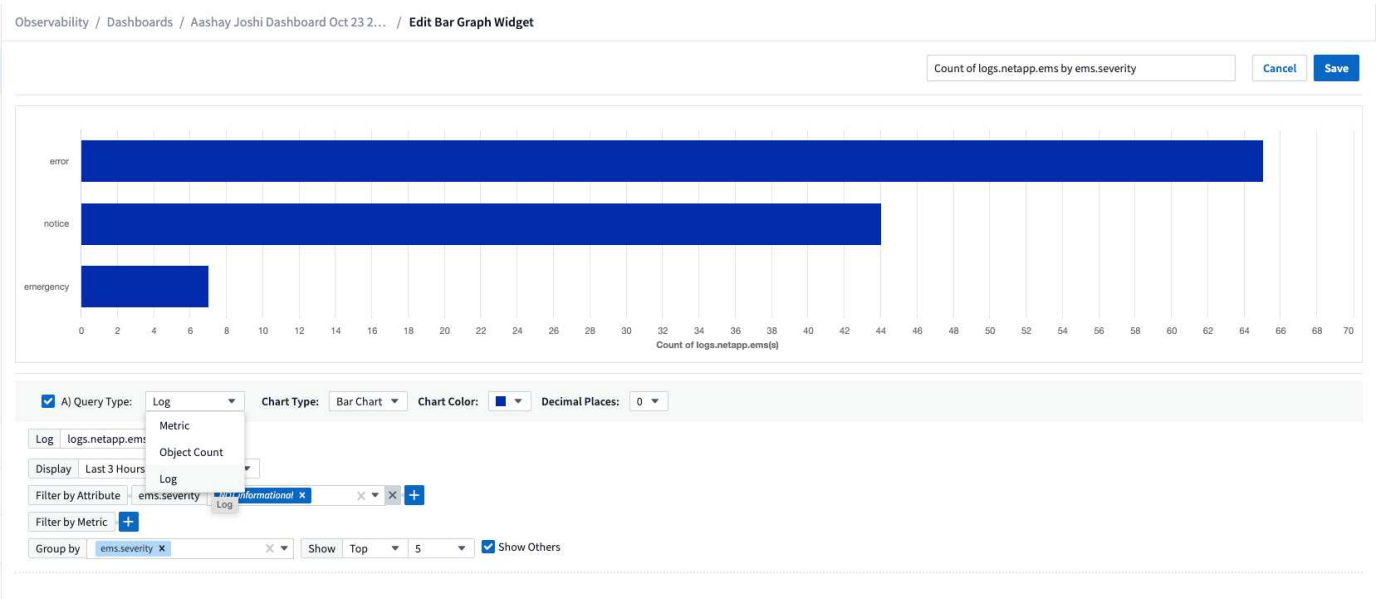
Regeln für Warnbenachrichtigungen vereinfachen die Benachrichtigungsverwaltung über Monitore und Teams hinweg.

Kontrollieren Sie die Warnübermittlung über die Kanäle Ihres Unternehmens und stellen Sie sicher, dass die richtigen Informationen das richtige Team erreichen. Sie müssen keine separaten Monitore für verschiedene Teams verwalten. Leiten Sie Warnungen basierend auf verwandten Objektattributen (Speichername, Rechenzentrum, Anwendungsname) oder Monitorattributen (Gruppe, Schweregrad) weiter.



Log Analytics in Dashboards

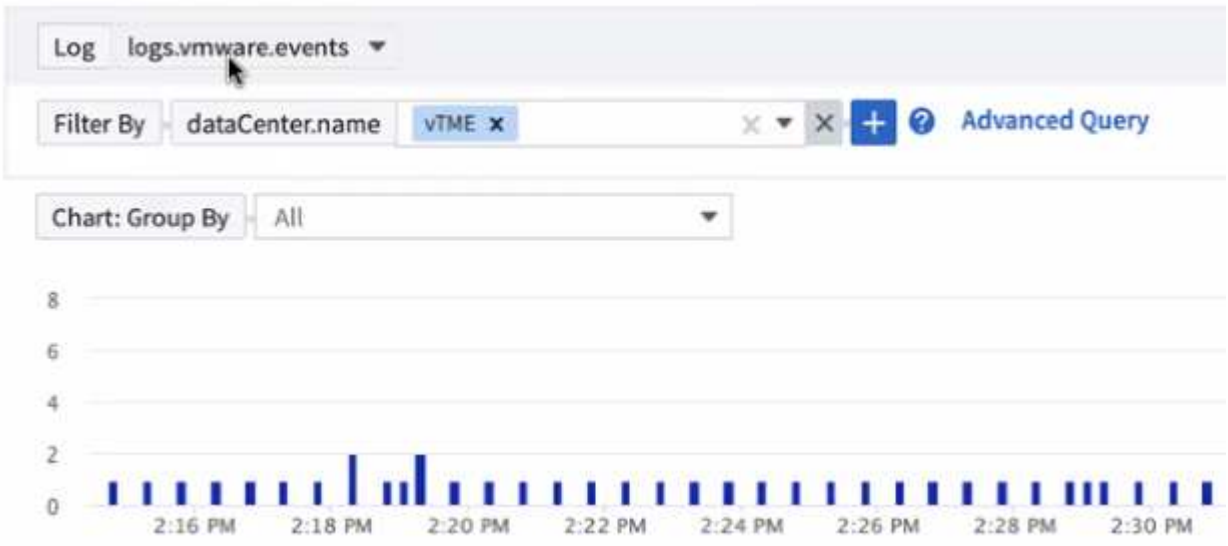
Sie können jetzt Protokollereignisse in Ihre Dashboards aufnehmen, um Ereignisdaten zu visualisieren und ein umfassenderes und kontextbezogeneres Verständnis Ihrer Umgebung zu erhalten. Untersuchen Sie Protokolle und zeigen Sie zugehörige Metriken an, ohne das Dashboard zu verlassen!



Bessere VMware-Beobachtbarkeit mit VMware Events

Verwalten und beheben Sie Probleme in Ihrer VMware-Umgebung proaktiv mit Echtzeitereignissen. VMware-Ereignisse bieten Einblicke in VM-Migrationen, Ressourcenzuweisungen und Host-Integrität. Jetzt zur Verwendung in Abfragen, Dashboards und Monitoren verfügbar. Erfordert VMware Version 8 oder höher. Wählen Sie einfach die Quelle *logs.vmware.events* aus.

VMware-Ereignisse werden auch für die oben erwähnte neue Konfigurationsänderungsanalyse von DII verwendet.



Aktualisierungen des Datensammlers:

- **Pure FlashBlade**: Dieser Collector sammelt Inventar- und Leistungsdaten von FlashBlade-Clustern, die Version 2 ihrer REST-API bereitstellen.

September 2024

Einführung von Data Infrastructure Insights, ehemals Cloud Insights

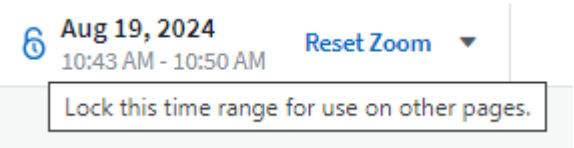
Am Dienstag, den 24. September 2024, hat NetApp den Namen von Cloud Insights offiziell in * Data Infrastructure Insights* (DII) geändert. Dies wurde während der Insight-Benutzerkonferenz von Haiyan Song in ihrer Keynote-Präsentation auf der Hauptbühne und in einer Produkt-Pressemitteilung der Insight-Konferenz angekündigt.

Der DII-Dienst bleibt derselbe; es gibt keine Funktionsänderungen oder Modifikationen. Dies ist eine Namensänderung, um den Dienstnamen besser an seine Fähigkeiten für die gesamte IT-Infrastruktur anzupassen.

August 2024

Anzeigen spezifischer Daten für Ihren Zeitraum

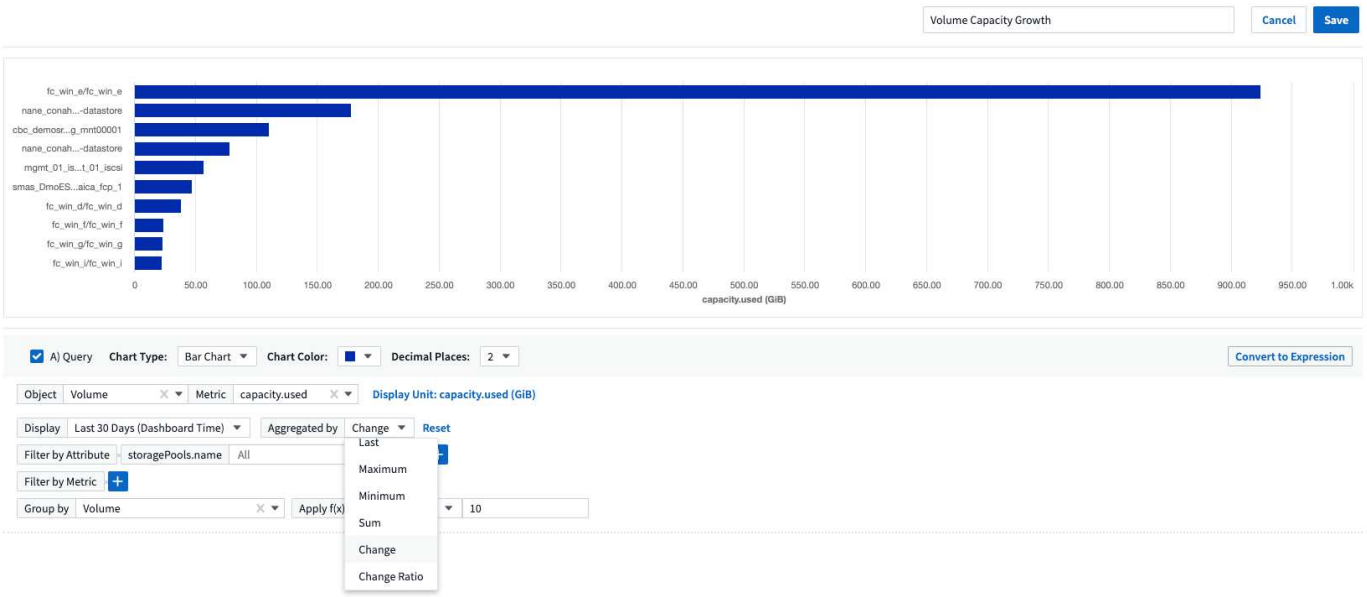
Untersuchen Sie eine Warnung? In ein Diagramm hineingezoomt? Diese Aktionen ändern den Zeitbereich für diese Seiten. Jetzt können Sie diesen Zeitraum sperren, zu anderen Cloud Insights -Seiten navigieren und Daten anzeigen, die für diesen gesperrten Zeitraum spezifisch sind. Die Untersuchung und Fehlerbehebung ist jetzt viel einfacher!



Analyse von Veränderungen und Veränderungsverhältnissen (%)

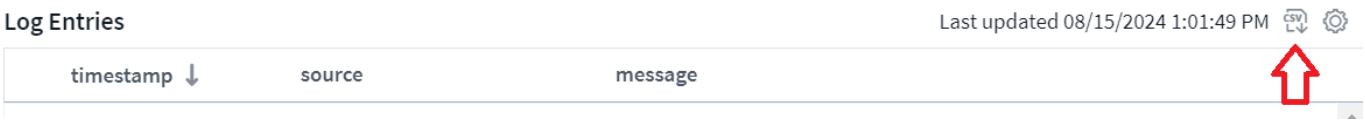
Mithilfe von Änderungsverhältnis-Zeitaggregationen können Sie signifikante Änderungen und Trends in Metrikwerten im Zeitverlauf erkennen. Diese Erkenntnisse sind der Schlüssel zum Verständnis der Änderungen, beispielsweise eines erheblichen Kapazitätswachstums für einen bestimmten Zeitraum oder einer Änderung der Leistung einzelner Ports.

- **Änderung** – Beobachten Sie die Änderung einer Metrik zwischen zwei Punkten innerhalb eines ausgewählten Zeitraums.
- **Änderungsverhältnis** – beobachten Sie die proportionale Änderung einer Metrik zwischen zwei Punkten im Vergleich zum Anfangspunkt innerhalb eines ausgewählten Zeitraums.



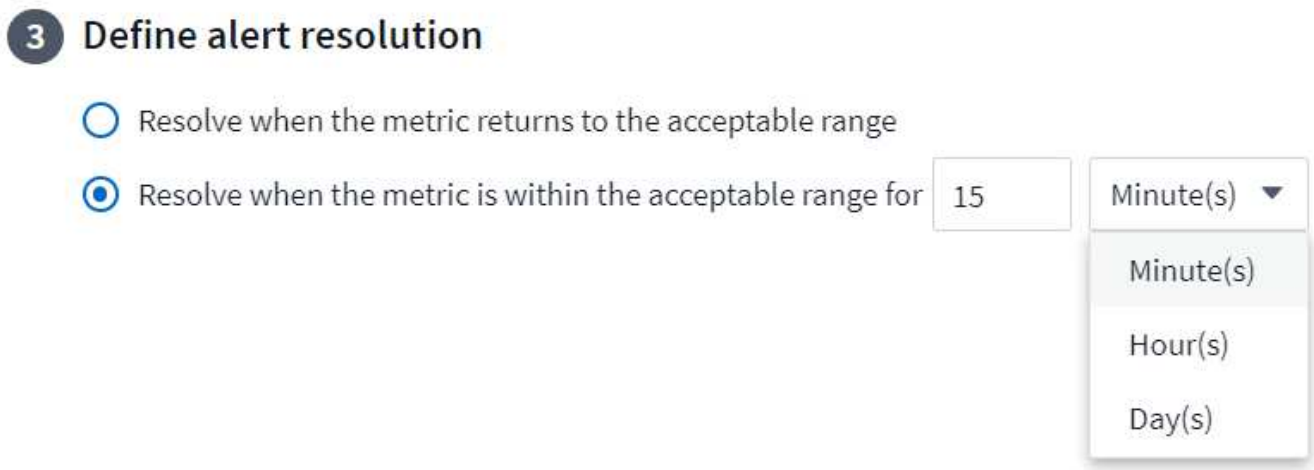
Exportieren Sie die Ergebnisse der Protokollabfrage in eine CSV-Datei

Beim Anzeigen der Ergebnisse der Protokollabfrage können Sie durch Klicken auf die neue Schaltfläche „Exportieren“ ganz einfach bis zu 10.000 Zeilen in das CSV-Format exportieren. Dies verbessert die Datenzugänglichkeit, vereinfacht die Datenanalyse und -berichterstattung und ermöglicht eine nahtlose Integration mit anderen Datenverarbeitungstools.



Beheben Sie Warnungen nach Zeit

Cloud Insights bietet Ihnen jetzt die Möglichkeit, eine Warnung aufzulösen, wenn die überwachte Metrik für eine bestimmte Dauer innerhalb des akzeptablen Bereichs bleibt. Dadurch können Sie sich auf echte Probleme konzentrieren und den Lärm reduzieren, der durch wiederholtes Überschreiten definierter Schwellenwerte bei Metriken entsteht, indem Sie mehrere Warnungen zu einer einzigen zusammenfassen.



Juli 2024

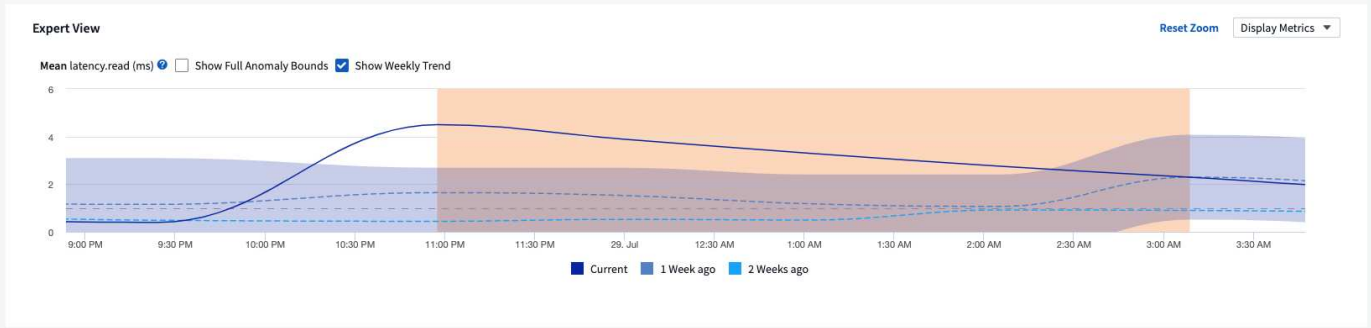
AIOps: Anomalieerkennung

Cloud Insights nutzt maschinelles Lernen, um unerwartete Änderungen in den Datenmustern Ihrer Umgebung zu erkennen und proaktive Warnungen bereitzustellen, die Ihnen helfen, Probleme frühzeitig zu erkennen.

Ein Rechenzentrum verhält sich zu verschiedenen Tageszeiten und an verschiedenen Wochentagen unterschiedlich. Cloud Insights verwendet wöchentliche Saisonalität, um das historische Verhalten für jeden Tag und jede Uhrzeit zu vergleichen.

Die Überwachung der Anomalieerkennung kann Warnmeldungen für Situationen ausgeben, in denen beispielsweise die Definition von „normal“ unklar ist, sich das Verhalten im Laufe der Zeit ändert oder mit großen Datenmengen gearbeitet wird, bei denen die manuelle Definition von Schwellenwerten nicht praktikabel ist.

Neu"Anomalieerkennungsmonitore" Warnmeldung, wenn derartige Anomalien bei den von Ihnen ausgewählten Objektmetriken auftreten.



Verbesserungen der Workload-Sicherheit

NFS 4.1-Unterstützung

Der SVM Data Collector unterstützt jetzt NFS-Versionen bis einschließlich **NFS 4.1** mit ONTAP 9.15.1 oder höher.

Neue API für forensische Aktivitäten

Die forensische Aktivität"API" hat eine neue Version. Verwenden Sie beim Aufrufen der API für Forensics Activity die API **cloudsecure_forensics.activities.*v2***.

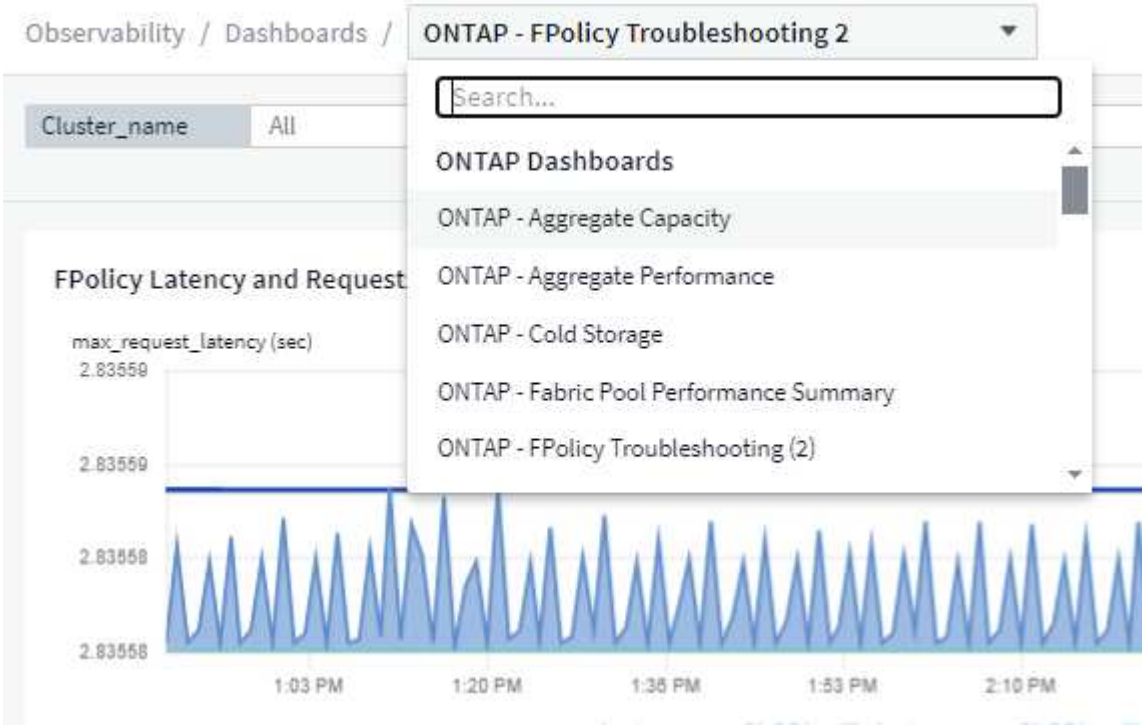
Beachten Sie, dass Sie bei mehreren Aufrufen dieser API für optimale Ergebnisse sicherstellen müssen, dass die Aufrufe nacheinander und nicht parallel erfolgen. Mehrere parallele Aufrufe können zu einem Timeout der API führen.

Einfachere Dashboard-Navigation

Bei dieser Funktion geht es darum, Ihre Betriebsabläufe zu optimieren und die Zusammenarbeit zwischen Teams zu erleichtern.

Durch die Gruppierung Ihrer Dashboards erhalten Sie schneller die benötigte Übersicht. Mit dem neuen Navigationsmenü können Sie jetzt zwischen verschiedenen Dashboards wechseln, ohne den Überblick zu verlieren. So können Sie Ihre Infrastruktur ganz einfach erkunden und verwalten. Richten Sie Dashboard-

Gruppen an Ihren operativen Runbooks aus, um Ihre Erfahrung weiter zu verbessern.



Juni 2024

Betriebssystemunterstützung

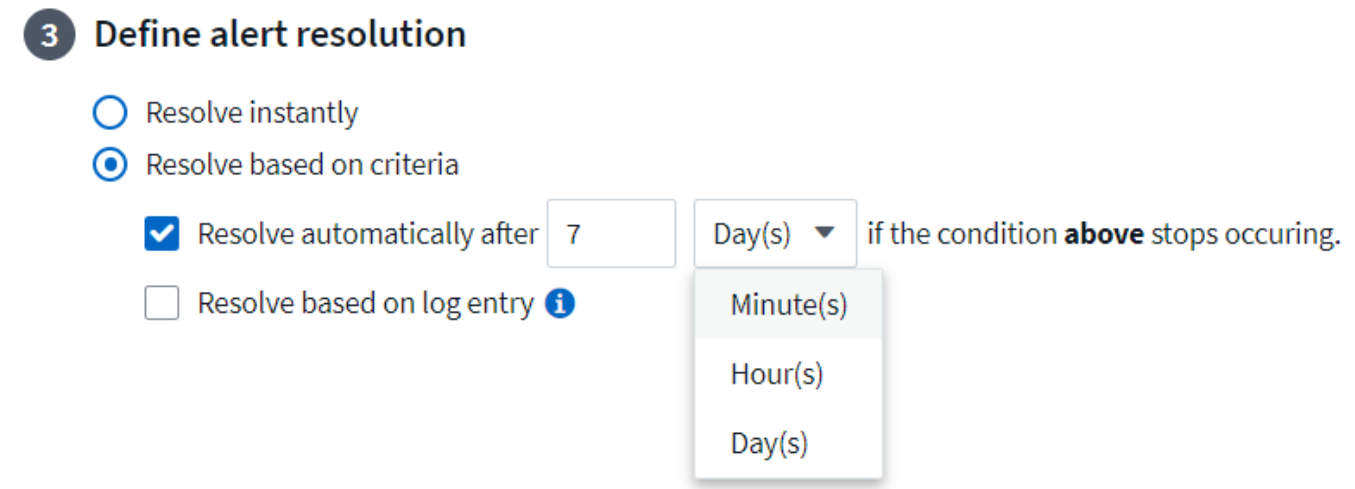
Die folgenden Betriebssysteme werden mit Cloud Insights Acquisition Units unterstützt, zusätzlich zu denen"bereits unterstützt" :

- Red Hat Enterprise Linux 8.9, 8.10, 9.4
- Rocky 9.4
- AlmaLinux 9.3 und 9.4

Mai 2024

Automatisches Lösen von Warnmeldungen basierend auf der Zeit

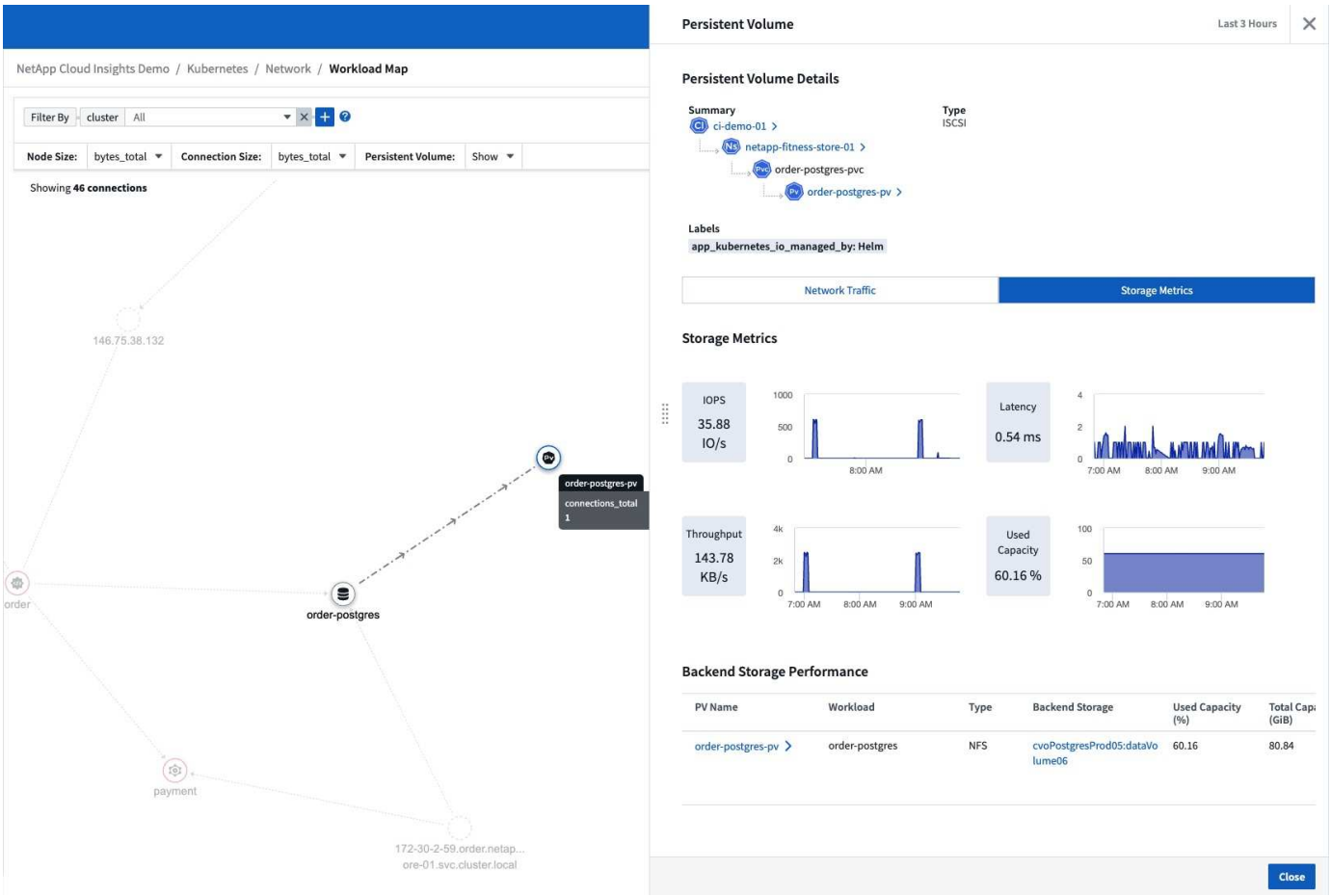
Protokollwarnungen können jetzt zeitbasiert aufgelöst werden. Wenn die Warnbedingung nicht mehr auftritt, kann Cloud Insights die Warnung nach Ablauf einer angegebenen Zeit automatisch auflösen. Sie können wählen, ob die Warnung innerhalb von Minuten, Stunden oder Tagen behoben werden soll.



April 2024

iSCSI-Unterstützung für Kubernetes

Cloud Insights unterstützt jetzt die Zuordnung des mit Kubernetes verknüpften iSCSI-Speichers. Dies ermöglicht eine schnellere Fehlerbehebung mithilfe der Kubernetes-Netzwerkkarte und die Möglichkeit, über Reporting Chargeback- oder Showback-Berichte bereitzustellen.



Betriebssystemunterstützung

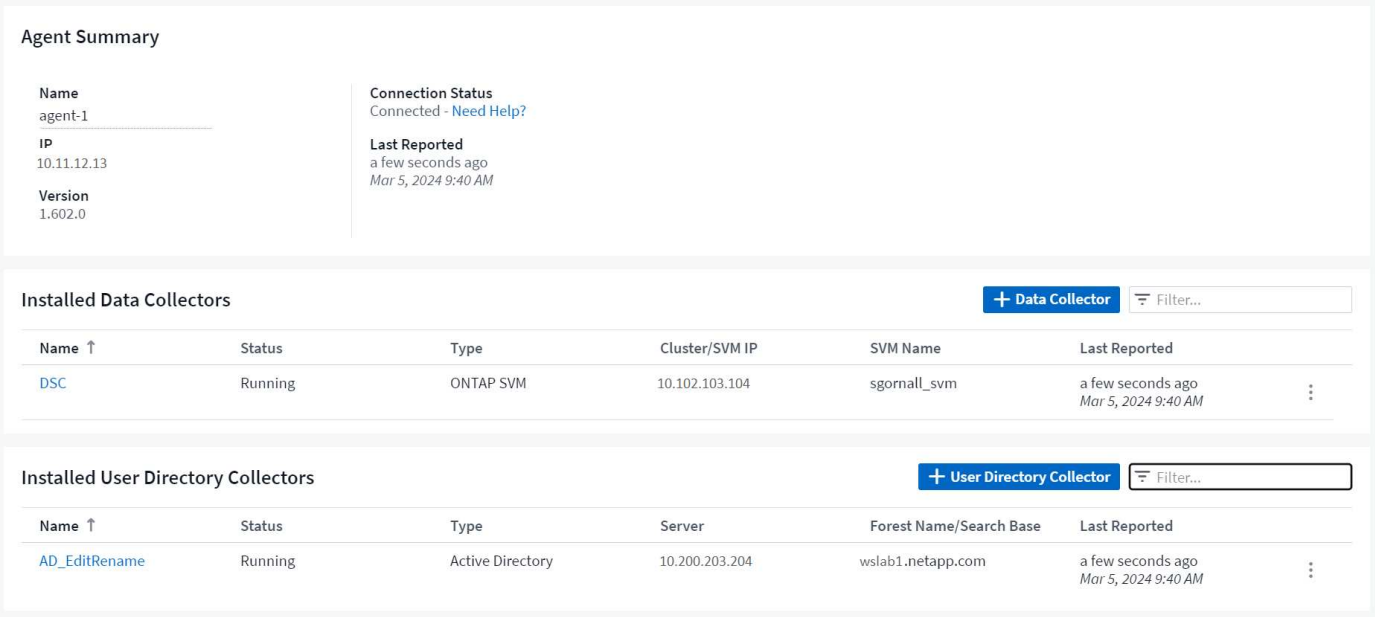
Die folgenden Betriebssysteme werden mit Cloud Insights Acquisition Units unterstützt, zusätzlich zu denen"bereits unterstützt" :

- Oracle Enterprise Linux 8.8
- Red Hat Enterprise Linux 8.8
- Rocky 9.3
- OpenSUSE Leap 15.1 bis 15.5
- SUSE Enterprise Linux Server 15, 15 SP2 bis 15 SP5

März 2024

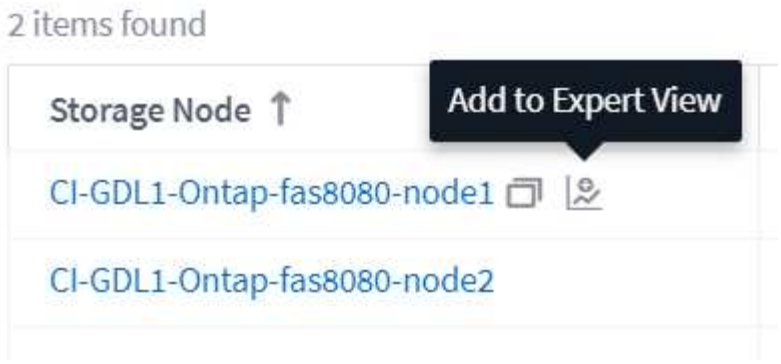
Details zum Workload Security Agent

Jeder Ihrer Workload Security Agents verfügt über eine eigene Zielseite, auf der Sie leicht zusammenfassende Informationen zum Agenten sowie zu den installierten Daten- und Benutzerverzeichnis-Sammlern sehen können, die mit diesem Agenten verknüpft sind.

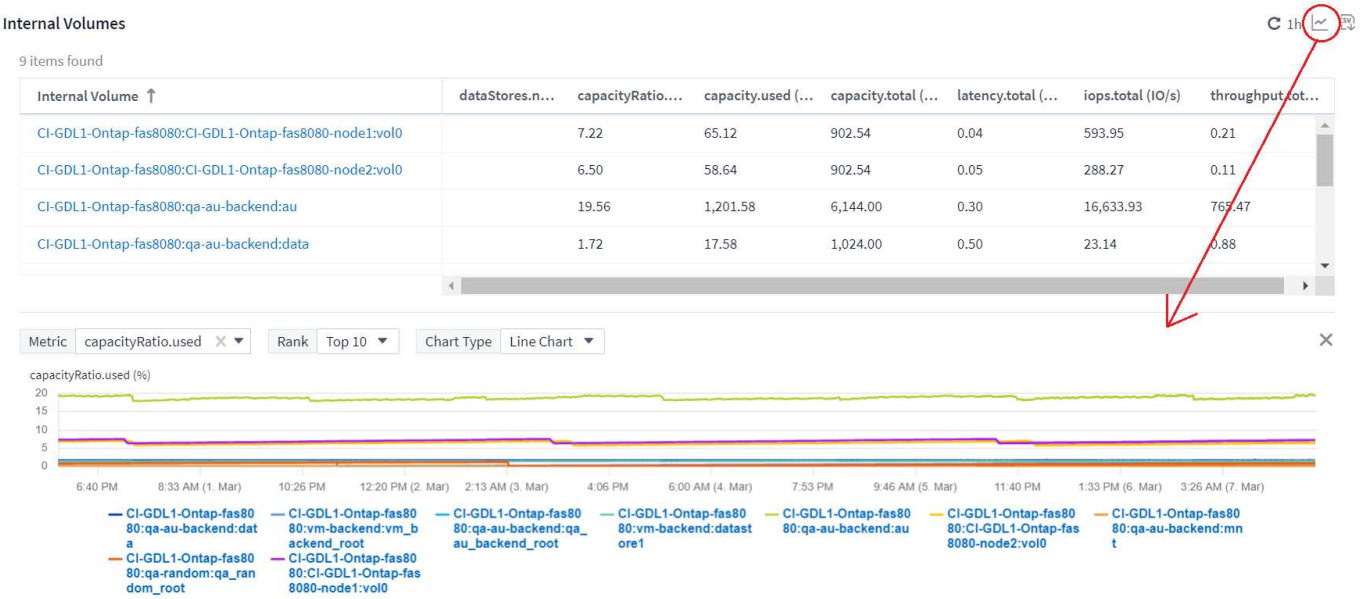


Schnelleres Darstellen größerer Datenmengen

Beim Analysieren von Daten auf der Zielseite eines Assets ist das Hinzufügen zusätzlicher Daten zu den Diagrammen der Expertenansicht ein Kinderspiel. Wenn ein Objekttyp relevante Daten enthält, bewegen Sie für jede Tabelle auf der Zielseite den Mauszeiger über das Objekt, um das Symbol „Zur Expertenansicht hinzufügen“ anzuzeigen. Durch Auswahl dieses Symbols wird das Objekt zu den zusätzlichen Ressourcen hinzugefügt und in den Diagrammen der Expertenansicht angezeigt.



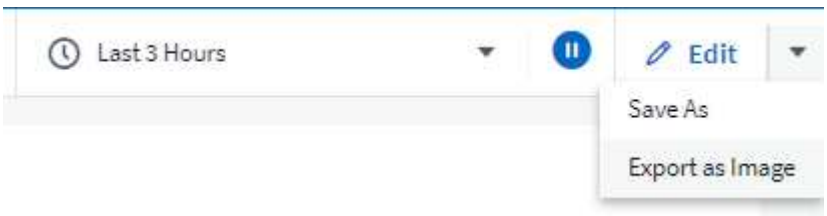
Oder Sie möchten die Daten einer Zielseitentabelle in einem eigenen Diagramm anzeigen. Wählen Sie einfach das Symbol *Diagramm anzeigen* aus, um das Diagramm unter der Tabelle zu öffnen:



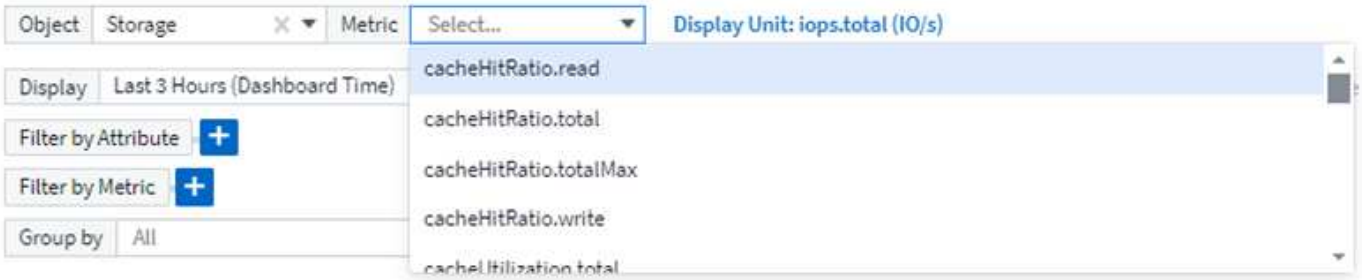
Februar 2024

Verbesserungen der Benutzerfreundlichkeit

Speichern Sie einen **Schnappschuss** Ihres aktuellen Dashboards, indem Sie im Dropdown-Menü in der rechten Ecke „Als Bild exportieren“ auswählen. Cloud Insights erstellt eine PNG-Datei mit den aktuellen Widget-Zuständen.

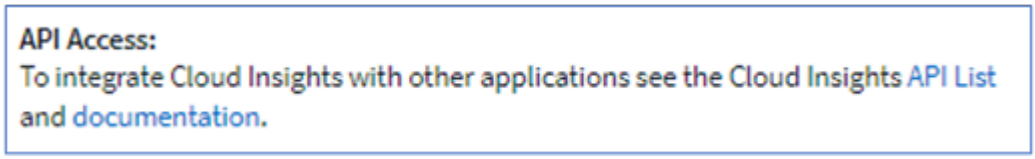


Die **Objekt- und Metrikauswahl** ist für Widgets, Monitore usw. einfacher als je zuvor. Wählen Sie den gewünschten Objekttyp und dann im separaten Dropdown-Menü eine für dieses Objekt relevante Metrik aus.



Exportieren Sie Listen mit Datensammlern und Erfassungseinheiten in das CSV-Format, indem Sie das Symbol oben auf diesen Seiten auswählen.

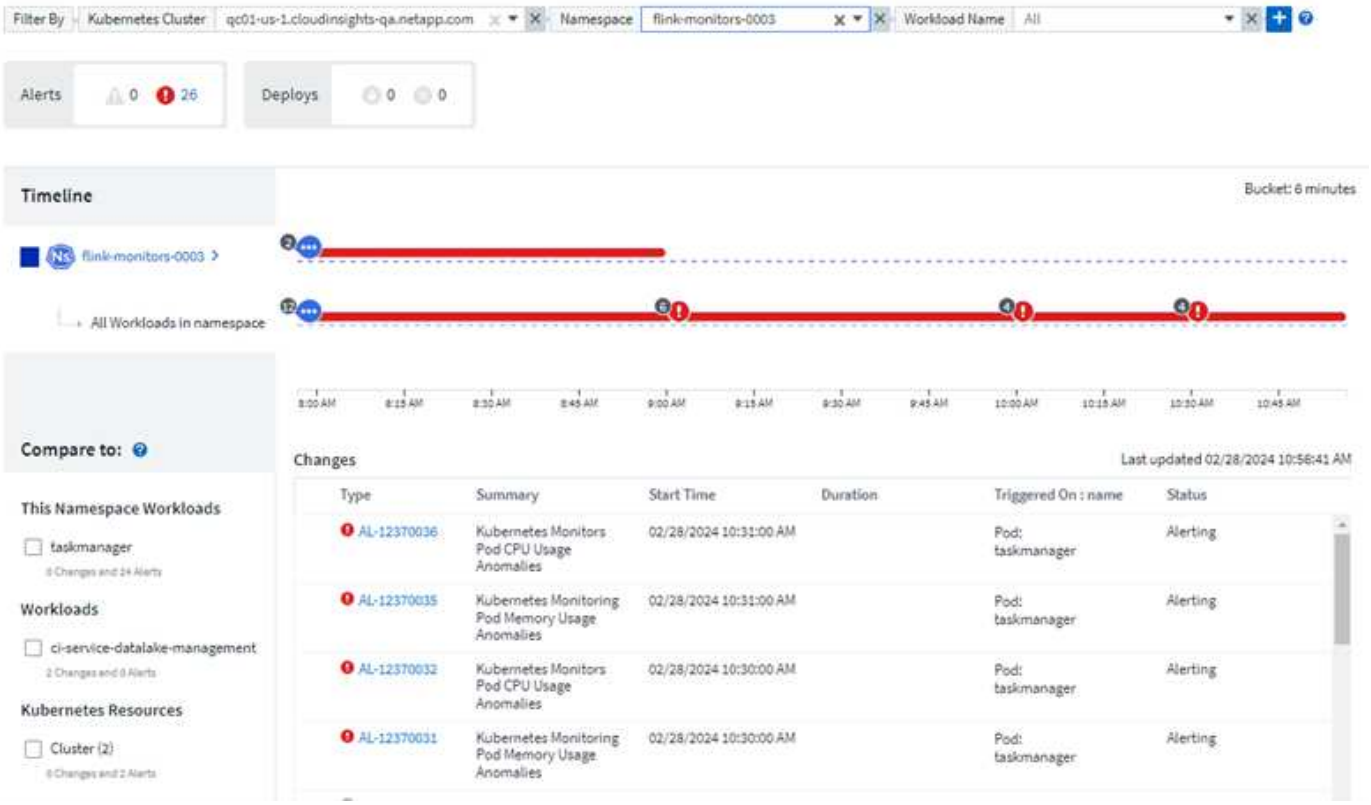
Wir haben die Seite „Hilfe > Support“ **neu organisiert**, damit Sie leichter finden, wonach Sie suchen. Und weil Sie danach gefragt haben, haben wir auf dieser Seite direkte Links zu **API Swagger** und zur Benutzerdokumentation hinzugefügt.



Links in der Spalte „TriggeredOn“ auf der Seite mit der Warnmeldungsliste navigieren zur entsprechenden Zielseite, sofern für dieses Objekt eine Zielseite verfügbar ist.

Alle Änderungen in Ihrem Namespace anzeigen

Mit der Kubernetes-Änderungsanalyse können Sie jetzt eine Zeitleiste der Änderungen anzeigen, wenn Sie Cluster und Namespace auswählen. Zuvor muss auch Workload ausgewählt worden sein. Beim Filtern nach Cluster und Namespace wird die Zeitleiste aller Workloadänderungen in diesem Namespace in einer Zeile angezeigt.



Zugehörige Protokolle für Warnungen

Beim Anzeigen einer Protokollwarnung werden zugehörige Protokolleinträge in einer neuen Tabelle angezeigt. Ein Protokolleintrag ist relevant, wenn er aus derselben Quelle und im selben Zeitraum wie die Warnung stammt und denselben Bedingungen unterliegt. Wählen Sie „Protokolle analysieren“, um weitere Informationen zu erhalten.

Erfassen Sie ONTAP Switch-Daten

Cloud Insights kann Daten von den Back-End-Switches des ONTAP Systems sammeln. Aktivieren Sie dazu einfach die Sammlung im Abschnitt „Erweiterte Konfiguration“ des Datensammlers und stellen Sie sicher, dass das ONTAP System so konfiguriert ist, dass es"Switch-Informationen" und verfügt über die entsprechenden"Berechtigungen" Satz.

Workload Security Data Collector-API

In großen Umgebungen können Sie die Erstellung von Workload Security-Collectoren mithilfe der neuen Data Collectors-API automatisieren. Navigieren Sie zu **Admin > API-Zugriff > API-Dokumentation** und wählen Sie

den API-Typ *Workload Security* aus, um mehr zu erfahren.

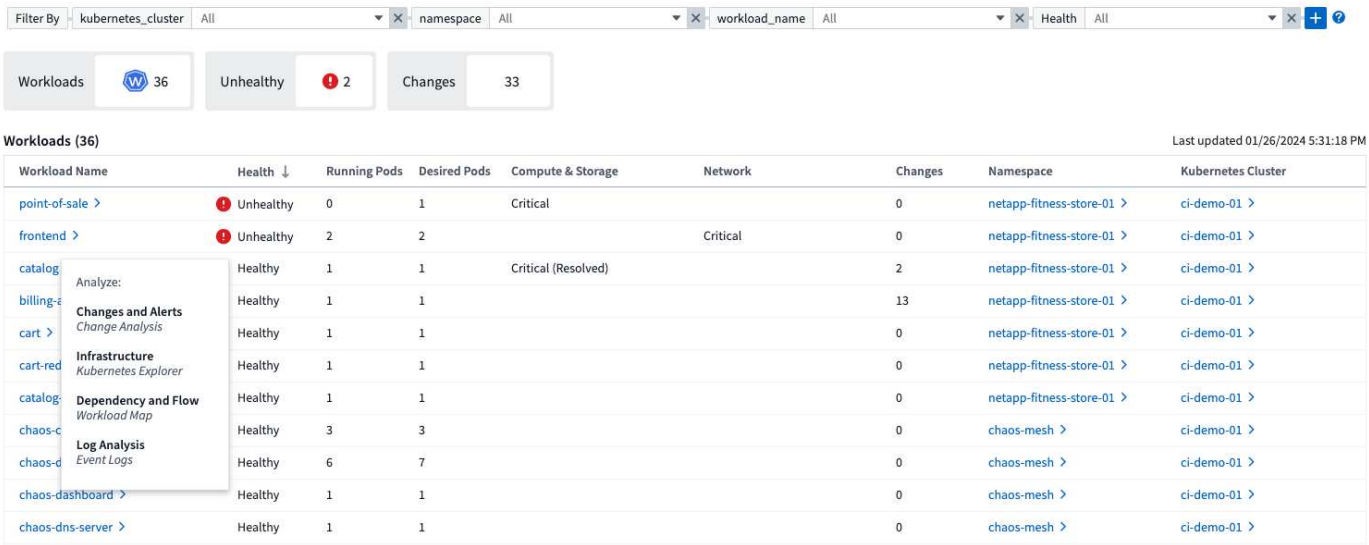
Januar 2024

Testen Sie Cloud Insights -Funktionen, die Sie noch nicht verwendet haben

Zusätzlich zu Ihrer ersten Testversion von Cloud Insights können Sie auch folgende Vorteile nutzen:"Modulevaluationen" . Wenn Sie beispielsweise Cloud Insights abonniert haben und Speicher und virtuelle Maschinen überwacht haben, starten Sie beim Hinzufügen von Kubernetes zu Ihrer Umgebung automatisch eine 30-tägige Testversion von Kubernetes Observability. Die Nutzung der verwalteten Einheiten von Kubernetes Observability wird erst nach Ablauf des Testzeitraums auf Ihren abonnierten Anspruch angerechnet.

Wie gesund ist meine Arbeitsbelastung?

Der Workload-Status ist auf der Seite **Kubernetes > Erkunden > Workloads** auf einen Blick verfügbar, sodass Sie schnell erkennen können, welche Workloads gut funktionieren und welche möglicherweise etwas Hilfe benötigen. Ermitteln Sie mühelos, ob das Integritätsproblem mit Infrastruktur-, Netzwerk- oder Konfigurationsänderungen zusammenhängt, und analysieren Sie die Grundursache im Detail.



Datensammler-Updates

Datendomänenidentifizierung

Der Data Domain-Collector wurde verbessert, um HA-Systeme für eine längere Lebensdauer bei Failover-Ereignissen besser zu identifizieren. Diese Änderung führt zu einer **einmaligen** Neuidentifizierung von Data Domain-Geräten in HA-Systemen, was anschließend dazu führt, dass alle Anmerkungen zu diesen Assets entfernt werden (da diese Arrays neu identifiziert werden). Sie müssen Ihren Data Domain-Objekten erneut Anmerkungen hinzufügen.

Verbesserter ML-Algorithmus zur Ransomware-Erkennung

Workload Security umfasst einen neuen ML-Algorithmus der 2. Generation zur Ransomware-Erkennung, um die raffiniertesten Angriffe schneller und genauer zu erkennen.

„Saisonalität“ des Verhaltens: Das Verhalten am Wochenende kann anderen Mustern folgen als an Wochentagen oder das Verhalten am Morgen anders als am Nachmittag. Die Algorithmen der Workload-Sicherheit berücksichtigen diese Saisonalität.

Veraltete Funktionalität

Gelegentlich werden Funktionen aufgrund der Weiterentwicklung veraltet. Hier sind einige der Features und Funktionen, die in Cloud Insights veraltet sind:

Workload Secure REST cloudsecure_forensics.activities.v1 API ist veraltet

Die API *cloudsecure_forensics.activities.v1* ist veraltet. Diese API gibt Informationen zu Aktivitäten zurück, die mit Entitäten in der Storage Workload Security-Umgebung verknüpft sind. Diese API wurde durch cloudsecure_forensics.activities.*v2*_ ersetzt.

GET für diese API hat zuvor Folgendes zurückgegeben:

```
{
  "count": 24594,
  "limit": 1000,
  "offset": 0,
  "results": [
    {
      "accessLocation":
```

Diese API gibt jetzt Folgendes zurück:

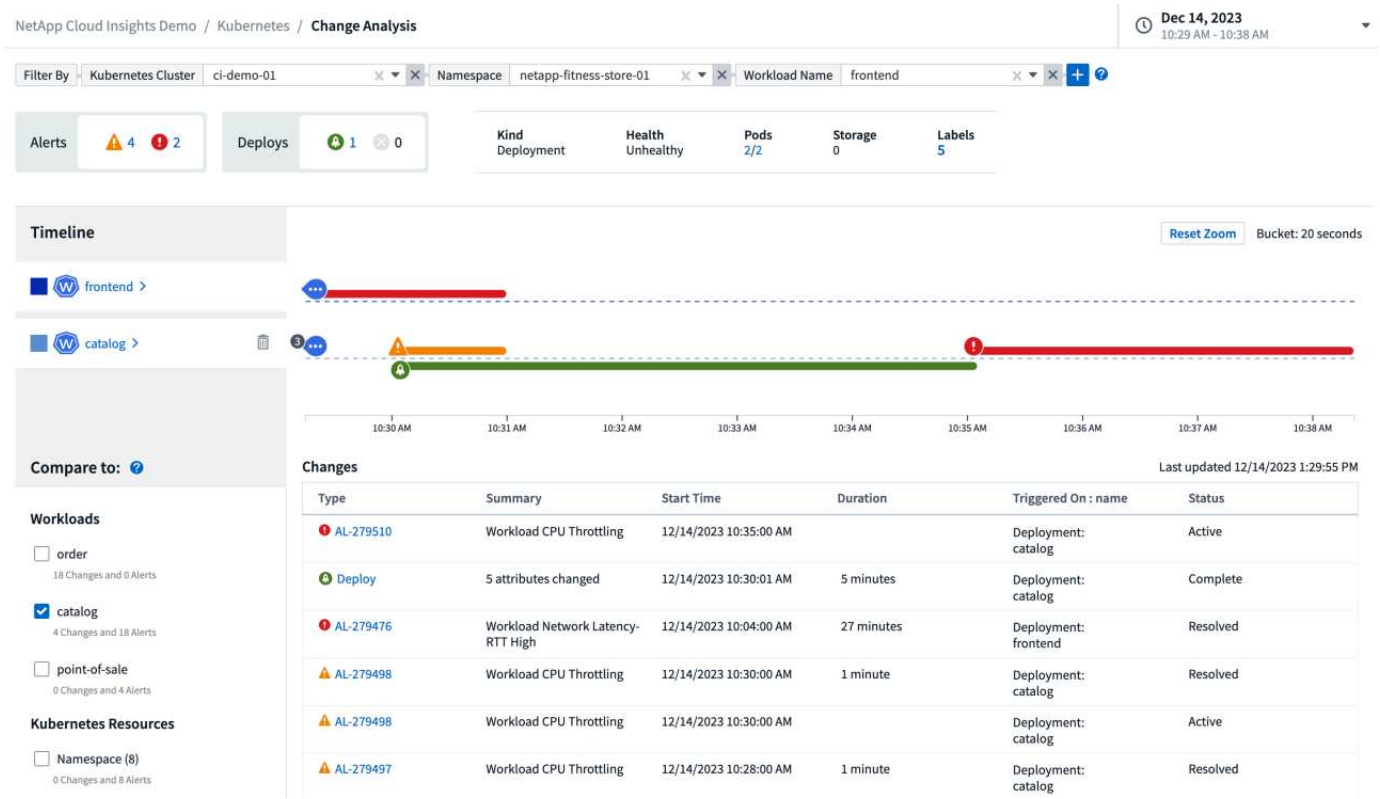
```
{
  "limit": 1000,
  "meta": {
    "page": {
      "after": "lvlvk3pp.4cpzcg4kpybl",
      "before": "lvlxy3dz.4cq5ajdnl9fk",
      "size": 1000
    }
  },
  "results": [
    {
      "accessLocation": "10.249.6.220",
```

Weitere Einzelheiten finden Sie in der Swagger-Dokumentation unter „Admin > API-Zugriff > API-Dokumentation > Workload-Sicherheit“.

Dezember 2023

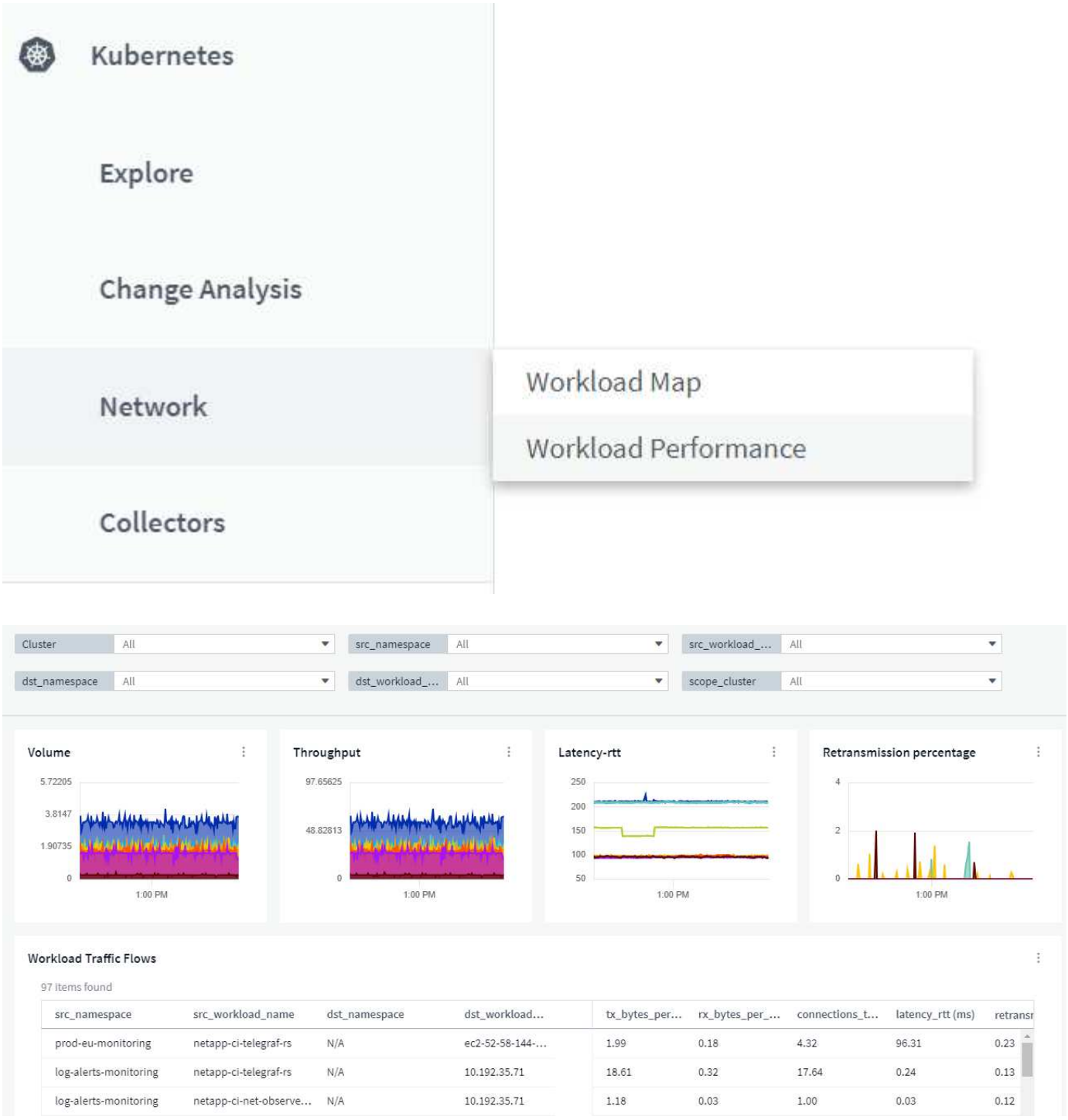
Change Analytics auf einen Blick

Kubernetes"Änderungsanalyse" bietet Ihnen eine umfassende Übersicht über die jüngsten Änderungen an Ihrer Kubernetes-Umgebung. Sie haben immer Zugriff auf Warnmeldungen und den Bereitstellungsstatus. Mit Change Analytics können Sie jede Bereitstellungs- und Konfigurationsänderung verfolgen und mit dem Zustand und der Leistung der Dienste, Infrastruktur und Cluster von K8s korrelieren.



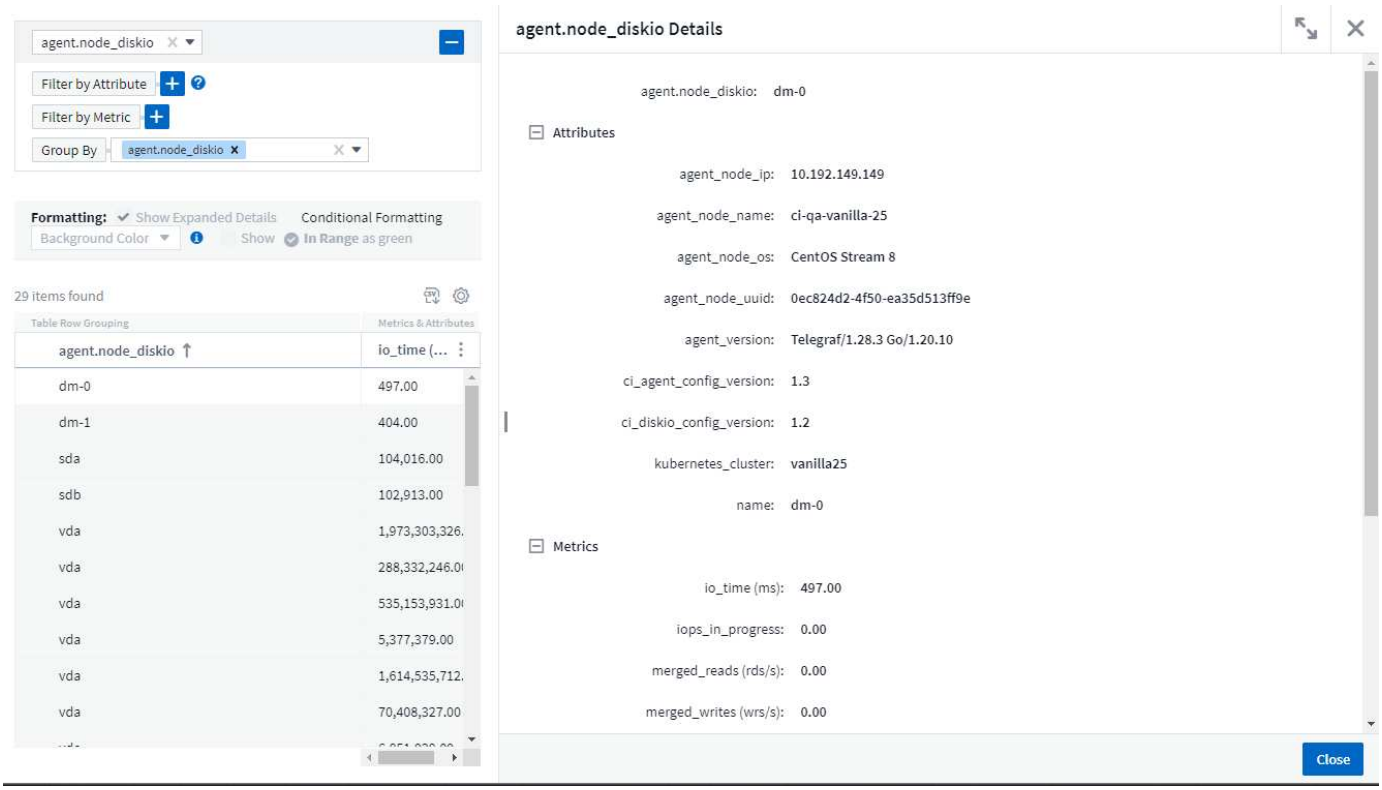
Kubernetes-Workload-Leistungs-Dashboard

Die Workload-Leistung ist im umfassenden Kubernetes Workload Performance-Dashboard auf einen Blick verfügbar. Zeigen Sie schnell Diagramme zu Volumen, Durchsatz, Latenz und Neuübertragungstrends sowie eine Tabelle mit dem Workload-Verkehr für jeden Namespace in Ihrer Umgebung an. Filter ermöglichen eine einfache Fokussierung auf interessante Bereiche.



Abfragedetails auf einem Bildschirm

Wenn Sie in einer Abfrage eine Zeile auswählen, wird ein Seitenbereich geöffnet, in dem Attribut-, Anmerkungs- und Metrikdetails für die ausgewählte Zeile angezeigt werden. So erhalten Sie hilfreiche Informationen, ohne dass Sie sich in die Zielseite des Objekts einarbeiten müssen. Links in der Zeile oder im Seitenbereich ermöglichen eine einfache Navigation.



Aktualisierungen des Datensammlers:

- * Brocade FOS REST*: Dieser Collector wurde aus der „Vorschau“ entfernt und ist jetzt allgemein verfügbar. Einige Dinge, die Sie beachten sollten:
  - FOS hat seine REST-API mit FOS 8.2 eingeführt. Einige Funktionen wie das Routing erhielten jedoch erst mit 9.0 REST-API-Funktionen.
  - Wenn Sie über ein Fabric verfügen, das aus gemischten FOS-Assets ab 8.2 sowie einigen < 8.2 besteht, kann der Cloud Insights FOS REST-Collector diese älteren Assets nicht erkennen. Sie können den FOS REST-Collector bearbeiten und eine durch Kommas getrennte Liste der IPv4-Adressen der Geräte erstellen, die von diesem Collector ausgeschlossen werden sollen.
- **SELinux**: Cloud Insights enthält Verbesserungen an der Erstinstallation der Linux Acquisition Unit, um die Robustheit des Betriebs in Linux-Umgebungen mit aktivierter SELinux-Durchsetzung sicherzustellen. Diese Verbesserungen wirken sich nur auf *neue* AU-Bereitstellungen aus. Wenn Sie SELinux-Probleme im Zusammenhang mit AU-Upgrades haben, wenden Sie sich an den NetApp Support, um Ihre SELinux-Konfiguration zu beheben.

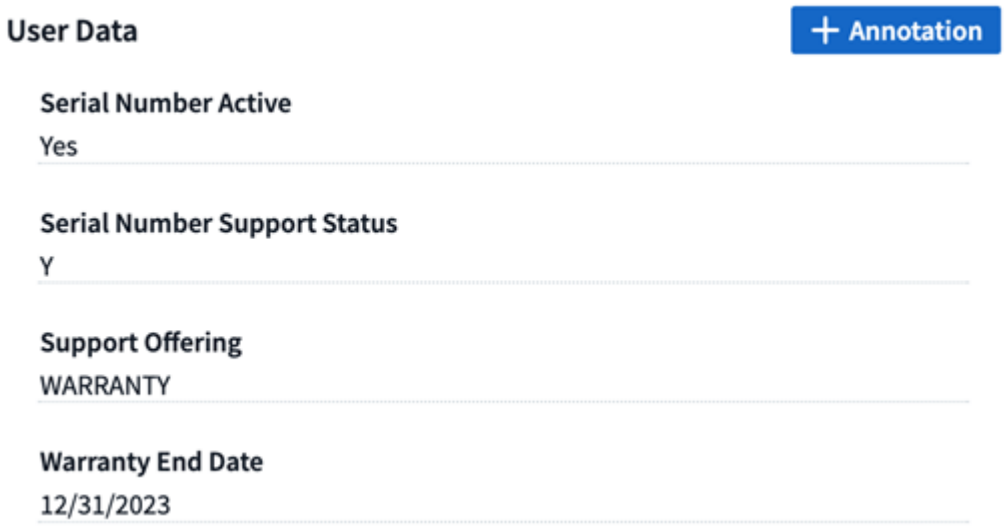
November 2023

Workload-Sicherheit: Einen Collector anhalten/fortsetzen

In Workload Security können Sie einen Datensammler anhalten, wenn sich der Sammler im Status „Wird ausgeführt“ befindet. Öffnen Sie das „Drei-Punkte“-Menü für den Collector und wählen Sie PAUSE. Während der Collector angehalten ist, werden keine Daten von ONTAP gesammelt und keine Daten vom Collector an ONTAP gesendet. Wählen Sie „Fortsetzen“, um erneut mit dem Sammeln zu beginnen.

Informationen zum Storage Node-Support

Auf der Zielseite eines Speicherknotens bietet der Abschnitt „Benutzerdaten“ auf einen Blick Informationen zu Ihrem Supportangebot, dem aktuellen Status, dem Supportstatus und dem Garantieende. Beachten Sie, dass Cloud Insights diese Informationen derzeit nur für NetApp -Geräte automatisch veröffentlicht. Beachten Sie auch, dass es sich bei diesen Supportfeldern um Anmerkungen handelt, sodass sie in Abfragen und Dashboards verwendet werden können.



VMWare-Tags zu Cloud Insights -Anmerkungen zuordnen

Der"VMWare" Mit dem Datensammler können Sie Cloud Insights -Textanmerkungen mit gleichnamigen Tags füllen, die auf VMWare konfiguriert sind.

Verbesserungen der Brocade CLI-Collector-Zuverlässigkeit für FOS 9.1.1c und höhere Firmware

Auf einigen Brocade Fibre Channel-Switches mit der Firmware 9.1.1c kann der Ausgabe bestimmter CLI-Befehle der Anmeldebannertext „motd“ oder Warnungen für Benutzer vorangestellt sein, die Standardkennwörter zu ändern. Der Brocade CLI-Collector wurde erweitert, um diese beiden Arten von irrelevantem Text zu ignorieren.

Vor dieser Verbesserung waren mit diesem Collector-Typ wahrscheinlich nur FOS 9.1.1c-Switches ohne vorhandene Virtual Fabrics erkennbar.

Oktober 2023

Verbesserte Workload-Sicherheit

Die Workload-Sicherheit wurde wie folgt verbessert:

- **Zugriff verweigert**: Workload Security integriert sich mit ONTAP , um"„Zugriff verweigert“-Ereignisse" und bieten eine zusätzliche Analyse- und automatische Antwortebene.
- **Erlaubte Dateitypen**: Wenn ein Ransomware-Angriff für eine bekannte Dateierweiterung erkannt wird,

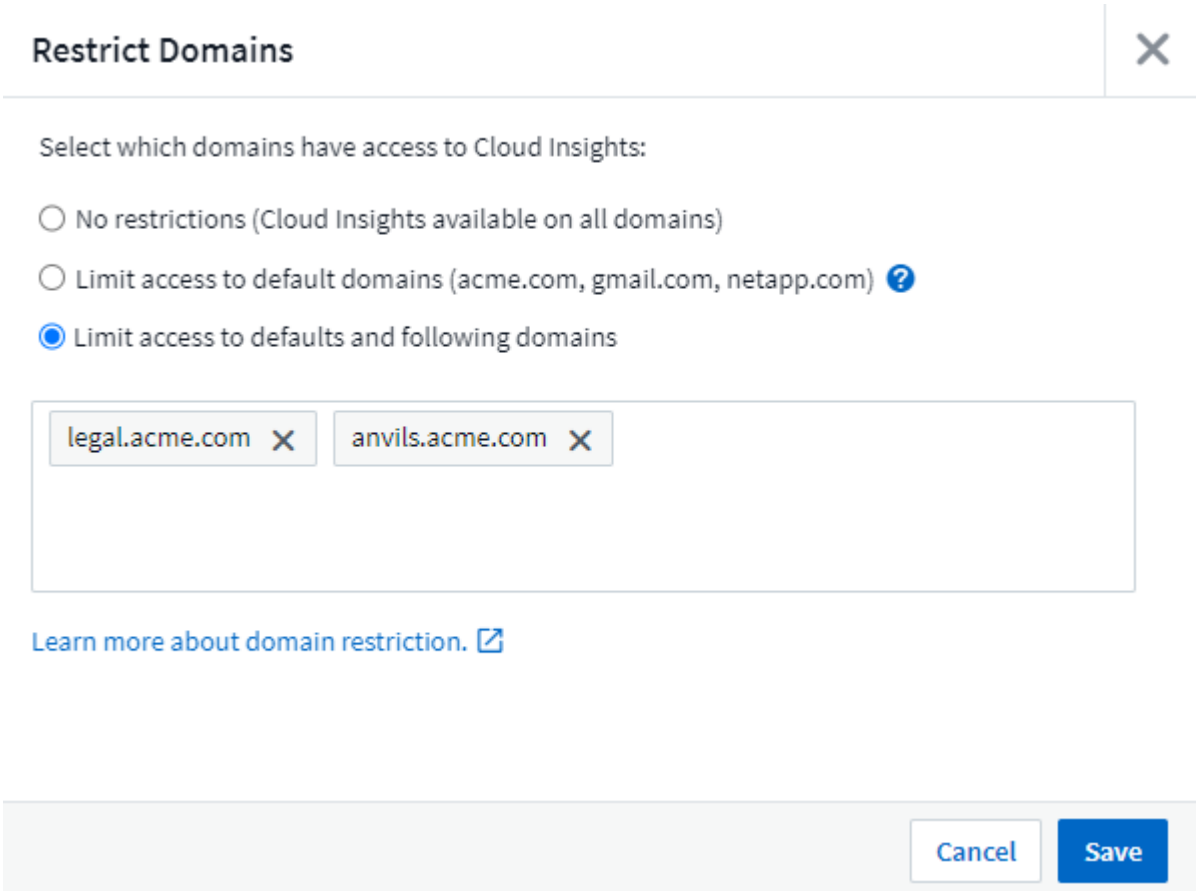
kann diese Dateierweiterung zu einem"zulässige Dateitypen" Liste, um unnötige Alarme zu vermeiden.

Modulversuche

Zusätzlich zu Ihrer ersten Testversion von Cloud Insights können Sie auch folgende Vorteile nutzen:"Modulevaluationen" . Wenn Sie beispielsweise Infrastructure Observability bereits abonniert haben, aber Kubernetes zu Ihrer Umgebung hinzufügen, beginnen Sie automatisch mit einer 30-tägigen Testversion von Kubernetes Observability. Die Nutzung Ihrer verwalteten Kubernetes Observability-Einheit wird Ihnen erst am Ende des Evaluierungszeitraums in Rechnung gestellt.

Beschränken Sie den Zugriff auf bestimmte Domänen

Administratoren und Kontoinhaber haben nun die Möglichkeit,"Beschränken Sie den Zugriff auf Cloud Insights" an die von ihnen angegebenen E-Mail-Domänen. Gehen Sie zu **Admin > Benutzerverwaltung** und wählen Sie die Schaltfläche *Domänen einschränken*.



Datensammler-Updates

Die folgenden Änderungen an der Datenerfassungseinheit wurden vorgenommen:

- **Isilon / PowerScale REST**: Den erweiterten Analysefunktionen von Cloud Insights wurden unter dem Namen *emc_isilon.node_pool.** verschiedene neue Attribute und Metriken hinzugefügt. Mithilfe dieser Zähler und Attribute können Benutzer Dashboards und Monitore für den Kapazitätsverbrauch von Knotenpools erstellen. Benutzer mit Isilon-Clustern, die aus unterschiedlichen Hardwareknotenmodellen erstellt wurden, verfügen über mehrere Knotenpools. Die Kenntnis Ihres HDD-/SSD-/Gesamtkapazitätsverbrauchs auf Knotenpoolebene ist sowohl für die Überwachung als auch für die Planung hilfreich.

- **Rubrik** Unterstützung für die Authentifizierung „Dienstkonto“: Der Rubrik-Collector von Cloud Insights unterstützt jetzt sowohl die herkömmliche HTTP-Basisauthentifizierung (Benutzername und Passwort) als auch den Dienstkontoansatz von Rubrik, der einen Benutzernamen + Geheimnis + Organisations-ID erfordert.

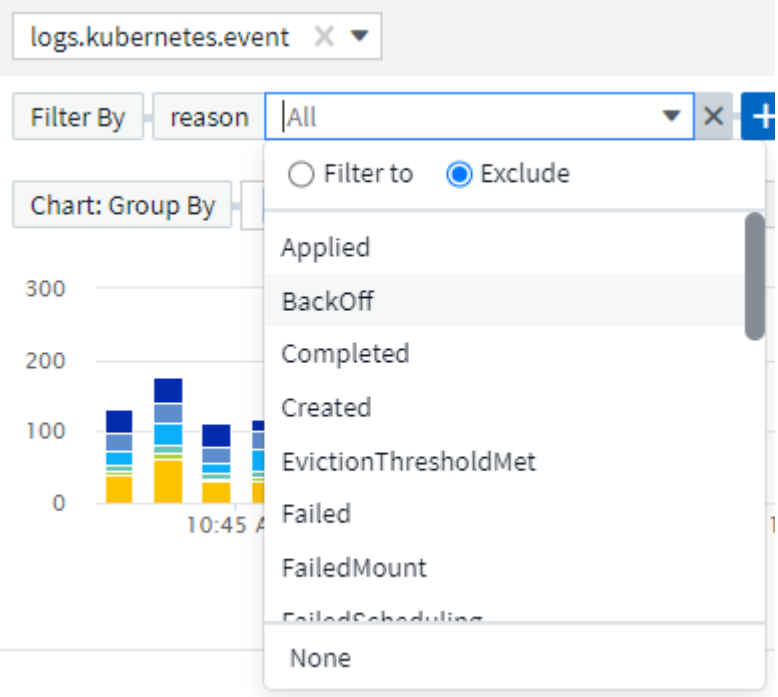
September 2023

Finden Sie ganz einfach, was Sie in den Protokollen suchen

Log Query (**Observability > Log Queries > +New Log Query**) beinhaltet eine Reihe von"Verbesserungen" um die Protokollerkundung einfacher und informativer zu gestalten.

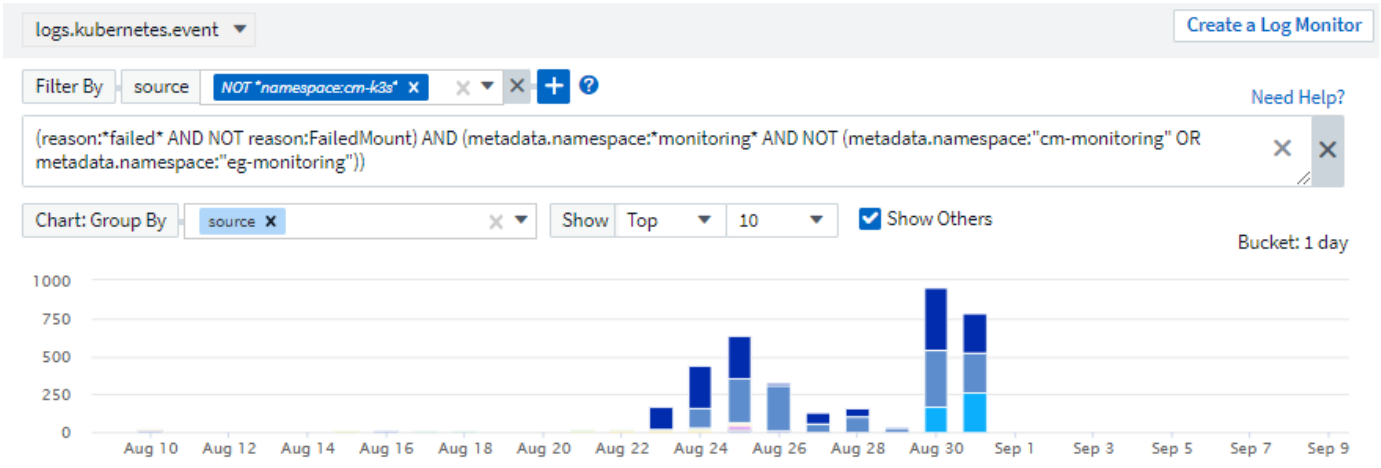
Einschließen/Ausschließen

Beim Filtern nach einem Wert können Sie einfach auswählen, ob Sie Ergebnisse, die dem Filter entsprechen, **einschließen** oder **ausschließen** möchten. Durch Auswahl von „Ausschließen“ wird ein „NICHT <Wert>“-Filter erstellt. Sie können Einschluss- und Ausschlusswerte in einem einzigen Filter kombinieren.



Erweiterte Abfrage

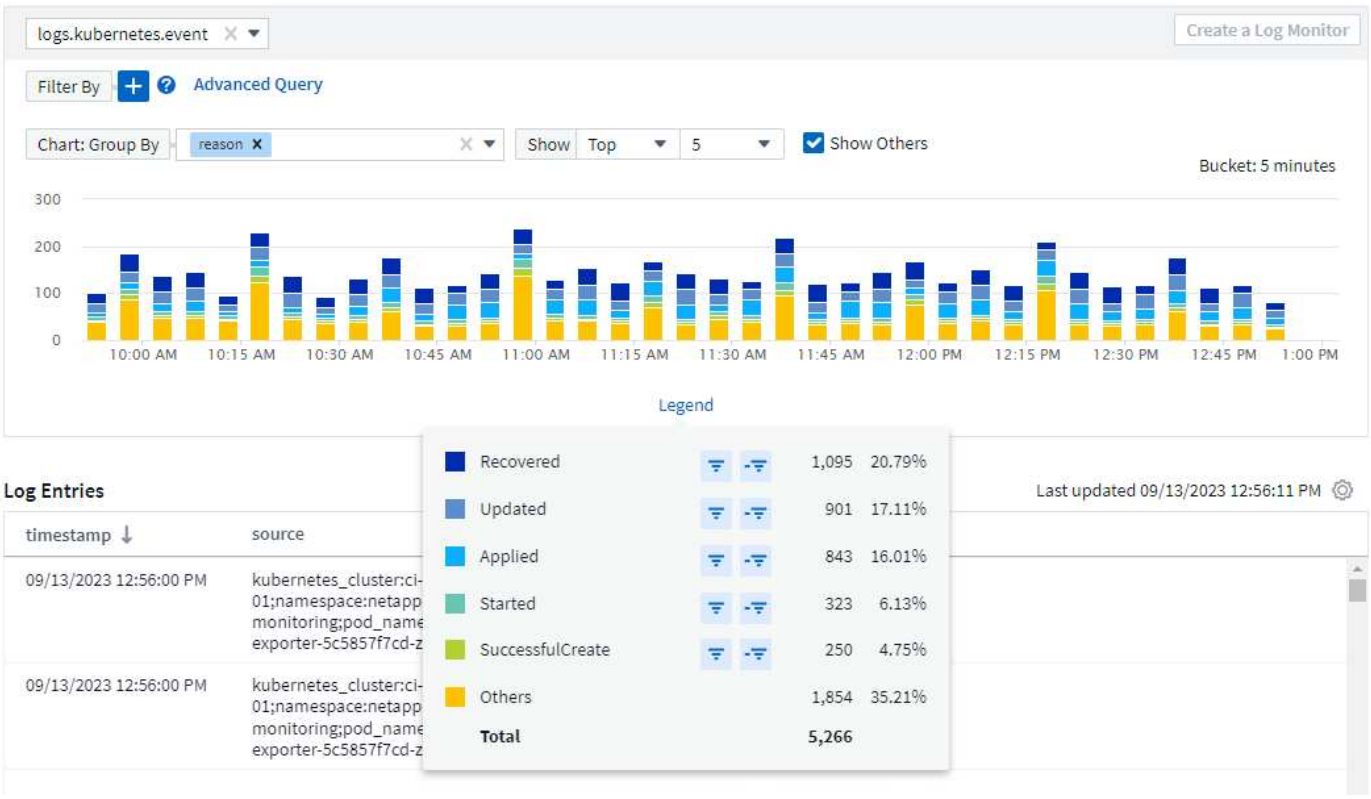
Erweiterte Abfragen bieten Ihnen die Möglichkeit, Freiformfilter zu erstellen und Werte mithilfe von UND, NICHT, ODER, Platzhaltern usw. zu kombinieren oder auszuschließen.



„Filtern nach“ und „Erweiterte Abfrage“ werden per „UND“ verknüpft, um eine einzige Abfrage zu bilden. Die Ergebnisse werden in der Ergebnisliste und im Diagramm angezeigt.

Gruppierung im Diagramm

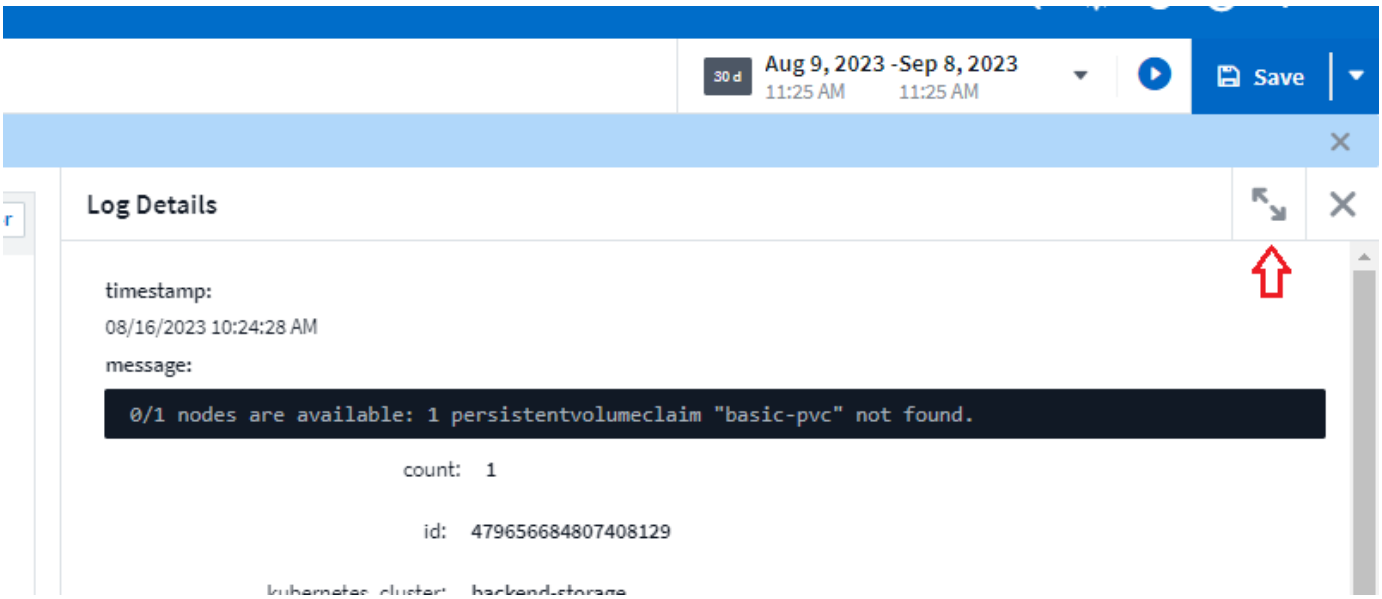
Wenn Sie ein Protokollattribut zum **Gruppieren nach** auswählen, zeigen die Liste und das Diagramm die Ergebnisse des aktuellen Filters. Im Diagramm sind die Spalten nach Farben gruppiert. Wenn Sie mit der Maus über eine Spalte im Diagramm fahren, werden Details zu den jeweiligen Einträgen angezeigt, ähnlich den Gesamtinformationen, die beim Erweitern der Diagrammlegende angezeigt werden. In der Legende können Sie auch einen Einschluss- oder Ausschlussfilter für eine bestimmte Gruppierung festlegen.



„Floating“-Log-Detailbereich

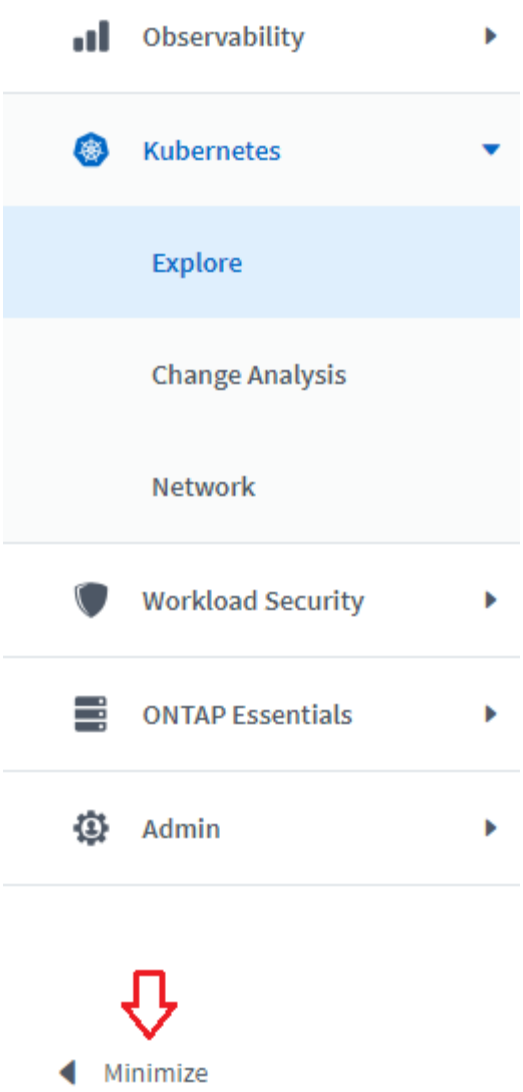
Wenn Sie Protokolle mithilfe der Protokollabfrage untersuchen, wird durch Auswahl eines Eintrags in der Liste ein Detailbereich für diesen Eintrag geöffnet. Sie können nun wählen, ob das Slideout-Panel „schwebend“ (d.

h. über dem Rest des Bildschirms angezeigt) oder „auf der Seite“ (d. h. als eigener Rahmen innerhalb der Seite angezeigt) angezeigt werden soll. Um zwischen diesen Ansichten zu wechseln, wählen Sie die Schaltfläche „Auf der Seite/Schwebend“ in der oberen rechten Ecke des Bedienfelds.



Menü einklappen

Sie können das Cloud Insights -Navigationsmenü auf der linken Seite reduzieren, indem Sie die Schaltfläche „Minimieren“ unter dem Menü auswählen. Wenn das Menü minimiert ist, können Sie mit der Maus über ein Symbol fahren, um zu sehen, welcher Abschnitt geöffnet wird. Wenn Sie das Symbol auswählen, wird das Menü geöffnet und Sie gelangen direkt zu diesem Abschnitt.



Verbesserungen beim Datensammler

Cloud Insights hat das Anzeigen und Auffinden von Datensammlerinformationen vereinfacht:

- **Die Verarbeitung von Datensammlerlisten** ist effizienter, was bedeutet, dass die zum Anzeigen und Navigieren dieser Listen benötigte Zeit erheblich reduziert wird. Wenn Sie über eine große Umgebung mit vielen Datensammlern verfügen, werden Sie eine erhebliche Verbesserung feststellen, wenn Sie Ihre Datensammler auflisten.
- Die **Data Collector Support Matrix** wurde von einer PDF-Datei auf eine HTML-basierte Seite verschoben, die schneller zu navigieren und einfacher zu verwalten ist. Schauen Sie sich hier die neue Matrix an: https://docs.netapp.com/us-en/cloudinsights/reference_data_collector_support_matrix.html

August 2023

Sammeln von Isilon/PowerScale-Protokollen und erweiterten Analysedaten

Die Isilon REST- und PowerScale REST-Kollektoren enthalten die folgenden Verbesserungen:

- Isilon-Protokollereignisse stehen für Abfragen und Warnungen zur Verfügung
- Isilon Advanced Analytic-Attribute stehen zur Verwendung in Abfragen, Dashboards und Warnungen zur Verfügung:
  - emc_isilon.cluster
  - emc_isilon.node
  - emc_isilon.node_disk
  - emc_isilon.net_iface

Diese sind standardmäßig für Benutzer der Isilon REST- und/oder PowerScale REST-Collectors aktiviert. NetApp empfiehlt Benutzern des Isilon CLI-basierten Collectors dringend, auf den neuen REST API-basierten Collector zu migrieren, um Verbesserungen wie die oben genannten zu erhalten.

Verbesserte Workload-Karte

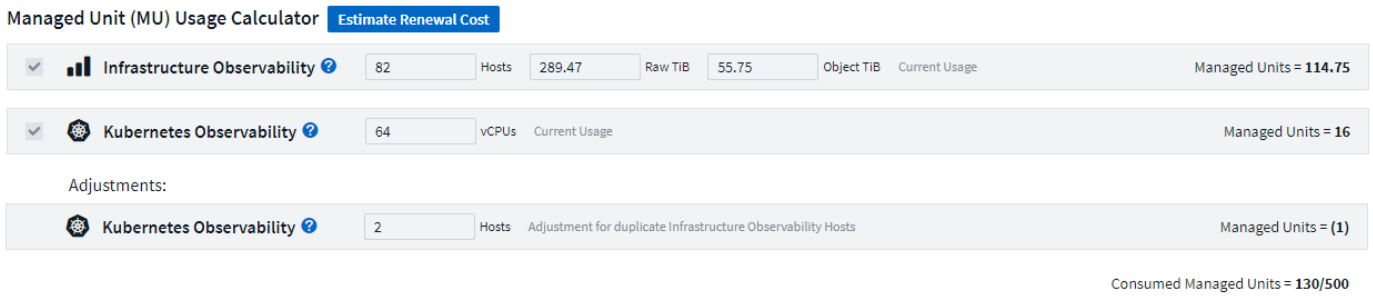
Die Workload-Karte ist benutzerfreundlicher und weniger verrauscht. Sie gruppiert alle ähnlichen externen Dienste in einem Knoten, wenn sie mit denselben Workloads kommunizieren. Dadurch wird die Komplexität des Diagramms reduziert und es wird leichter verständlich, wie die Dienste miteinander verbunden sind.

Wenn Sie einen gruppierten Knoten auswählen, wird eine detaillierte Tabelle mit den Netzwerkverkehrsmetriken für jeden für diesen Knoten relevanten externen Dienst angezeigt.

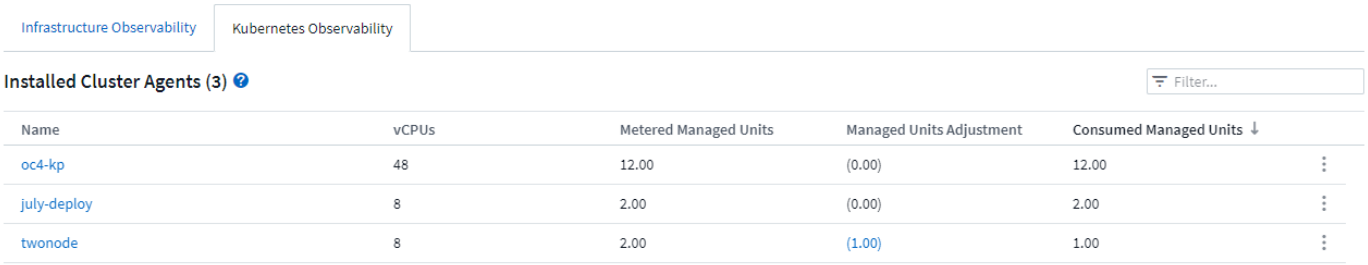
Anpassung der Kubernetes Managed Unit-Nutzung

Falls eine Rechenressource in Ihrer Kubernetes-Clusterumgebung sowohl vom NetApp Kubernetes Monitoring Operator als auch von einem zugrunde liegenden Infrastrukturdatensammler (z. B. VMware) gezählt wird, wird Ihre Nutzung dieser Ressourcen angepasst, um eine möglichst effiziente Zählung der verwalteten Einheiten zu gewährleisten. Sie können die Kubernetes MU-Anpassungen auf der Seite „Admin > Abonnement“ sowohl auf der Registerkarte „Zusammenfassung“ als auch auf der Registerkarte „Nutzung“ anzeigen.

Registerkarte „Zusammenfassung“:



Registerkarte „Verwendung“:



Änderungen beim Sammler/Erwerb:

Die folgenden Änderungen an der Datenerfassungseinheit wurden vorgenommen:

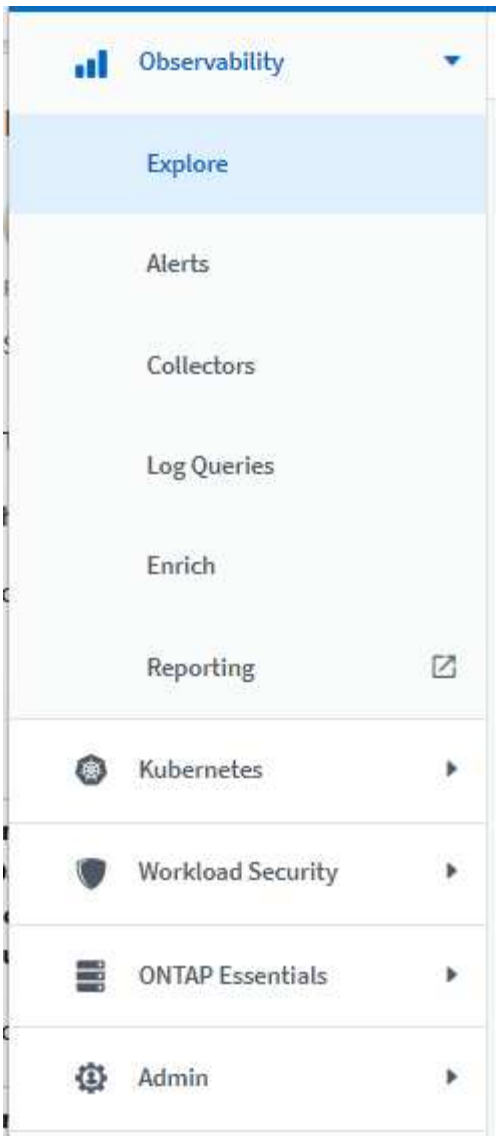
- Akquisitionseinheiten unterstützen jetzt RHEL 8.7.

Verbesserte Menüs

Wir haben das linke Navigationsmenü aktualisiert, um die Arbeitsabläufe unserer Kunden besser zu unterstützen. Neue Elemente der obersten Ebene wie *Kubernetes* bieten beschleunigten Zugriff auf die Anforderungen des Kunden und eine konsolidierte Administratorkonsole unterstützt die Rolle des Mandanteneigentümers.

Hier sind einige weitere Beispiele für die Änderungen:

- Das Menü „Observability“ auf oberster Ebene zeigt Datenerkennung, Alarmierung und Protokollabfragen.
- Die API-Zugriffsfunktion für Observability und Workload-Sicherheit befindet sich in einem Menü.
- Gleiches gilt für die Funktion „Benachrichtigungen“ für Observability und Workload Security, jetzt ebenfalls unter einem Menü



Hier ist eine kurze Liste der Funktionen, die Sie unter jedem Menü finden:

Beobachtbarkeit:

- Erkunden (Dashboards, Metrikabfragen, Infrastruktureinblicke)
- Warnungen (Monitore und Warnungen)
- Sammler (Datensammler und Erfassungseinheiten)
- Protokollabfragen
- Anreichern (Anmerkungen und Anmerkungsregeln, Anwendungen, Geräteauflösung)
- Berichterstattung

Kubernetes:

- Cluster-Erkundung und Netzwerkkarte

Workload-Sicherheit:

- Warnungen

- Forensik
- Sammler
- Richtlinien

ONTAP Essentials:

- Datensicherung
- Sicherheit
- Warnungen
- Infrastruktur
- Vernetzung
- Arbeitslasten *VMware

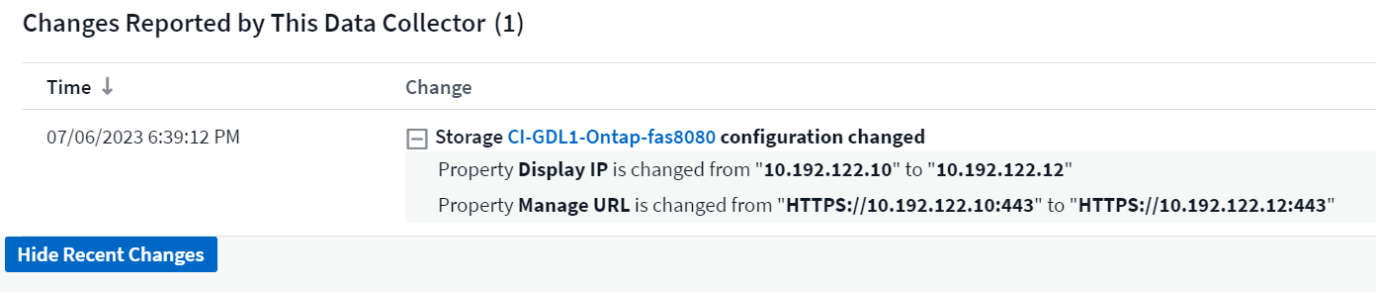
Administrator:

- API-Zugriff
- Wirtschaftsprüfung
- Benachrichtigungen
- Abonnementinformationen
- Benutzerverwaltung

Juli 2023

Letzte Änderungen anzeigen

Die Zielseiten des Datensammlers enthalten jetzt eine Liste der letzten Änderungen. Klicken Sie einfach auf die Schaltfläche „Letzte Änderungen“ unten auf einer beliebigen Zielseite des Datensammlers, um die letzten Änderungen am Datensammler anzuzeigen.



Verbesserungen für den Operator

Die folgenden Verbesserungen wurden vorgenommen an"Kubernetes-Operator" Einsatz:

- Option zum Umgehen der Docker-Metrikerfassung
- Möglichkeit, Toleranzen zu Telegraf-Daemonsets und Replicasets hinzuzufügen und anzupassen

Einblick: Kühllager zurückgewinnen

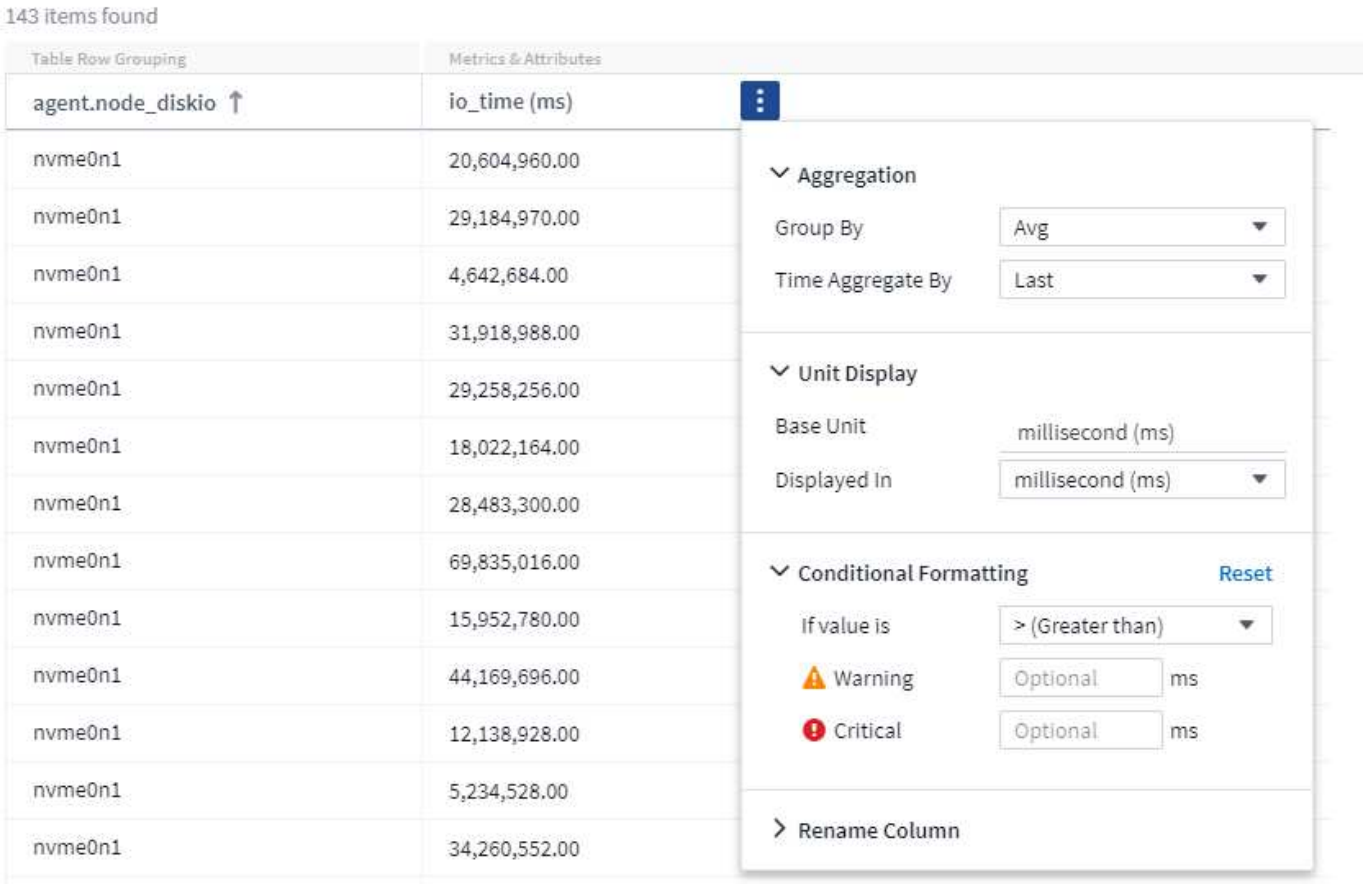
Der"Gewinnen Sie ONTAP Cold Storage Insights zurück" unterstützt jetzt FlexGroups und ist jetzt für alle Kunden verfügbar.

Bildsignatur des Bedieners

Kunden, die ein privates Repository für ihren NetApp Kubernetes Monitoring Operator verwenden, können jetzt während der Operator-Installation den öffentlichen Schlüssel der Image-Signatur kopieren und so die Authentizität der heruntergeladenen Software bestätigen. Wählen Sie im optionalen Schritt „Operatorbild in Ihr privates Repository hochladen“ die Schaltfläche „Öffentlichen Schlüssel der Bildsignatur kopieren“ aus.

Aggregation, bedingte Formatierung und mehr für Abfragen

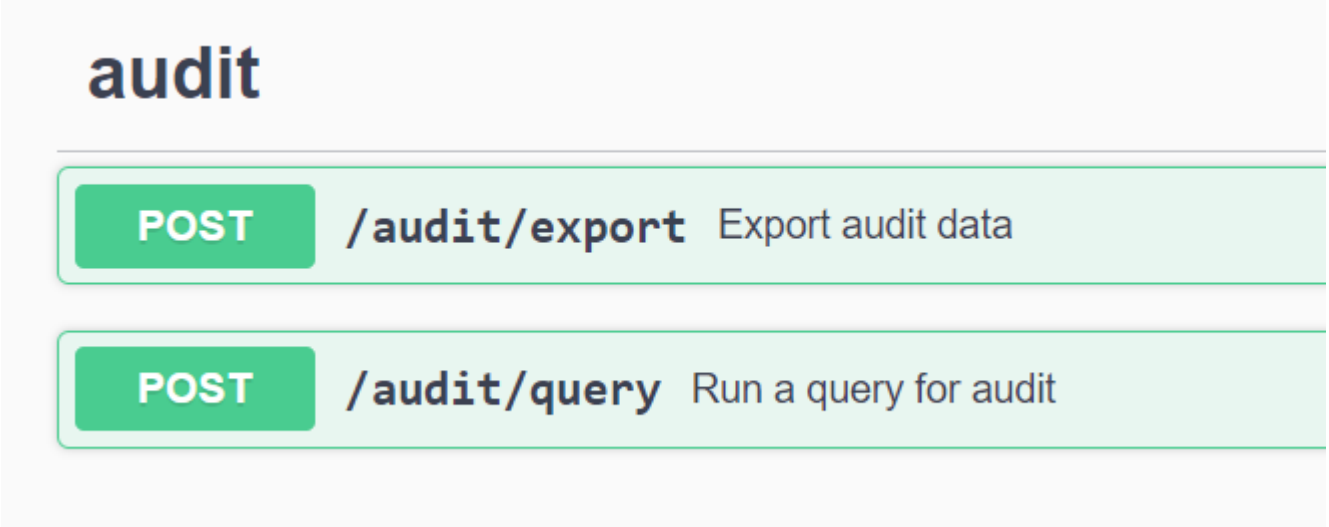
Aggregation, Einheitenauswahl, bedingte Formatierung und Spaltenumbenennung gehören zu den nützlichsten Funktionen eines Dashboard-Tabellen-Widgets, und jetzt sind dieselben Funktionen verfügbar für"Abfragen" .



Diese Funktionen sind jetzt für Daten vom Integrationstyp (Kubernetes, ONTAP Advanced Metrics usw.) verfügbar und werden in Kürze für Infrastrukturobjekte (Speicher, Volume, Switch usw.) verfügbar sein.

API für Audit

Sie können jetzt eine API verwenden, um überwachte Ereignisse abzufragen oder zu exportieren. Gehen Sie zu Admin > API-Zugriff und wählen Sie den Link *API-Dokumentation* aus, um weitere Informationen zu erhalten.



Datensammler: Trident Economy

Cloud Insights unterstützt jetzt den Trident Economy Driver und bietet folgende Vorteile:

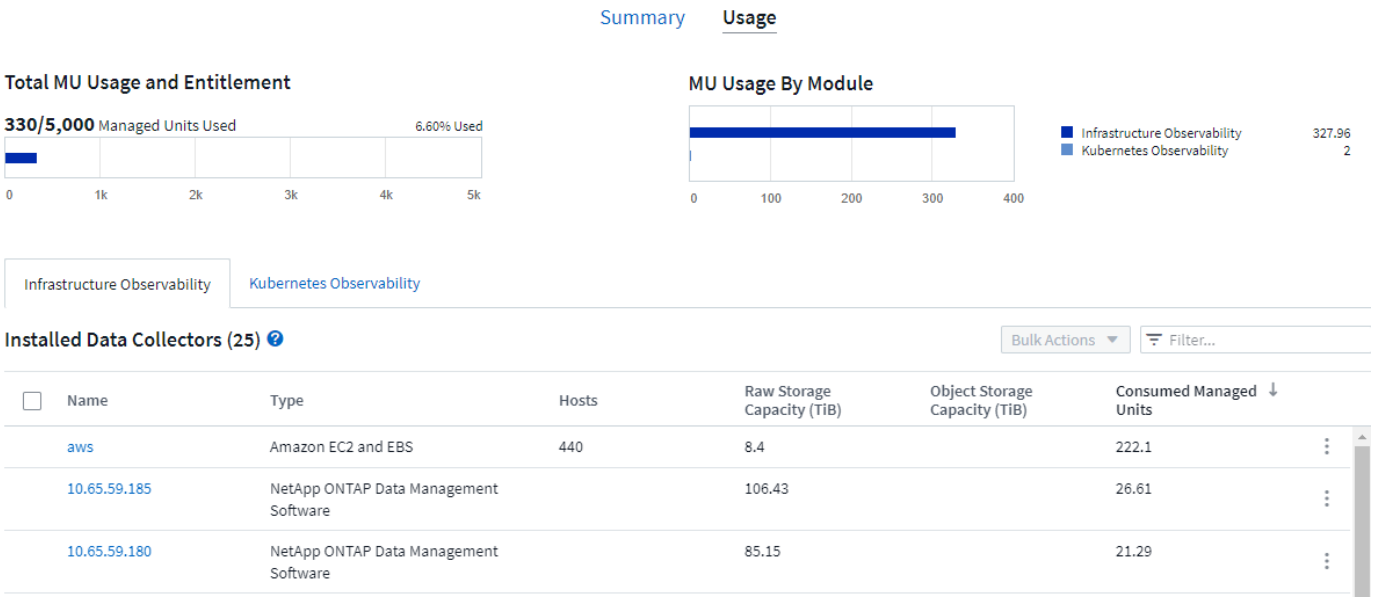
- Erhalten Sie Einblick in die Pod-to- ONTAP Qtree-Zuordnung und Leistungsmetriken.
- Sorgen Sie für nahtlose Fehlerbehebung und einfache Navigation von Kubernetes-Pods zum Backend-Speicher
- Erkennen Sie proaktiv Backend-Leistungsprobleme mit Monitoren

---

Juni 2023

Überprüfen Sie Ihre Nutzung

Ab Juni 2023 bietet Cloud Insights eine Aufschlüsselung der Nutzung verwalteter Einheiten basierend auf dem Funktionsumfang. Jetzt können Sie die Nutzung verwalteter Einheiten (MU) für Ihre Infrastruktur sowie die an Kubernetes gebundene MU-Nutzung schnell anzeigen und überwachen.



Kubernetes Network Monitoring und Map ist für alle verfügbar

Der"*Kubernetes-Netzwerkleistung und -Karte*" Vereinfacht die Fehlerbehebung durch die Abbildung von Abhängigkeiten zwischen Kubernetes-Workloads und bietet Echtzeit-Einblicke in die Leistungslatenzen und -anomalien des Kubernetes-Netzwerks, um Leistungsprobleme zu erkennen, bevor sie sich auf die Benutzer auswirken. Viele Kunden fanden es während der Vorschau hilfreich und jetzt steht es allen zur Verfügung.

Änderungen beim Sammler/Erwerb:

Die folgenden Änderungen an der Datenerfassungseinheit wurden vorgenommen:

- Data Domain- und Cohesity-MUs werden mit 40 TiB : 1 MU gemessen.
- Acquisition Units unterstützen jetzt RHEL und Rocky 9.0 und 9.1.

Neue ONTAP Essentials Dashboards

Die folgenden ONTAP Essentials-Dashboards waren in Vorschauumgebungen verfügbar und sind jetzt für alle verfügbar:

- Sicherheits-Dashboard
- Datenschutz-Dashboard (beinhaltet Übersichten zum lokalen und Remote-Schutz)

Zusätzliche Systemmonitore

Die folgenden Systemmonitore sind in Cloud Insights enthalten:

- Storage VM FCP-Dienst nicht verfügbar
- Storage VM iSCSI-Dienst nicht verfügbar

Mai 2023

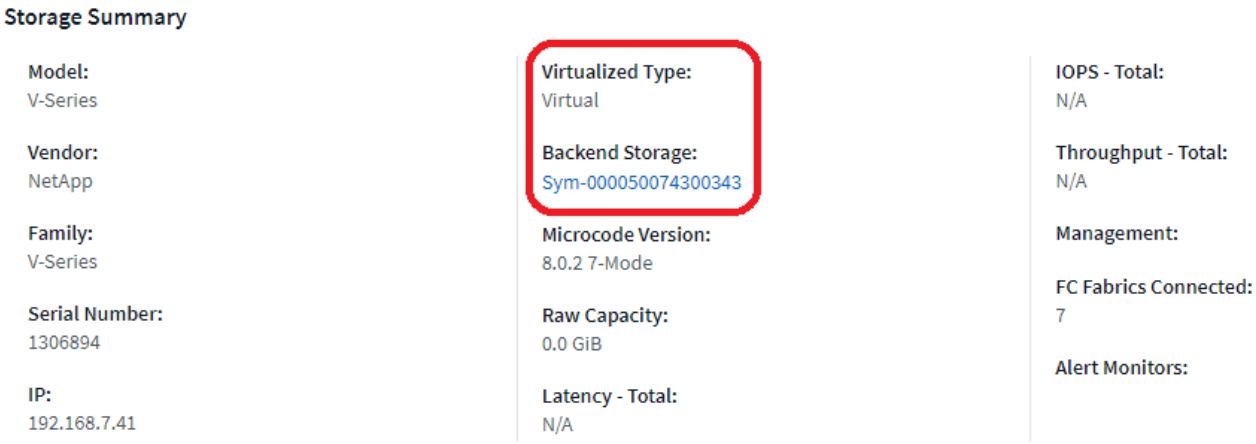
Verbesserte Installation des Kubernetes-Überwachungsoperators

Installation und Konfiguration des"NetApp Kubernetes Monitoring Operator" ist mit den folgenden Verbesserungen einfacher als je zuvor:

- Umfeld"Konfigurationseinstellungen" werden in einer einzigen, selbstdokumentierten Konfigurationsdatei gespeichert.
- Schritt-für-Schritt-Anleitung zum Hochladen von Kubernetes Monitoring Operator-Images in Ihr privates Repository.
- Einfaches Upgrade mit einem einzigen Befehl zum Aktualisieren Ihres Kubernetes-Monitorings unter Beibehaltung benutzerdefinierter Konfigurationen.
- Mehr Sicherheit: API-Schlüssel verwalten Geheimnisse sicher.
- Einfache Integration und Bereitstellung mit Ihren CI/CD-Automatisierungstools.

Speichervirtualisierung

Cloud Insights kann zwischen einem Speicherarray mit lokalem Speicher oder der Virtualisierung anderer Speicherarrays unterscheiden. Dadurch haben Sie die Möglichkeit, Kosten in Beziehung zu setzen und die Leistung vom Front-End bis zum Back-End Ihrer Infrastruktur zu unterscheiden.



Neue Webhook-Parameter

Beim Erstellen einer"Webhook" Benachrichtigung: Sie können jetzt diese Parameter in Ihre Webhook-Definition aufnehmen:

- %%TriggeredOnKeys%%
- %%AusgelöstDurchWerte%%

Berichterstellung zu Kubernetes-Daten

Von Cloud Insights erfasste Kubernetes-Daten – einschließlich Persistent Volumes (PV), PVC, Workloads, Cluster und Namespaces – stehen jetzt für die Berichterstellung zur Verfügung und ermöglichen Chargeback, Trendanalyse, Prognosen, TTF-Berechnungen und andere Geschäftsberichte zu Metriken für Kubernetes.

Standardmäßige ONTAP -Systemmonitore für Neukunden aktiviert

Viele ONTAP -Systemmonitore sind in neuen Cloud Insights Umgebungen standardmäßig aktiviert (d. h. *Fortgesetzt*). Zuvor befanden sich die meisten Monitore standardmäßig im Zustand „Angehalten“. Da die Geschäftsanforderungen von Unternehmen zu Unternehmen unterschiedlich sind, empfehlen wir immer einen Blick auf die"Systemmonitore" in Ihrer Umgebung und pausieren oder setzen Sie jeden Vorgang basierend auf Ihren Alarmierungsanforderungen fort.

April 2023

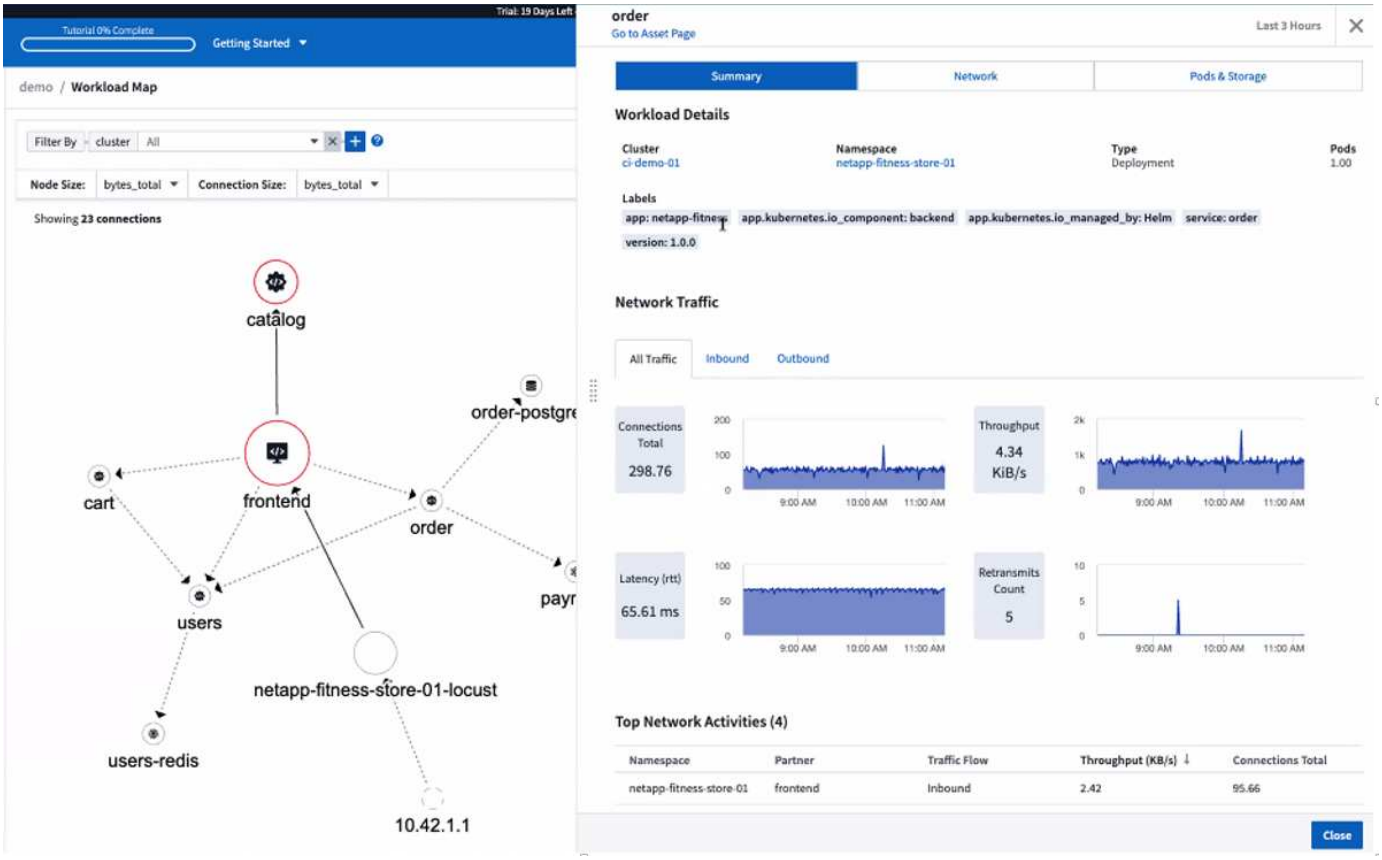
Kubernetes-Leistungsüberwachung und -Karte

Der"*Kubernetes-Netzwerkleistung und -Karte*" Die Funktion vereinfacht die Fehlerbehebung durch die Zuordnung von Abhängigkeiten zwischen Kubernetes-Workloads. Es bietet Echtzeit-Einblicke in die Leistungslatenzen und -anomalien des Kubernetes-Netzwerks, um Leistungsprobleme zu erkennen, bevor sie sich auf die Benutzer auswirken. Diese Funktion hilft Unternehmen, die Gesamtkosten durch die Analyse und Prüfung von Kubernetes-Verkehrsflüssen zu senken.

Hauptfunktionen: • Die Workload Map stellt Kubernetes-Workload-Abhängigkeiten und -Flows dar und hebt Netzwerk- und Leistungsprobleme hervor. • Überwachen Sie den Netzwerkverkehr zwischen Kubernetes-Pods, Workloads und Knoten; identifizieren Sie die Quelle von Verkehrs- und Latenzproblemen. • Reduzieren

Sie die Gesamtkosten, indem Sie eingehenden, ausgehenden, regions- und zonenübergreifenden Netzwerkverkehr analysieren.

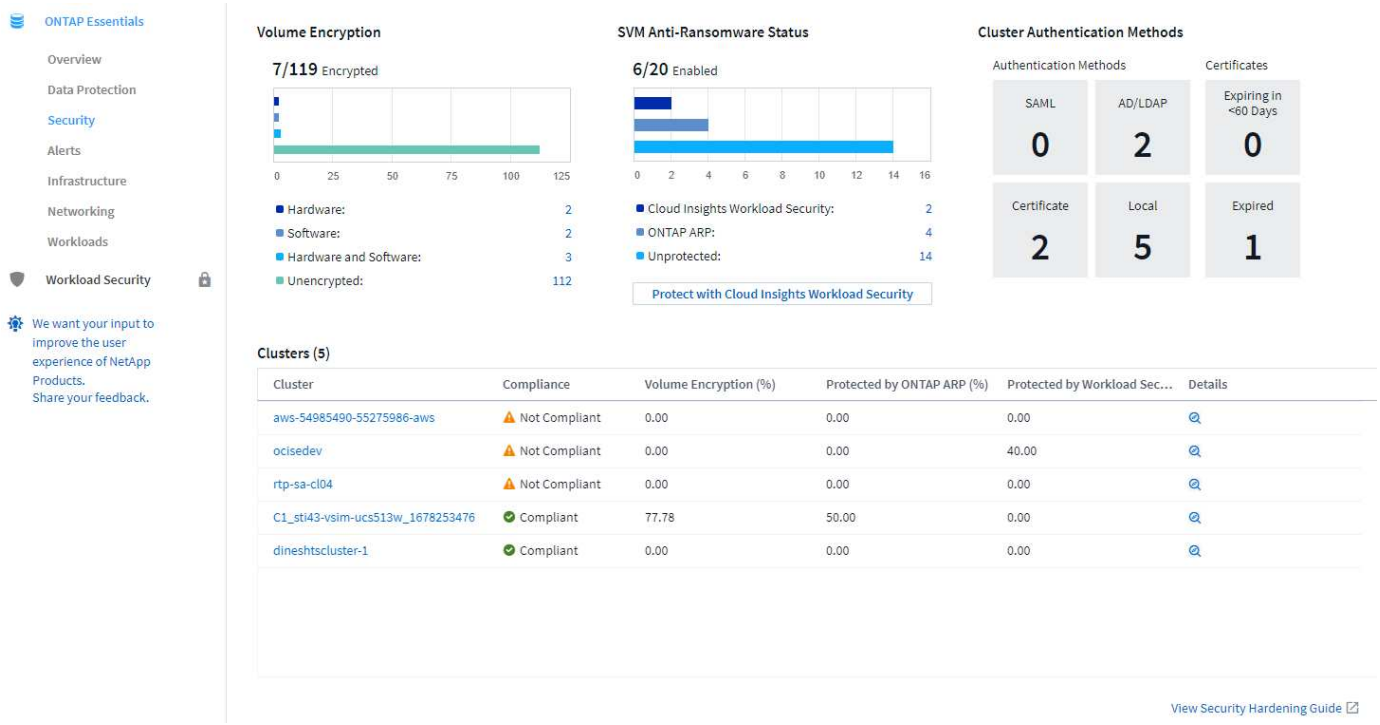
Arbeitslastkarte mit „Slideout“-Details:



Kubernetes Performance Monitoring und Map ist verfügbar als"Vorschau" Besonderheit.

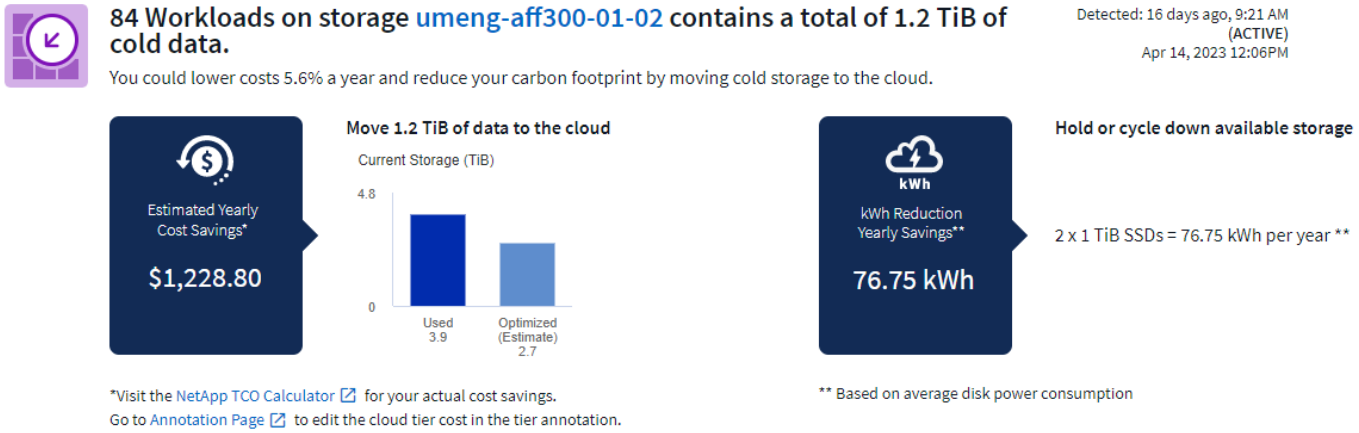
ONTAP Essentials Sicherheits-Dashboard

Der"Sicherheits-Dashboard" bietet Ihnen einen sofortigen Überblick über Ihre aktuelle Sicherheitslage und zeigt Diagramme zur Hardware- und Software-Volume-Verschlüsselung, zum Anti-Ransomware-Status und zu Cluster-Authentifizierungsmethoden. Das Security Dashboard ist verfügbar als"Vorschau" Besonderheit.



ONTAP Cold Storage zurückgewinnen

Der *Reclaim ONTAP Cold Storage* Insight bietet Daten zur Kaltkapazität, zu potenziellen Kosten-/Stromeinsparungen und empfohlenen Aktionselementen für Volumes auf ONTAP Systemen.



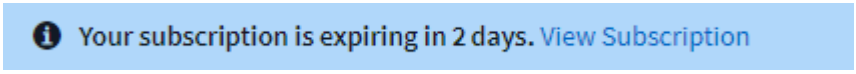
Mit diesem Einblick können Sie Fragen wie die folgenden beantworten:

- Welche Menge an kalten Daten in einem Speichercluster befindet sich auf (a) teuren SSD-Festplatten, (b) HDD-Festplatten und (c) virtuellen Festplatten?
- Welche Workloads tragen im Hinblick auf den nicht optimierten Speicher am meisten dazu bei?
- Wie lange (in Tagen) waren die Daten bei einer bestimmten Arbeitslast kalt?

Reclaim ONTAP Cold Storage gilt als"*Vorschau*" Funktion und kann sich daher ändern.

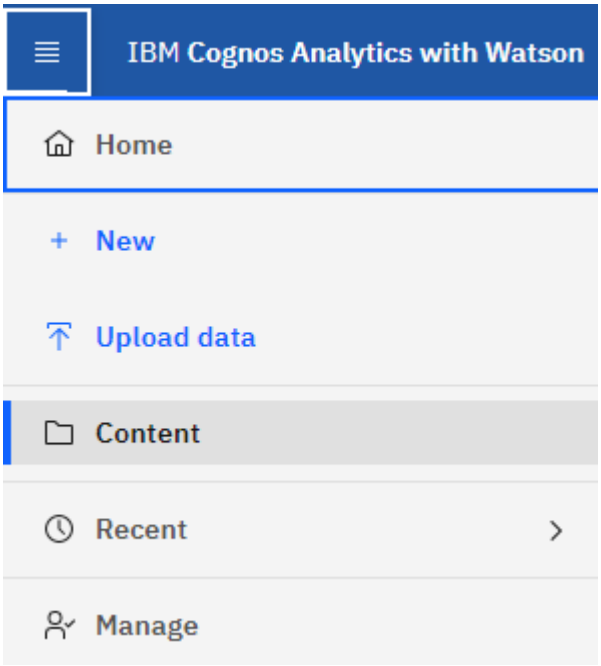
Die Abonnementbenachrichtigung steuert auch Bannernachrichten

Durch das Festlegen von Empfängern für Abonnementbenachrichtigungen (Admin > Benachrichtigungen) wird jetzt auch gesteuert, wer abonnementbezogene Bannerbenachrichtigungen im Produkt sieht.



Reporting im neuen Look

Sie werden feststellen, dass die Bildschirme der Cloud Insights Berichterstellung ein neues Aussehen haben und dass sich einige Teile der Menünavigation geändert haben. Diese Bildschirme und Navigationsänderungen wurden in der aktuellen"Berichtsdokumentation" .



Monitore standardmäßig angehalten

Beachten Sie bei neuen Cloud Insights -Umgebungen, dass"systemdefinierte Monitore" Senden Sie standardmäßig keine Warnbenachrichtigungen. Sie müssen Benachrichtigungen für jeden Monitor aktivieren, der Sie benachrichtigen möchte, indem Sie eine oder mehrere Übermittlungsmethoden für den Monitor hinzufügen. Für vorhandene Cloud Insights -Umgebungen wurde die standardmäßige *globale* Benachrichtigungsempfängerliste für alle systemdefinierten Monitore entfernt, die sich derzeit im Status *Angehalten* befinden. Benutzerdefinierte Benachrichtigungen bleiben unverändert, ebenso wie die Benachrichtigungseinstellungen für derzeit aktive systemdefinierte Monitore.

Suchen Sie nach der Registerkarte „API-Messung“?

Die API-Messung wurde von der Abonnementseite auf die Seite **Admin > API-Zugriff** verschoben.

März 2023

Cloud Connection für ONTAP 9.9+ veraltet

Der Datensammler Cloud Connection für ONTAP 9.9+ wird nicht mehr unterstützt. Ab dem 4. April 2023 erfassen Cloud Connection-Datensammler in Ihrer Umgebung keine Daten mehr und zeigen stattdessen beim Polling einen Fehler an. Der Cloud Connection-Datensammler wird in einem nachfolgenden Update vollständig aus Cloud Insights entfernt.

Vor dem 4. April 2023 muss für alle ONTAP -Systeme, die derzeit von Cloud Connection erfasst werden, ein neuer Datensammler für die NetApp ONTAP Data Management Software konfiguriert werden.

Januar 2023

Neue Protokollmonitore

Wir haben fast zwei Dutzend hinzugefügt"zusätzliche Systemmonitore" um vor unterbrochenen Verbindungsverbindungen, Heartbeat-Problemen und mehr zu warnen. Darüber hinaus wurden drei neue Protokollmonitore für den Datenschutz hinzugefügt, um auf Änderungen bei SnapMirror Auto Resync, MetroCluster Mirroring und FabricPool Mirror Resync hinzuweisen.

Beachten Sie, dass einige dieser Monitore standardmäßig *aktiviert* sind. Sie müssen sie *anhalten*, wenn Sie keine Warnungen erhalten möchten. Beachten Sie auch, dass diese Monitore nicht für die Übermittlung von Benachrichtigungen konfiguriert sind. Sie müssen Benachrichtigungsempfänger auf diesen Monitoren konfigurieren, wenn Sie Warnungen per E-Mail oder Webhook senden möchten.

.CSV-Export für alle Dashboard-Tabellen-Widgets

Die Gewährleistung des Zugriffs auf Ihre Daten ist von entscheidender Bedeutung. Deshalb haben wir den CSV-Export für alle Metrikabfragen, Dashboard-Tabellen-Widgets und Objekt-Landingpages verfügbar gemacht, unabhängig von der Art der Daten (Asset oder Integration), die Sie abfragen.

Datenanpassungen wie Spaltenauswahl, Umbenennen von Spalten und Einheitenumrechnungen sind jetzt auch in der neuen Exportfunktion enthalten.

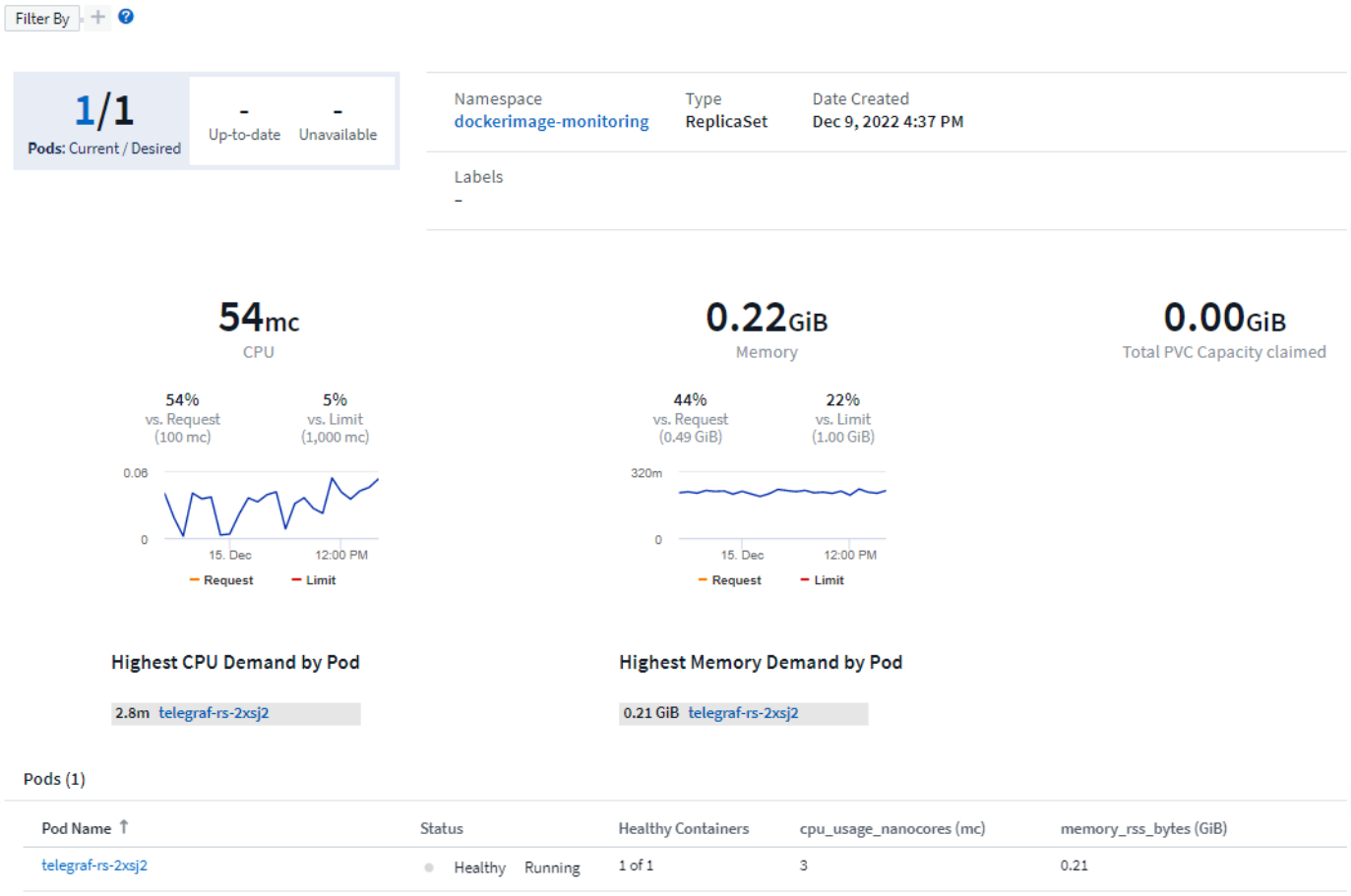
Dezember 2022

Entdecken Sie Ransomware-Schutz und andere Sicherheitsfunktionen während der Cloud Insights -Testversion

Wenn Sie sich ab heute für eine neue Testversion von Cloud Insights anmelden, können Sie Sicherheitsfunktionen wie Ransomware-Erkennung und eine automatische Reaktionsrichtlinie zur Benutzerblockierung erkunden. Wenn Sie sich noch nicht für Ihre Testversion angemeldet haben, tun Sie es noch heute!

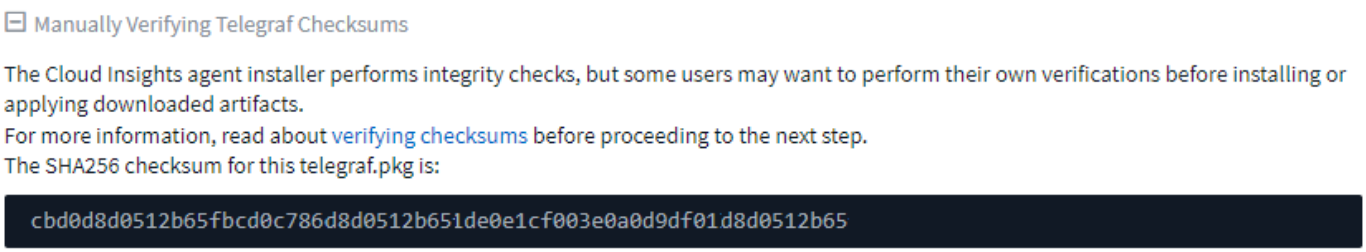
Kubernetes Workloads haben eine eigene Landingpage

Workloads sind ein wichtiger Teil Ihrer Kubernetes-Umgebung, daher bietet Cloud Insights jetzt Zielseiten für diese Workloads. Von hier aus können Sie Probleme anzeigen, untersuchen und beheben, die Ihre Kubernetes-Workloads betreffen.



Überprüfen Sie Ihre Prüfsummen

Sie haben uns gebeten, Ihnen während der Installation des Agenten für Windows und Linux Prüfsummenwerte bereitzustellen, und wir halten das für eine großartige Idee. Hier sind sie:

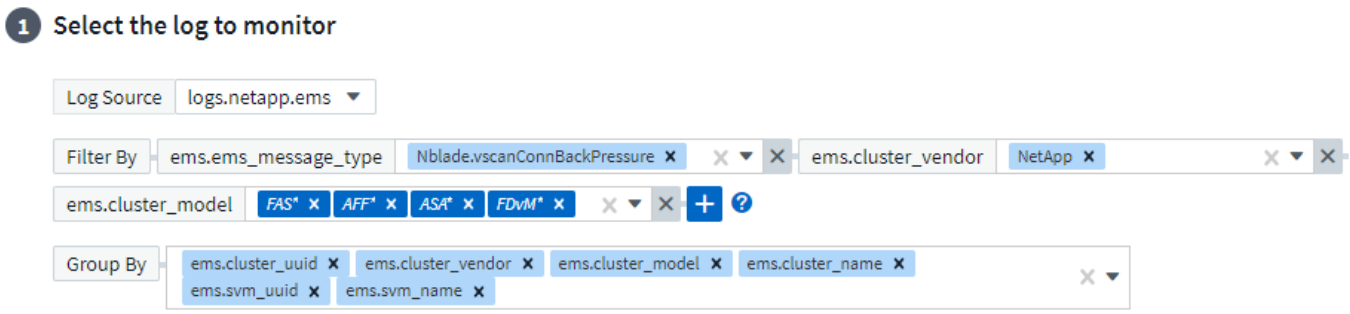


Verbesserungen bei der Protokollwarnung

Gruppieren nach

Beim Erstellen oder Bearbeiten eines Protokollmonitors können Sie jetzt „Gruppieren nach“-Attribute festlegen, um gezieltere Warnmeldungen zu ermöglichen. Suchen Sie in Ihrer Monitordefinition unter den „Filter“-

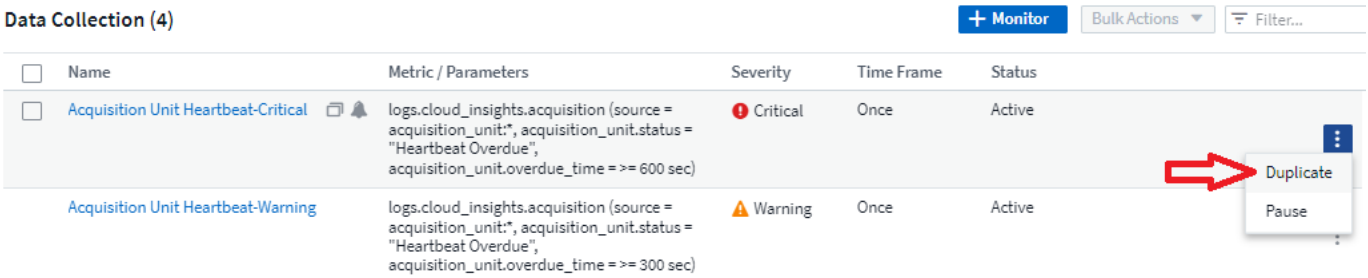
Einstellungen nach den „Gruppieren nach“-Attributen.



Diese Änderung bringt Metrikmonitore und Protokollmonitore in die gleiche Funktion, indem der „Gruppieren nach“-Aspekt von Monitordefinitionen normalisiert wird. Diese Parität ermöglicht es Kunden, **alle** systemdefinierten Standardmonitore zur weiteren Anpassung zu klonen/duplizieren.

Duplizieren

Sie können jetzt die Monitore „Änderungsprotokoll“, „Kubernetes-Protokoll“ und „Datensammlerprotokoll“ klonen (duplizieren). Dadurch wird ein neuer benutzerdefinierter Protokollmonitor erstellt, den Sie an Ihre spezifischen Definitionen anpassen können.



11 neue Standard ONTAP -Monitore für SnapMirror zur Gewährleistung der Geschäftskontinuität

Wir haben fast ein Dutzend neue"Systemmonitore" für SnapMirror for Business Continuity (SMBC), das bei Änderungen an SMBC-Zertifikaten und ONTAP Mediatoren warnt.

November 2022

Mehr als 40 neue Sicherheits-, Datenerfassungs- und CVO-Monitore!

Wir haben Dutzende neuer systemdefinierter Monitore hinzugefügt, um Sie auf potenzielle Probleme mit Cloud Volumes, Sicherheit und Datenschutz aufmerksam zu machen. Lesen Sie mehr über diese Monitore"hier," .

Oktober 2022

Bessere und genauere Ransomware-Erkennung mit der ONTAP Autonomous Ransomware Protection-Integration

Cloud Secure verbessert Ransomware-Erkennung durch Integration mit ONTAP"Autonomer Ransomware-Schutz" (ARP).

Cloud Secure empfängt ONTAP ARP-Ereignisse bei potenzieller Volume-Dateiverschlüsselungsaktivität und

- Korreliert Volume-Verschlüsselungsereignisse mit der Benutzeraktivität, um den Verursacher des Schadens zu identifizieren.
- Implementiert automatische Reaktionsrichtlinien, um den Angriff zu blockieren.
- Identifiziert, welche Dateien betroffen waren, und trägt so zu einer schnelleren Wiederherstellung und zur Durchführung von Untersuchungen zu Datenschutzverletzungen bei.

September 2022

Monitore in der Basic Edition verfügbar

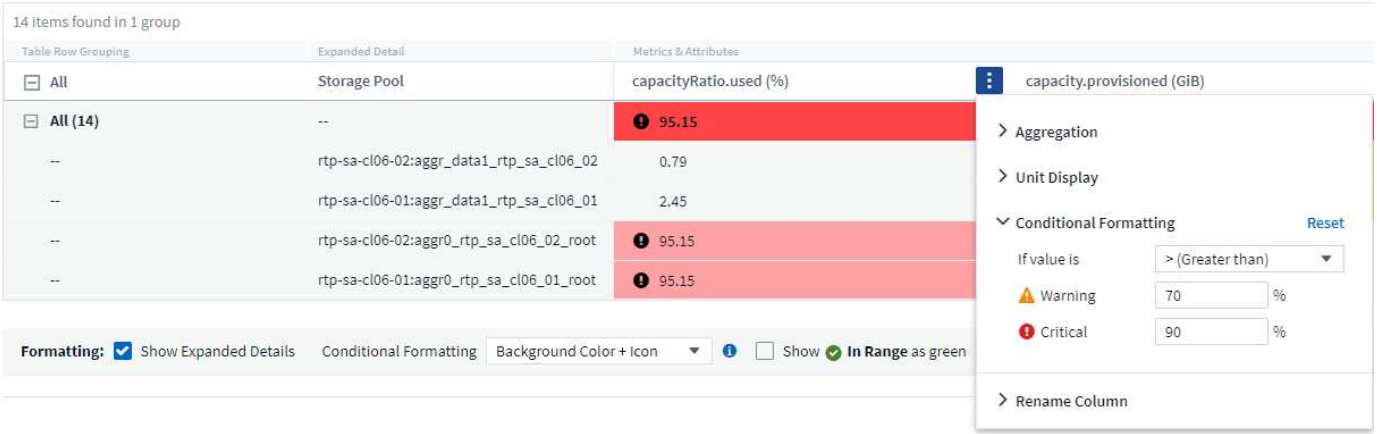
ONTAP"Standardmonitore" jetzt zur Verwendung in der Cloud Insights Basic Edition verfügbar. Dazu gehören mehr als 70 Infrastrukturmonitore und 30 Workload-Beispiele.

ONTAP Power- und StorageGRID Dashboards

Die Dashboard-Galerie enthält ein neues Dashboard für ONTAP Power und Temperature sowie vier Dashboards für StorageGRID. Wenn Ihre Umgebung ONTAP Leistungsmetriken und/oder StorageGRID Daten sammelt, importieren Sie diese Dashboards, indem Sie **+Aus Galerie** auswählen.

Schwellenwertsichtbarkeit in Tabellen auf einen Blick

Mit der bedingten Formatierung können Sie Schwellenwerte für Warn- und kritische Werte in Tabellen-Widgets festlegen und hervorheben, sodass Ausreißer und außergewöhnliche Datenpunkte sofort sichtbar werden.



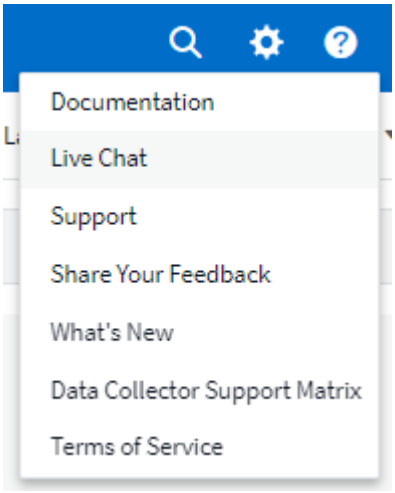
Sicherheitsmonitor

Cloud Insights kann Sie benachrichtigen, wenn es erkennt, dass der FIPS-Modus auf dem ONTAP -System deaktiviert ist. Lesen Sie mehr über"Systemmonitore" , und schauen Sie hier nach weiteren

Sicherheitsmonitoren, die bald verfügbar sind!

Chatten Sie von überall

Chatten Sie von jedem Cloud Insights -Bildschirm aus mit einem NetApp -Support-Spezialisten, indem Sie den neuen Link **Hilfe > Live-Chat** auswählen. Hilfe erhalten Sie über das Symbol „?“ oben rechts auf dem Bildschirm.



Mehr sichtbare Einblicke

Wenn in Ihrer Umgebung ein"Einblick" Bei Problemen wie „Gemeinsam genutzte Ressourcen unter Stress“ oder „Kubernetes-Namespaces haben nicht genügend Speicherplatz“ enthalten die Asset-Landingpages für betroffene Ressourcen jetzt Links zum Insight selbst, sodass eine schnellere Erkundung und Fehlerbehebung möglich ist.

Neue Datensammler

- Amazon S3 (in der Vorschau verfügbar)
- Brocade FOS 9.0.x
- Dell/EMC PowerStore 3.0.0.0

Weitere Updates des Datensammlers

Alle Datenquellen sind jetzt optimiert, um die Leistungsabfrage nach Updates und/oder Patches der Erfassungseinheit wieder aufzunehmen.

Betriebssystemunterstützung

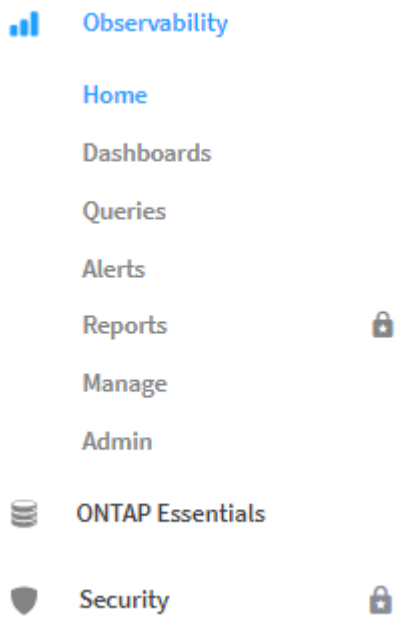
Die folgenden Betriebssysteme werden mit Cloud Insights Acquisition Units unterstützt, zusätzlich zu denen"bereits unterstützt" :

- Red Hat Enterprise Linux 8.5, 8.6

August 2022

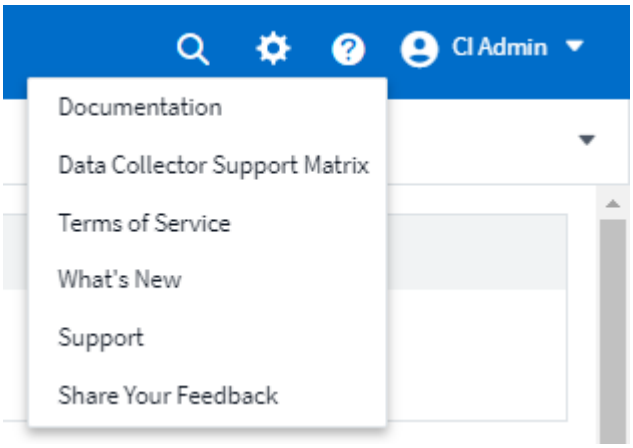
Cloud Insights hat ein neues Aussehen!

Ab diesem Monat wurde „Überwachen und Optimieren“ in **Beobachtbarkeit** umbenannt. Hier finden Sie alle Ihre Lieblingsfunktionen wie Dashboards, Abfragen, Warnungen und Berichte. Suchen Sie außerdem im neuen Menü **Sicherheit** nach Cloud Secure . Beachten Sie, dass sich nur die Menüs geändert haben; die Funktionalität der Funktionen bleibt gleich.



Suchen Sie nach dem **Hilfe**-Menü?

Die Hilfe befindet sich jetzt oben rechts auf dem Bildschirm.

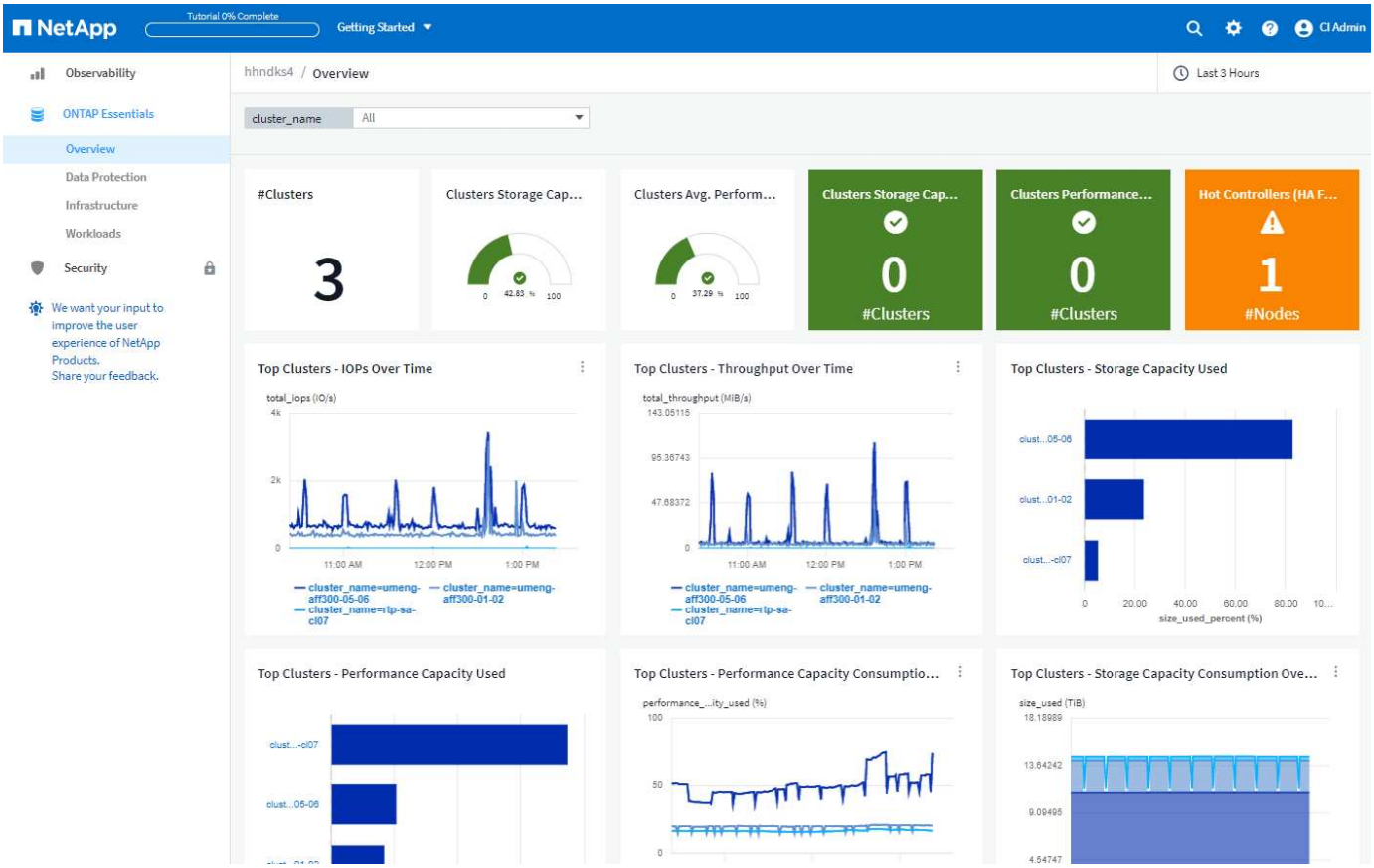


Sie wissen nicht, wo Sie anfangen sollen? Schauen Sie sich ONTAP Essentials an!

"* ONTAP Essentials*"ist eine Reihe von Dashboards und Workflows, die detaillierte Einblicke in Ihre NetApp ONTAP -Bestände, Workloads und Datensicherung bieten, einschließlich Vorhersagen zur Speicherkapazität und Leistung in Tagen bis zur vollständigen Auslastung. Sie können sogar sehen, ob Controller mit hoher Auslastung laufen. ONTAP Essentials ist der ideale Ort für alle Ihre NetApp ONTAP

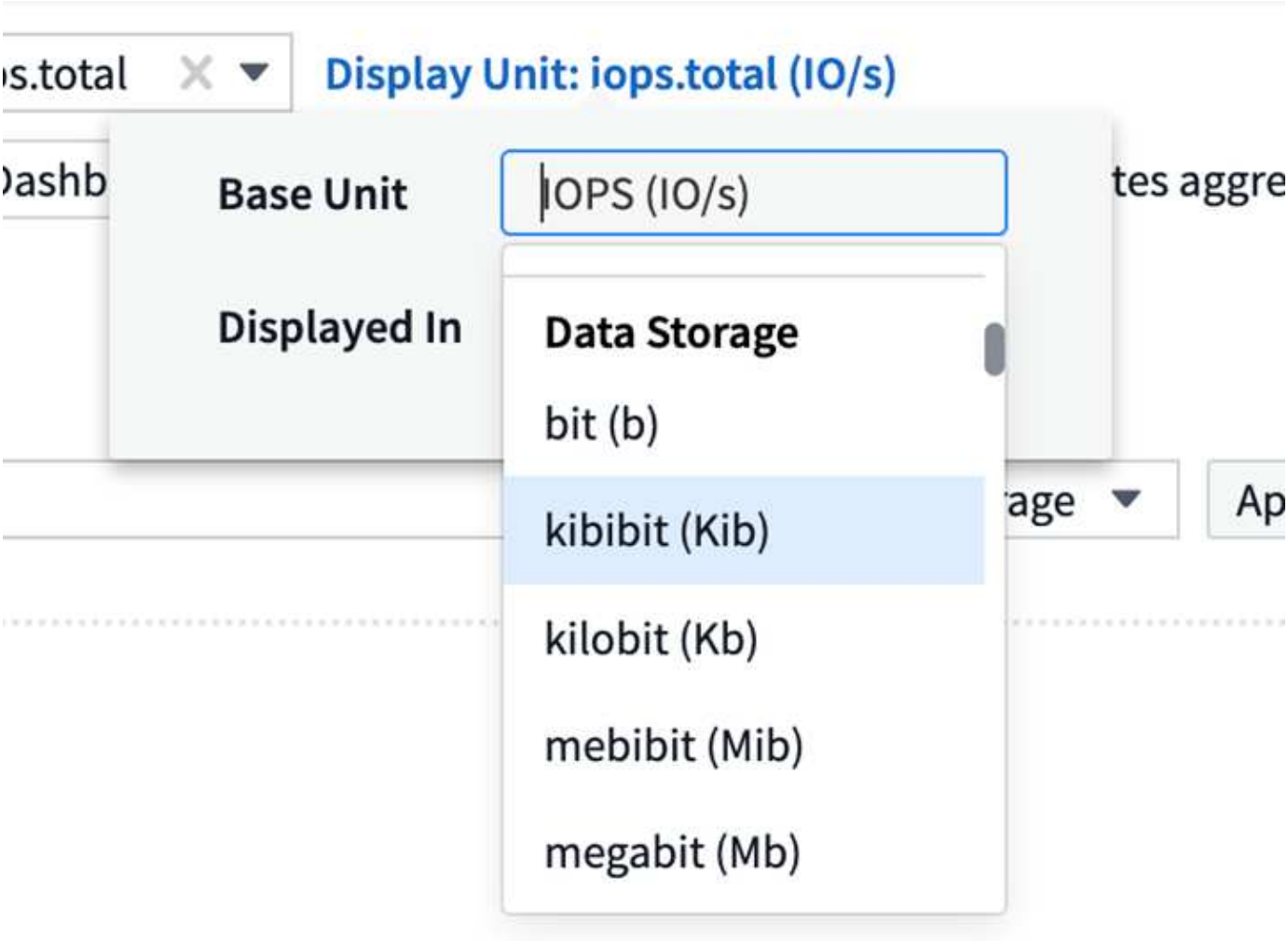
Überwachungsanforderungen!

ONTAP Essentials – in allen Editionen verfügbar – ist für bestehende ONTAP Betreiber und -Administratoren intuitiv zu bedienen und erleichtert den Übergang vom ActiveIQ Unified Manager zu servicebasierten Verwaltungstools.



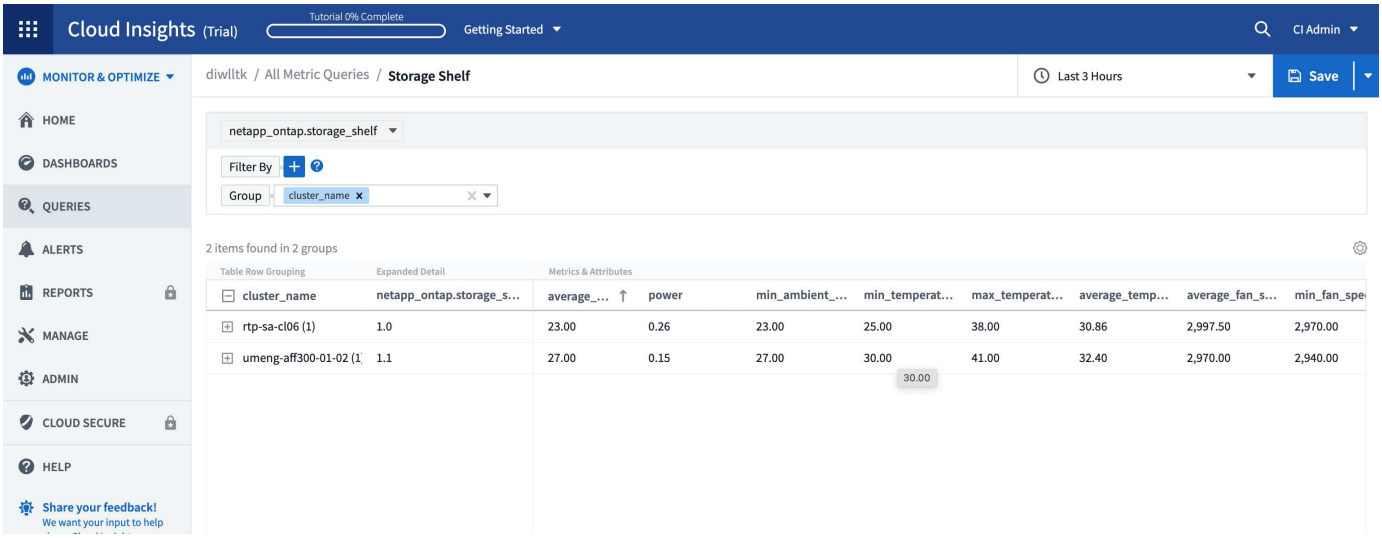
Speicherdatenfamilien werden zusammengeführt

Sie haben danach gefragt und jetzt haben Sie es. Speicherdateneinheiten zur Basis 2 und Basis 10 werden jetzt in einer Familie zusammengefasst, von Bits und Bytes bis hin zu Tebibits und Terabytes, wodurch die Anzeige von Daten auf Ihren Dashboards einfacher wird. Auch die Datenraten sind mittlerweile eine eigene große Familie.



Wie viel Strom verbraucht mein Speicher?

Zeigen Sie den Stromverbrauch, die Temperatur und die Lüftergeschwindigkeit Ihres ONTAP Speicherregals und -Knotens an und überwachen Sie ihn mithilfe der Metriken netapp_ontap.storage_shelf, netapp_ontap.system_node und netapp_ontap.cluster (nur Stromverbrauch).



Aus der Vorschau entfernte Funktionen

Die folgenden Funktionen wurden aus der Vorschau entfernt und stehen jetzt allen Kunden zur Verfügung:

Besonderheit	Beschreibung
Kubernetes-Namespaces haben nicht mehr genügend Speicherplatz	Der Einblick „Kubernetes-Namespaces haben keinen Speicherplatz mehr“ bietet Ihnen einen Überblick über die Workloads in Ihren Kubernetes-Namespaces, bei denen das Risiko besteht, dass der Speicherplatz knapp wird, und enthält eine Schätzung der verbleibenden Tage, bis jeder Speicherplatz voll ist."Mehr lesen"
Gemeinsam genutzte Ressource unter Stress	Die Einblicke in „Shared Resource Under Stress“ nutzen KI/ML, um automatisch zu erkennen, wo Ressourcenkonflikte zu Leistungseinbußen in Ihrer Umgebung führen, alle davon betroffenen Workloads hervorzuheben und Maßnahmen zur Behebung zu empfehlen, sodass Sie Leistungsprobleme schneller lösen können."Mehr lesen"
Cloud Secure – Benutzerzugriff bei Angriffen blockieren	Besserer Schutz Ihrer geschäftskritischen Daten durch die Möglichkeit, den Benutzerzugriff zu blockieren, wenn ein Angriff erkannt wird. Der Zugriff kann automatisch mithilfe automatisierter Antwortrichtlinien oder manuell über die Warn- oder Benutzerdetailseiten blockiert werden."Mehr lesen"

Wie steht es um die Gesundheit meiner Datenerfassung?

Cloud Insights bietet zwei neue Heartbeat-Monitore für Ihre Erfassungseinheiten sowie zwei Monitore, die Sie auf Fehler beim Datensammler aufmerksam machen. Diese können verwendet werden, um Sie schnell auf Probleme bei der Datenerfassung aufmerksam zu machen.

Die folgenden Monitore sind jetzt in der Monitorgruppe *Datenerfassung* verfügbar:

- Herzschlag der Erfassungseinheit – kritisch
- Heartbeat-Warnung der Erfassungseinheit
- Collector fehlgeschlagen
- Sammlerwarnung

Beachten Sie, dass sich diese Monitore standardmäßig im Status *Pausiert* befinden. Aktivieren Sie sie, um über Probleme bei der Datenerfassung benachrichtigt zu werden.

Automatisch erneuernde API-Token

API-Zugriffstoken können jetzt für die automatische Verlängerung eingestellt werden. Durch Aktivieren dieser Funktion werden für ablaufende Token automatisch neue/aktualisierte API-Zugriffstoken generiert. Cloud Insights Agenten, die ein ablaufendes Token verwenden, werden automatisch aktualisiert, um das entsprechende neue/aktualisierte API-Zugriffstoken zu verwenden, sodass sie weiterhin nahtlos funktionieren können. Aktivieren Sie beim Erstellen Ihres Tokens einfach das Kontrollkästchen „Token automatisch erneuern“. Diese Funktion wird derzeit auf Cloud Insights -Agenten unterstützt, die auf der Kubernetes-Plattform mit dem neuesten NetApp Kubernetes Monitoring Operator ausgeführt werden.

Die Basic Edition bietet Ihnen mehr als je zuvor

Ihre Testphase läuft ab, aber Sie sind sich noch nicht sicher, ob ein Abonnement das Richtige für Sie ist? Mit der Basic Edition hatten Sie schon immer die Möglichkeit, Cloud Insights weiterhin mit Ihrem aktuellen ONTAP Datensammler zu verwenden. Jetzt können Sie jedoch auch weiterhin VMWare-Versions-, Topologie- und IOPS-/Durchsatz-/Latenzdaten erfassen. NetApp -Kunden mit Premium-Support für ihre Speichersysteme haben auch Anspruch auf Support für Cloud Insights.

Möchten Sie mehr erfahren?

Im Abschnitt **Learning Center** auf der Seite „Hilfe > Support“ finden Sie Links zu den Kursangeboten von NetApp University Cloud Insights !

Betriebssystemunterstützung

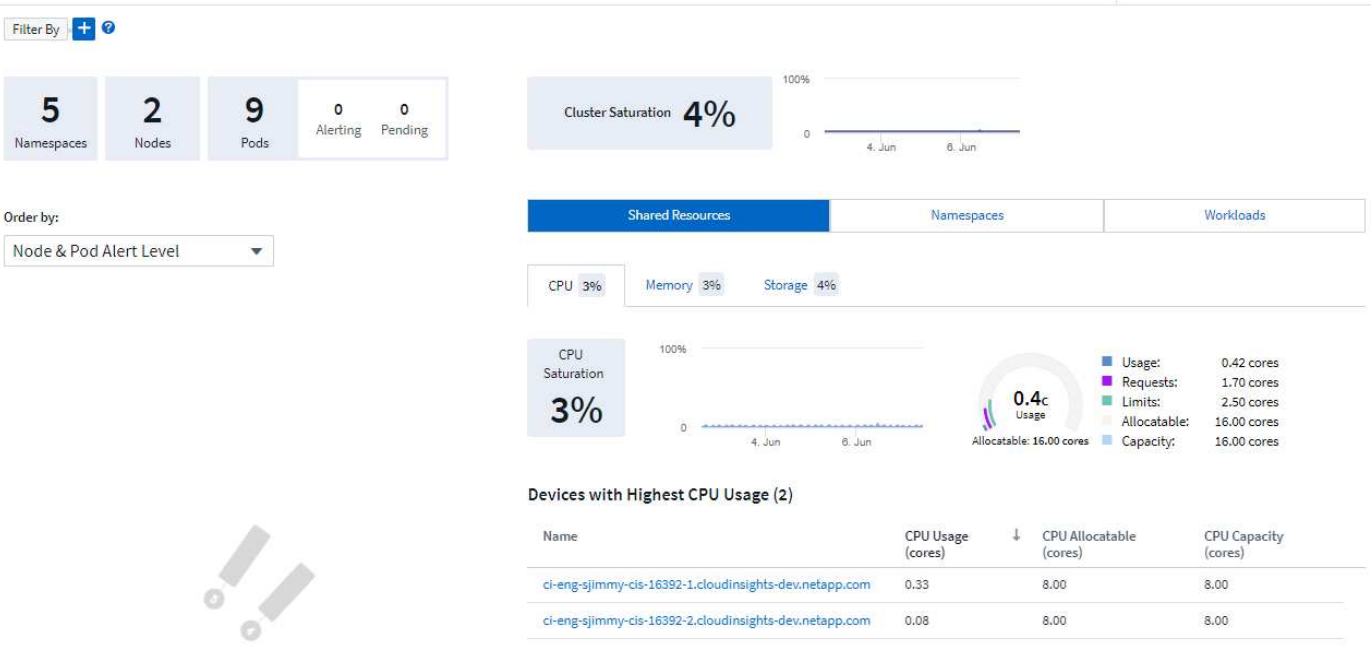
Das folgende Betriebssystem wird mit Cloud Insights Acquisition Units unterstützt, zusätzlich zu denen"bereits unterstützt" :

- Windows 11

Juni 2022

Kubernetes-Clustersättigung und andere Details

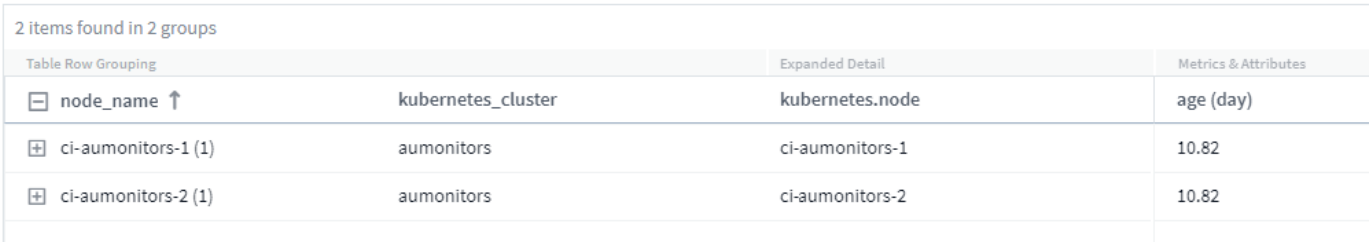
Mit Cloud Insights können Sie Ihre Kubernetes-Umgebung einfacher denn je erkunden. Die verbesserte Cluster-Detailseite bietet Sättigungsdetails sowie eine übersichtlichere Ansicht von Namespaces und Workloads.



Auf der Clusterlistenseite erhalten Sie neben der Anzahl der Knoten, Pods, Namespaces und Workloads auch einen schnellen Überblick über die Sättigung:

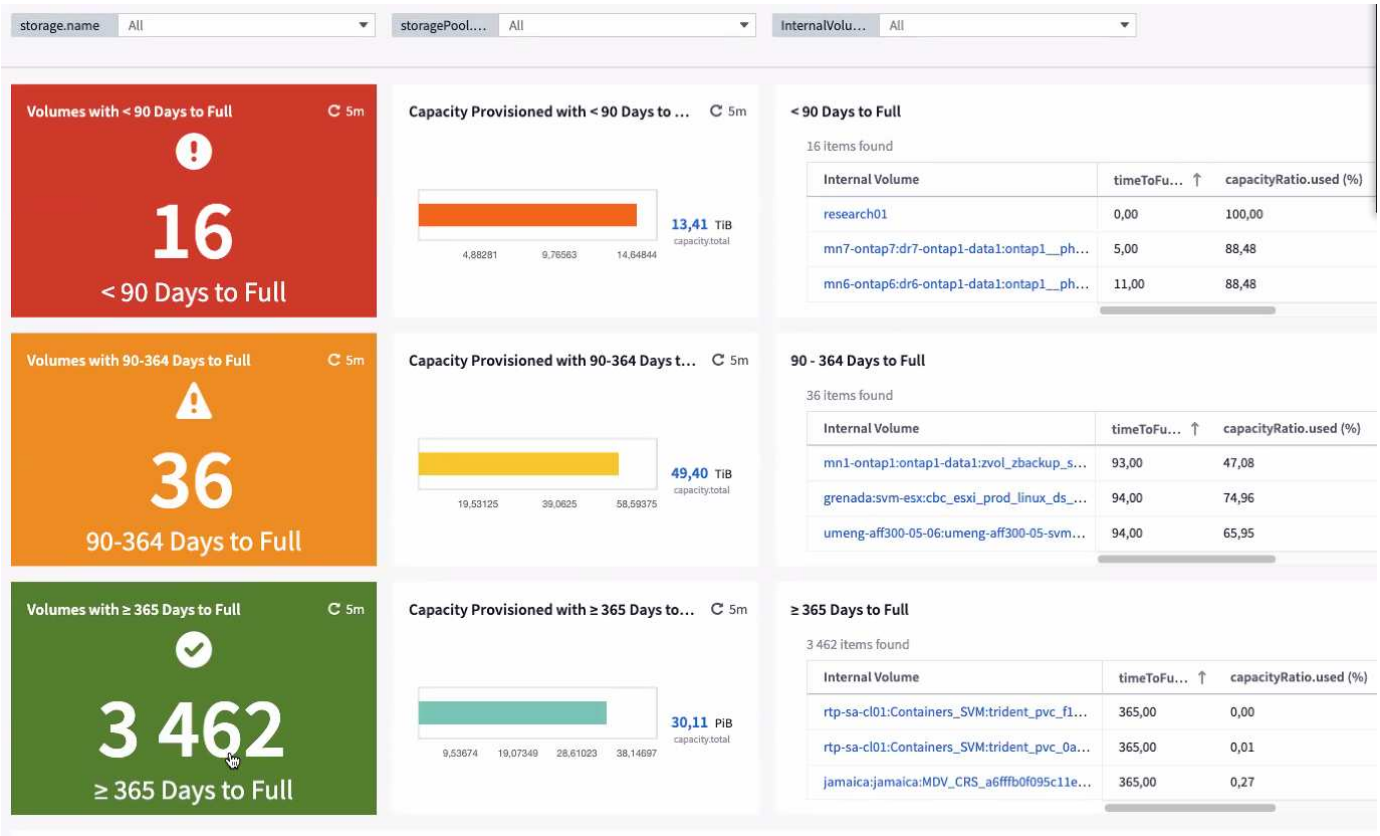
Wie alt ist Ihr Kubernetes-Cluster?

Steht Ihr Cluster noch ganz am Anfang seiner Entwicklung oder hat er bereits ein langes digitales Leben hinter sich? *Alter* wurde als für Kubernetes-Knoten erfasste Zeitmetrik hinzugefügt.



Kapazitätsprognose bis zur vollständigen Auslastung

Cloud Insights bietet ein Dashboard zur Prognose der Anzahl der Tage bis zur Kapazitätserschöpfung für jedes überwachte interne Volume. Diese Werte können dazu beitragen, das Ausfallrisiko deutlich zu reduzieren.

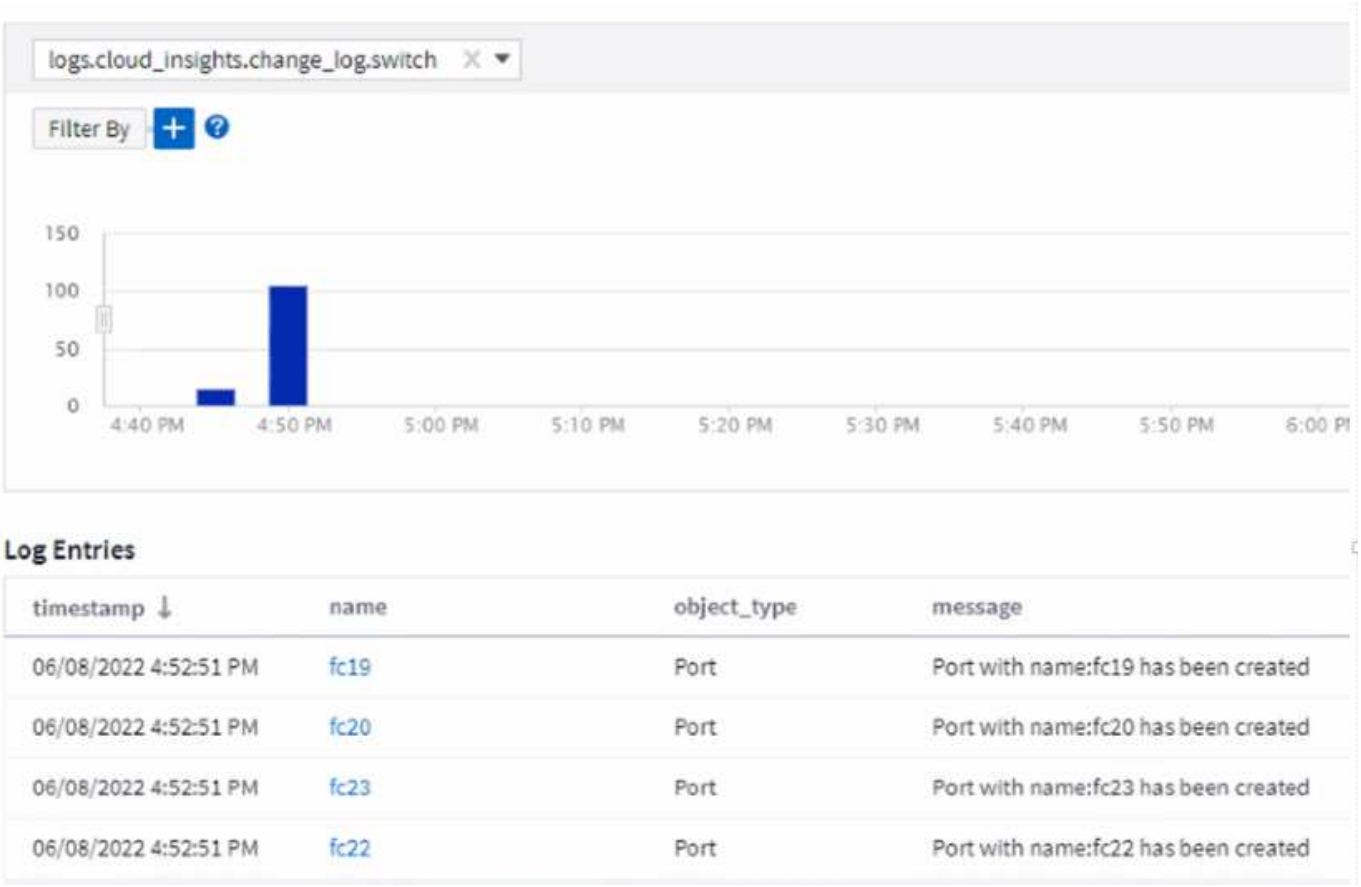


TTF-Zähler sind auch für Speicher, Speicherpool und Volume verfügbar. Behalten Sie diesen Bereich im Auge, um weitere Dashboards für diese Objekte zu erhalten.

Beachten Sie, dass die Time-to-Full-Prognose aus der *Vorschau*-Phase herausgenommen und für alle Kunden eingeführt wird.

Was hat sich in meiner Umgebung geändert?

ONTAP Änderungsprotokolleinträge können im Protokoll-Explorer angezeigt werden.



Betriebssystemunterstützung

Die folgenden Betriebssysteme werden mit Cloud Insights Acquisition Units unterstützt, zusätzlich zu denen"bereits unterstützt" :

- CentOS Stream 9
- Windows 2022

Aktualisierter Telegraf-Agent

Der Agent für die Aufnahme von Telegraf-Integrationsdaten wurde auf Version **1.22.3** aktualisiert und bietet Leistungs- und Sicherheitsverbesserungen. Benutzer, die ein Update durchführen möchten, können sich auf den entsprechenden Upgrade-Abschnitt der"Agent-Installation" Dokumentation. Frühere Versionen des Agenten funktionieren weiterhin, ohne dass ein Eingreifen des Benutzers erforderlich ist.

Vorschaufunktionen

Cloud Insights hebt regelmäßig eine Reihe spannender neuer Vorschaufunktionen hervor. Wenn Sie an einer Vorschau einer oder mehrerer dieser Funktionen interessiert sind, wenden Sie sich an Ihren"NetApp

Vertriebsteam" für weitere Informationen.

Besonderheit	Beschreibung
Kubernetes-Namespaces haben nicht mehr genügend Speicherplatz	Der Einblick „Kubernetes-Namespaces haben keinen Speicherplatz mehr“ bietet Ihnen einen Überblick über die Workloads in Ihren Kubernetes-Namespaces, bei denen das Risiko besteht, dass der Speicherplatz knapp wird, und enthält eine Schätzung der verbleibenden Tage, bis jeder Speicherplatz voll ist."Mehr lesen"
Cloud Secure – Benutzerzugriff bei Angriffen blockieren	Besserer Schutz Ihrer geschäftskritischen Daten durch die Möglichkeit, den Benutzerzugriff zu blockieren, wenn ein Angriff erkannt wird. Der Zugriff kann automatisch mithilfe automatisierter Antwortrichtlinien oder manuell über die Warn- oder Benutzerdetailseiten blockiert werden."Mehr lesen"
Gemeinsam genutzte Ressource unter Stress	Die Einblicke in „Shared Resource Under Stress“ nutzen KI/ML, um automatisch zu erkennen, wo Ressourcenkonflikte zu Leistungseinbußen in Ihrer Umgebung führen, alle davon betroffenen Workloads hervorzuheben und Maßnahmen zur Behebung zu empfehlen, sodass Sie Leistungsprobleme schneller lösen können."Mehr lesen"

Mai 2022

Chatten Sie live mit dem NetApp Support

Sie können jetzt live mit dem Support-Personal von NetApp chatten! Klicken Sie auf der Seite „Hilfe“ > „Support“ einfach auf das Chat-Symbol oder im Abschnitt „Kontakt“ auf „Chat“, um eine Chat-Sitzung zu starten. Für Benutzer der Standard- und Premium-Edition ist Chat-Support an US-Wochentagen verfügbar.

Kubernetes-Operator

Wir haben Ihnen den Einstieg mit der erweiterten Kubernetes-Überwachung und dem Cluster-Explorer von Cloud Insights erleichtert.

Der"Kubernetes-Überwachungsoperator" (NKMO) ist die bevorzugte Methode zum Installieren von Kubernetes für Cloud Insights Insights, für eine flexiblere Konfiguration der Überwachung in weniger Schritten sowie erweiterte Möglichkeiten zum Überwachen anderer im K8s-Cluster ausgeführter Software.

Klicken Sie auf den Link oben, um weitere Informationen und Voraussetzungen zu erhalten

Verwalten Sie Benutzer und Einladungen mit der API

Sie können jetzt Benutzer und Einladungen mithilfe der leistungsstarken API von Cloud Insights verwalten. Lesen Sie mehr im"API Swagger-Dokumentation" .

Datenerfassungswarnungen

Verpassen Sie keine wichtigen Messdaten aufgrund eines ausgefallenen Collectors!

Es ist einfacher denn je, den Überblick über Ihre Datensammler zu behalten mit neuen"Warnungen" für Ausfälle von Datensammlern und Erfassungseinheiten. Beachten Sie, dass diese Monitore standardmäßig *angehalten* sind. Um die Funktion zu aktivieren, navigieren Sie zu Ihrer Monitorseite und suchen und setzen Sie „Acquisition Unit Shutdown“ und „Collector Failed“ fort.

Warnmeldung zu Änderungen am ONTAP -Speicher

Lassen Sie nicht zu, dass unerwartete Speicheränderungen zu Ausfällen führen!

Sie können Cloud Insights jetzt so konfigurieren, dass eine Warnung ausgegeben wird, wenn auf ONTAP -Systemen Änderungen oder Entfernungen von FlexVols, Knoten und SVMs erkannt werden.

Vorschaufunktionen

Cloud Insights hebt regelmäßig eine Reihe spannender neuer Vorschaufunktionen hervor. Wenn Sie an einer Vorschau einer oder mehrerer dieser Funktionen interessiert sind, wenden Sie sich an Ihren"NetApp Vertriebsteam" für weitere Informationen.

Besonderheit	Beschreibung
Kubernetes-Namespaces haben nicht mehr genügend Speicherplatz	Der Einblick „Kubernetes-Namespaces haben keinen Speicherplatz mehr“ bietet Ihnen einen Überblick über die Workloads in Ihren Kubernetes-Namespaces, bei denen das Risiko besteht, dass der Speicherplatz knapp wird, und enthält eine Schätzung der verbleibenden Tage, bis jeder Speicherplatz voll ist."Mehr lesen"
Prognose der Zeit bis zur vollständigen Befüllung des internen Volumens und der Volumenkapazität	Cloud Insights kann für jedes überwachte interne Volume und Volume die Anzahl der Tage bis zur Kapazitätserschöpfung prognostizieren. Dieser Wert kann dazu beitragen, das Ausfallrisiko deutlich zu reduzieren.
Cloud Secure – Benutzerzugriff bei Angriffen blockieren	Besserer Schutz Ihrer geschäftskritischen Daten durch die Möglichkeit, den Benutzerzugriff zu blockieren, wenn ein Angriff erkannt wird. Der Zugriff kann automatisch mithilfe automatisierter Antwortrichtlinien oder manuell über die Warn- oder Benutzerdetailseiten blockiert werden."Mehr lesen"

Gemeinsam genutzte Ressource unter Stress	Die Einblicke in „Shared Resource Under Stress“ nutzen KI/ML, um automatisch zu erkennen, wo Ressourcenkonflikte zu Leistungseinbußen in Ihrer Umgebung führen, alle davon betroffenen Workloads hervorzuheben und Maßnahmen zur Behebung zu empfehlen, sodass Sie Leistungsprobleme schneller lösen können."Mehr lesen"

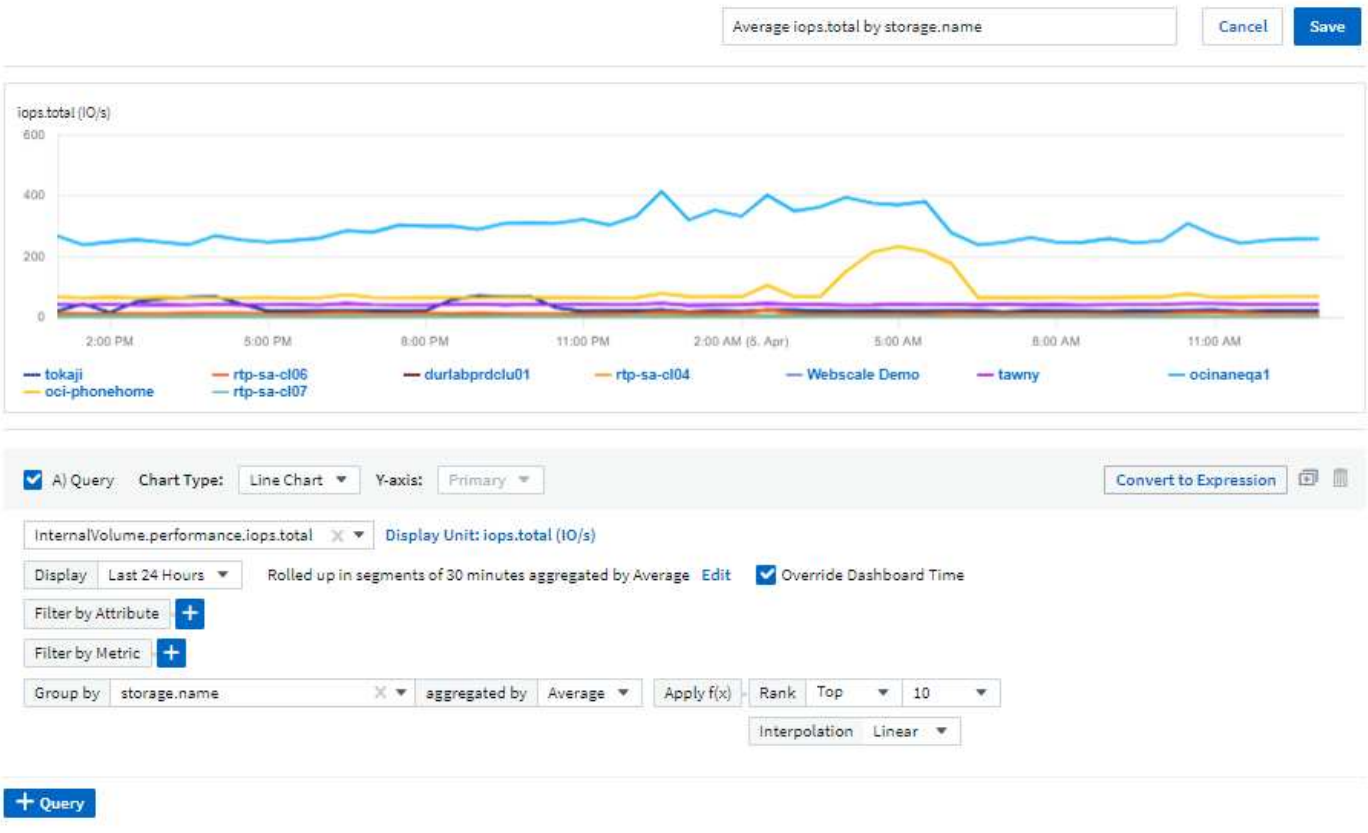
April 2022

Teile dein Feedback!

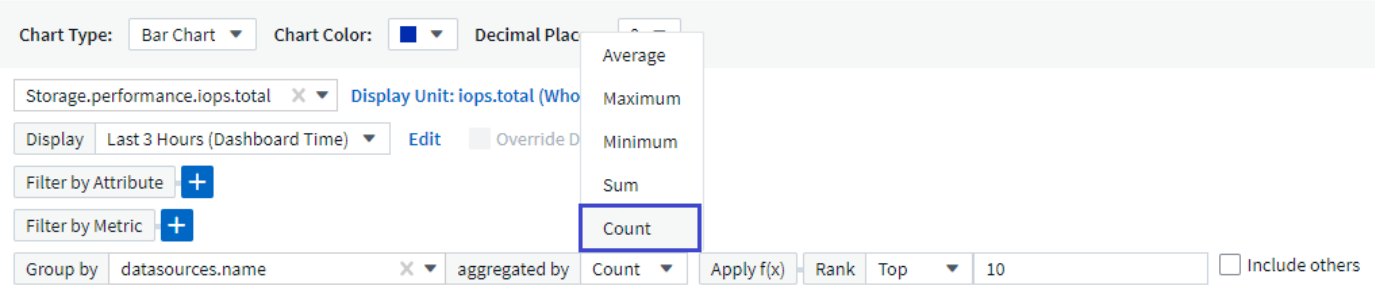
Wir möchten, dass Ihr Input dazu beiträgt, Cloud Insights zu gestalten. Sammeln Sie Punkte und Preise, indem Sie am **Insights to Action**-Programm von NetApp teilnehmen. **"Jetzt anmelden"** !

Aktualisierter Dashboard-Editor

Wir haben unsere Tools zur Dashboard-Erstellung überarbeitet, damit Sie Ihre Daten noch schneller visualisieren können. Navigieren Sie zur Seite „Dashboards“ von Cloud Insights, um ein vorhandenes Dashboard zu bearbeiten, eines aus unserer Dashboard-Galerie hinzuzufügen oder ein eigenes neues Dashboard zu erstellen, um es auszuprobieren.



Außerdem wurde eine neue Count-Aggregationsmethode eingeführt. Beim Gruppieren von Daten in Balkendiagramm-, Säulendiagramm- und Kreisdiagramm-Widgets können Sie schnell und einfach die Anzahl der relevanten Objekte für die ausgewählte Metrik anzeigen.



Darüber hinaus können Sie bei Liniendiagrammen jetzt eine von drei Optionen auswählen"Interpolation" Methoden:

- Keine - Es wird keine Interpolation durchgeführt
- Linear – Interpoliert einen Datenpunkt zwischen den vorhandenen Punkten
- Treppe – Verwendet den vorherigen Datenpunkt als interpolierten Datenpunkt

Verbesserte Überwachung Ihrer Kubernetes-Infrastruktur

Cloud Insights hält Sie über Änderungen in Ihrer Kubernetes-Umgebung auf dem Laufenden, indem es Sie benachrichtigt, wenn Pods, Daemonsets und Replikatsets erstellt oder entfernt werden, sowie wenn neue Bereitstellungen erstellt werden. Kubernetes-Monitore befinden sich standardmäßig im Zustand „angehalten“, Sie sollten daher nur die Monitore aktivieren, die Sie benötigen.

Vorschaufunktionen

Cloud Insights hebt regelmäßig eine Reihe spannender neuer Vorschaufunktionen hervor. Wenn Sie an einer Vorschau einer oder mehrerer dieser Funktionen interessiert sind, wenden Sie sich an Ihren"NetApp Vertriebsteam" für weitere Informationen.

Besonderheit	Beschreibung
Prognose der Zeit bis zur vollständigen Befüllung des internen Volumens und der Volumenkapazität	Cloud Insights kann für jedes überwachte interne Volume und Volume die Anzahl der Tage bis zur Kapazitätserschöpfung prognostizieren. Dieser Wert kann dazu beitragen, das Ausfallrisiko deutlich zu reduzieren.
Cloud Secure – Benutzerzugriff bei Angriffen blockieren	Besserer Schutz Ihrer geschäftskritischen Daten durch die Möglichkeit, den Benutzerzugriff zu blockieren, wenn ein Angriff erkannt wird. Der Zugriff kann automatisch mithilfe automatisierter Antwortrichtlinien oder manuell über die Warn- oder Benutzerdetailseiten blockiert werden."Mehr lesen"
Gemeinsam genutzte Ressource unter Stress	Die Einblicke in „Shared Resource Under Stress“ nutzen KI/ML, um automatisch zu erkennen, wo Ressourcenkonflikte zu Leistungseinbußen in Ihrer Umgebung führen, alle davon betroffenen Workloads hervorzuheben und Maßnahmen zur Behebung zu empfehlen, sodass Sie Leistungsprobleme schneller lösen können."Mehr lesen"

Neuer Datensammler

- **Cohesity SmartFiles** – Dieser auf REST-API basierende Collector erwirbt einen Cohesity-Cluster, erkennt die „Ansichten“ (als interne CI-Volumes) und die verschiedenen Knoten und sammelt Leistungsmetriken.

Weitere Updates des Datensammlers

Die Erfassung und Anzeige von Leistungsdaten wurde bei den folgenden Datensammlern verbessert:

- Brocade -CLI
- Dell/EMC VPlex, PowerStore, Isilon/PowerScale, VNX Block/Clariion CLI, XtremIO, Unity/VNXe
- Reines FlashArray

Diese Leistungsverbesserungen sind bereits in allen NetApp Datenkollektoren sowie VMware und Cisco verfügbar und werden in den nächsten Monaten auf alle anderen Datenkollektoren ausgeweitet.

März 2022

Cloud-Verbindung für ONTAP 9.9+

Der"NetApp Cloud Connection für ONTAP 9.9+" Der Datensammler macht die Installation einer externen Erfassungseinheit überflüssig und vereinfacht so die Fehlerbehebung, Wartung und Erstbereitstellung.

Neue FSx für NetApp ONTAP -Monitore

Die Überwachung Ihrer FSx für NetApp ONTAP -Umgebung ist einfach mit neuen"systemdefinierte Monitore" sowohl für die Infrastruktur (Metriken) als auch für die Arbeitslasten (Protokolle).

FSX Infrastructure (1) + Monitor | Bulk Actions | Filter...

Name	Metric / Parameters	Severity	Time Frame	Status
FSx Volume Cache Miss Ratio	netapp_ontap.workload_volume.cache_miss_ratio	Warning @ > 95 % Critical @ > 100 %	For 30 minutes	Paused

FSX Workload Examples (5) + Monitor | Bulk Actions | Filter...

Name	Metric / Parameters	Severity	Time Frame	Status
FSx Snapshot Reserve Space is Full	netapp_ontap.workload_volume.snapshot_size_used_percent	Warning @ > 90 % Critical @ > 95 %	Once	Paused
FSx Volume Capacity is Full	netapp_ontap.workload_volume.size_used_percent	Warning @ > 85 % Critical @ > 95 %	Once	Paused
FSx Volume High Latency	netapp_ontap.workload_volume.total_latency	Warning @ > 1,000 µs Critical @ > 2,000 µs	For 5 minutes	Paused
FSx Volume Inodes Limit	netapp_ontap.workload_volume.inodes_used_percent	Warning @ > 85 % Critical @ > 95 %	Once	Paused
FSx Volume Qtree Quota Overcommit	netapp_ontap.workload_volume.qtree_quota_commit_percent	Warning @ > 95 % Critical @ > 100 %	Once	Paused

Neue Cloud Secure -Funktionen für alle verfügbar

Ihre Umgebung ist mit den folgenden, jetzt allgemein verfügbaren Cloud Secure -Funktionen sicherer als je zuvor:

Besonderheit	Beschreibung
Datenvernichtung – Erkennung von Angriffen durch Dateilöschung	Erkennen Sie ungewöhnliche Aktivitäten beim Löschen von Dateien in großem Umfang, blockieren Sie den böswilligen Dateizugriff böswilliger Benutzer und erstellen Sie automatische Snapshots mit automatischen Reaktionsrichtlinien.
Separate Benachrichtigungen für Warnungen und Alarme	Warn- und Alarmbenachrichtigungen können an verschiedene Empfänger gesendet werden, um sicherzustellen, dass das richtige Team informiert bleibt.

Aktualisierter Telegraf-Agent

Der Agent für die Aufnahme von Telegraf-Integrationsdaten wurde auf Version **1.21.2** aktualisiert und bietet Leistungs- und Sicherheitsverbesserungen. Benutzer, die ein Update durchführen möchten, können sich auf den entsprechenden Upgrade-Abschnitt der"Agent-Installation" Dokumentation. Frühere Versionen des Agenten funktionieren weiterhin, ohne dass ein Eingreifen des Benutzers erforderlich ist.

Datensammler-Updates

- Der Datensammler der Broadcom Fibre Channel Switches wurde optimiert, um die Anzahl der bei jeder Bestandsabfrage ausgegebenen CLI-Befehle zu reduzieren.

Februar 2022

Cloud Insights behebt Apache Log4j-Schwachstellen

Die Sicherheit der Kunden hat bei NetApp höchste Priorität. Cloud Insights enthält Updates für seine Softwarebibliotheken, um die jüngsten Apache Log4j-Sicherheitslücken zu beheben.

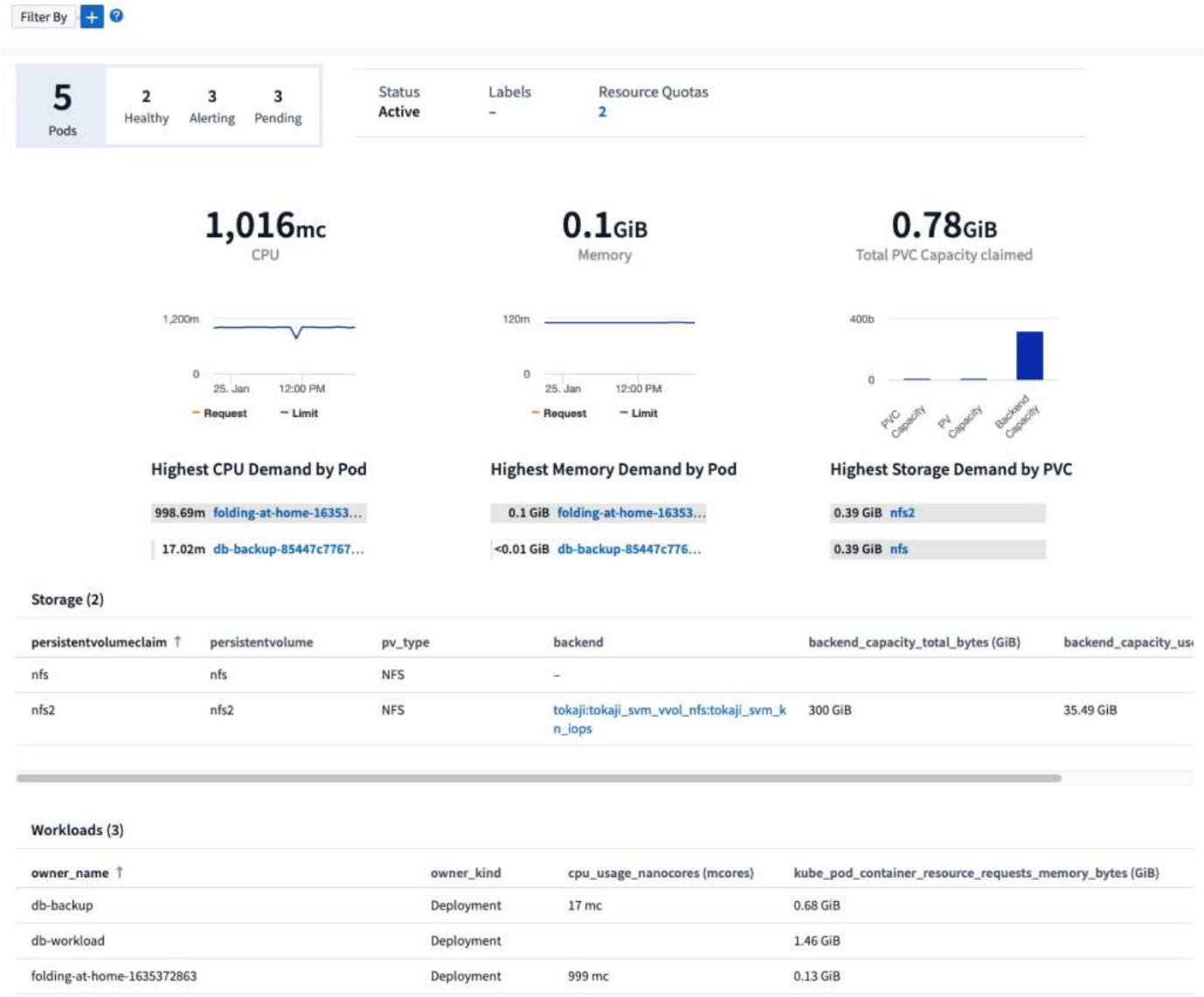
Bitte beachten Sie Folgendes auf der Product Security Advisory-Website von NetApp:

"CVE-2021-44228" "CVE-2021-45046" "CVE-2021-45105"

Weitere Informationen zu diesen Sicherheitslücken und zur Reaktion von NetApp finden Sie unter"NetApp Newsroom" .

Kubernetes-Namespace-Detailseite

Das Erkunden Ihrer Kubernetes-Umgebung ist jetzt besser als je zuvor, mit informativen Detailseiten für die Namespaces Ihres Clusters. Die Namespace-Detailseite bietet eine Zusammenfassung aller von einem Namespace verwendeten Assets, einschließlich aller Back-End-Speicherressourcen und ihrer Kapazitätsauslastung.



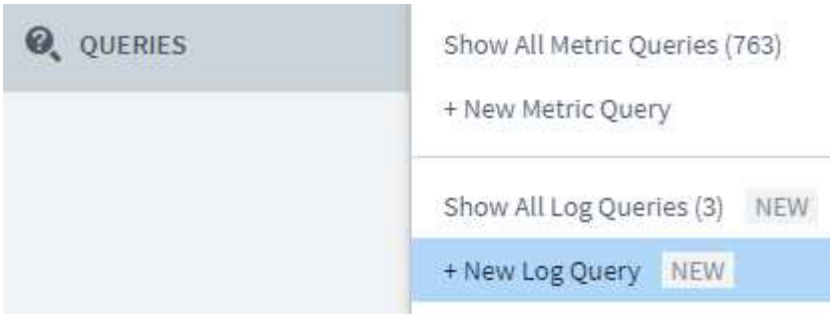
Dezember 2021

Tiefere Integration für ONTAP -Systeme

Vereinfachen Sie die Warnmeldung bei ONTAP Hardwarefehlern und mehr durch die neue Integration mit dem NetApp Event Management System (EMS). "Erkunden und alarmieren" auf Low-Level ONTAP -Nachrichten in Cloud Insights, um Fehlerbehebungs-Workflows zu informieren und zu verbessern und die Abhängigkeit von ONTAP Elementverwaltungstools weiter zu reduzieren.

Abfragen von Protokollen

Für ONTAP -Systeme umfassen Cloud Insights Queries eine leistungsstarke"Protokoll-Explorer" , sodass Sie EMS-Protokolleinträge einfach untersuchen und Fehler beheben können.



Benachrichtigungen auf Datensammlerebene.

Zusätzlich zu den systemdefinierten und benutzerdefinierten Monitoren für Warnmeldungen können Sie auch Warnbenachrichtigungen für ONTAP Datenkollektoren festlegen. So können Sie Empfänger für Warnmeldungen auf Kollektorebene angeben, unabhängig von anderen Monitorwarnungen.

Größere Flexibilität der Cloud Secure -Rollen

Benutzern kann der Zugriff auf Cloud Secure -Funktionen gewährt werden, basierend auf"Rollen" von einem Administrator festgelegt:

Rolle	Cloud Secure Zugriff
Administrator	Kann alle Cloud Secure -Funktionen ausführen, einschließlich der Funktionen für Warnungen, Forensik, Datensammler, Richtlinien für automatisierte Antworten und APIs für Cloud Secure. Ein Administrator kann auch andere Benutzer einladen, aber nur Cloud Secure -Rollen zuweisen.
Benutzer	Kann Warnungen anzeigen und verwalten sowie forensische Daten anzeigen. Die Benutzerrolle kann den Alarmstatus ändern, eine Notiz hinzufügen, manuell Schnappschüsse machen und den Benutzerzugriff blockieren.
Gast	Kann Warnungen und Forensik anzeigen. Mit der Gastrolle können Sie den Alarmstatus nicht ändern, keine Notiz hinzufügen, keine manuellen Schnappschüsse erstellen oder den Benutzerzugriff blockieren.

Betriebssystemunterstützung

Die CentOS 8.x-Unterstützung wird durch die **CentOS 8 Stream**-Unterstützung ersetzt. CentOS 8.x erreicht am 31. Dezember 2021 das End-of-Life.

Datensammler-Updates

Um Anbieteränderungen widerzuspiegeln, wurden eine Reihe von Cloud Insights Datensammlernamen hinzugefügt:

Anbieter/Modell	Vorheriger Name

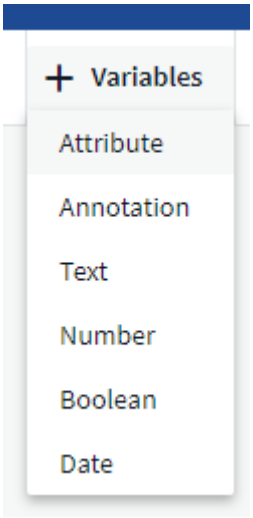
Dell EMC PowerScale	Isilon
HPE Alletra 9000 / Primera	3PAR
HPE Alletra 6000	Flink

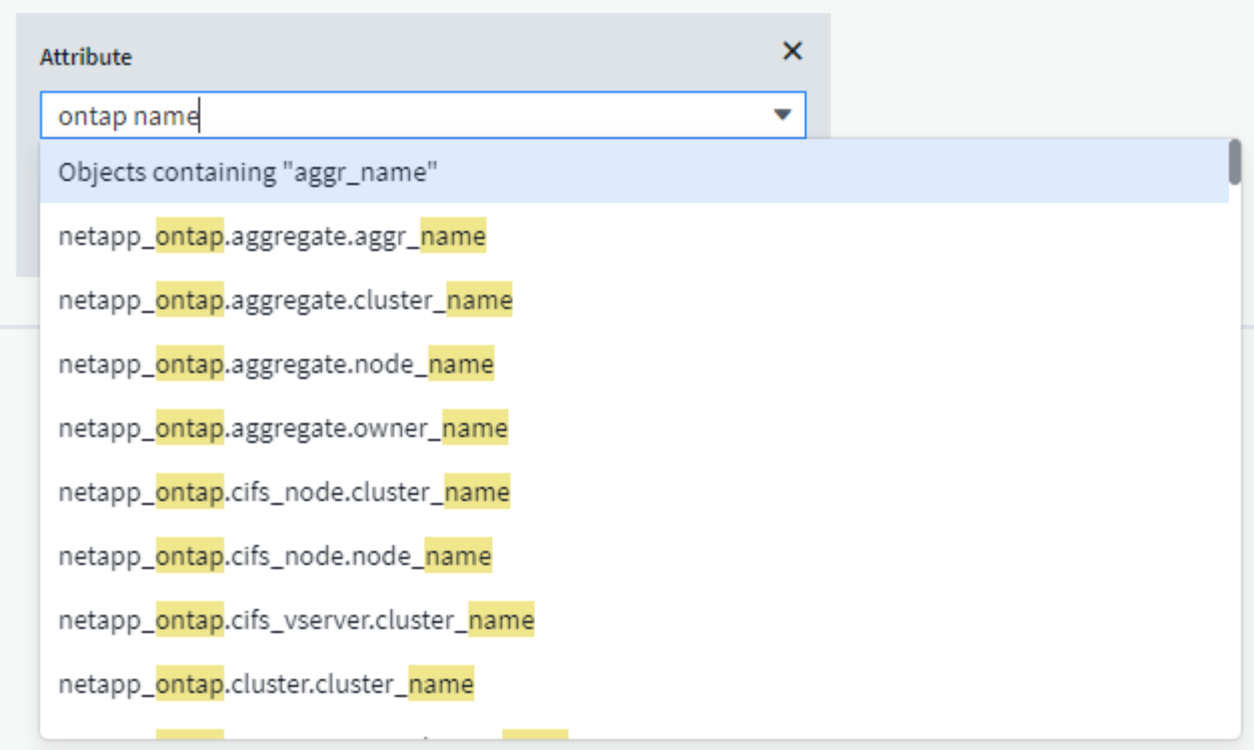
November 2021

Adaptive Dashboards

Neue Variablen für Attribute und die Möglichkeit, Variablen in Widgets zu verwenden.

Dashboards sind jetzt leistungsfähiger und flexibler als je zuvor. Erstellen Sie adaptive Dashboards mit Attributvariablen, um Dashboards schnell und im Handumdrehen zu filtern. Mit diesen und anderen bereits vorhandenen"Variablen" Sie können jetzt ein Dashboard auf hoher Ebene erstellen, um Metriken für Ihre gesamte Umgebung anzuzeigen und nahtlos nach Ressourcenname, Typ, Standort usw. zu filtern. Verwenden Sie Zahlenvariablen in Widgets, um Rohmesswerte mit Kosten zu verknüpfen, beispielsweise Kosten pro GB für Speicher als Service.





Zugriff auf die Berichtsdatenbank über die API

Erweiterte Funktionen für die Integration mit Reporting-, ITSM- und Automatisierungstools von Drittanbietern: Cloud Insights' leistungsstarke"API" ermöglicht es Benutzern, die Cloud Insights Reporting-Datenbank direkt abzufragen, ohne die Cognos Reporting-Umgebung zu durchlaufen.

Pod-Tabellen auf der VM-Landingpage

Nahtlose Navigation zwischen VMs und den sie verwendenden Kubernetes-Pods: Zur verbesserten Fehlerbehebung und Verwaltung des Leistungsspielraums wird jetzt auf den VM-Landingpages eine Tabelle mit den zugehörigen Kubernetes-Pods angezeigt.

Datensammler-Updates

- ECS meldet jetzt Firmware für Speicher und Knoten
- Isilon hat die Eingabeaufforderungserkennung verbessert
- Azure NetApp Files erfasst Leistungsdaten schneller
- StorageGRID unterstützt jetzt Single Sign-On (SSO)
- Brocade CLI meldet das Modell für X&-4 ordnungsgemäß

Weitere unterstützte Betriebssysteme

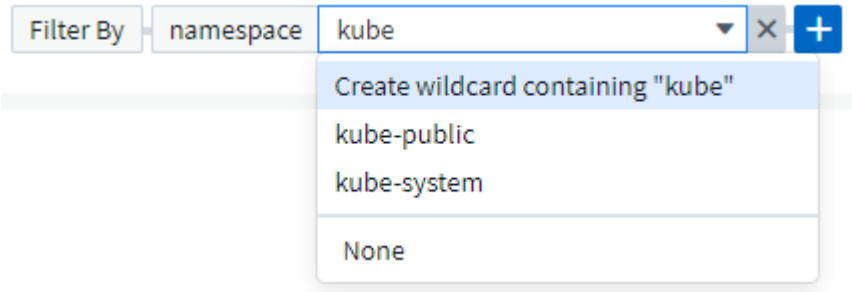
Die Cloud Insights Acquisition Unit unterstützt zusätzlich zu den bereits unterstützten Betriebssystemen die folgenden:

- Centos (64-Bit) 8.4
- Oracle Enterprise Linux (64-Bit) 8.4
- Red Hat Enterprise Linux (64-Bit) 8.4

Oktober 2021

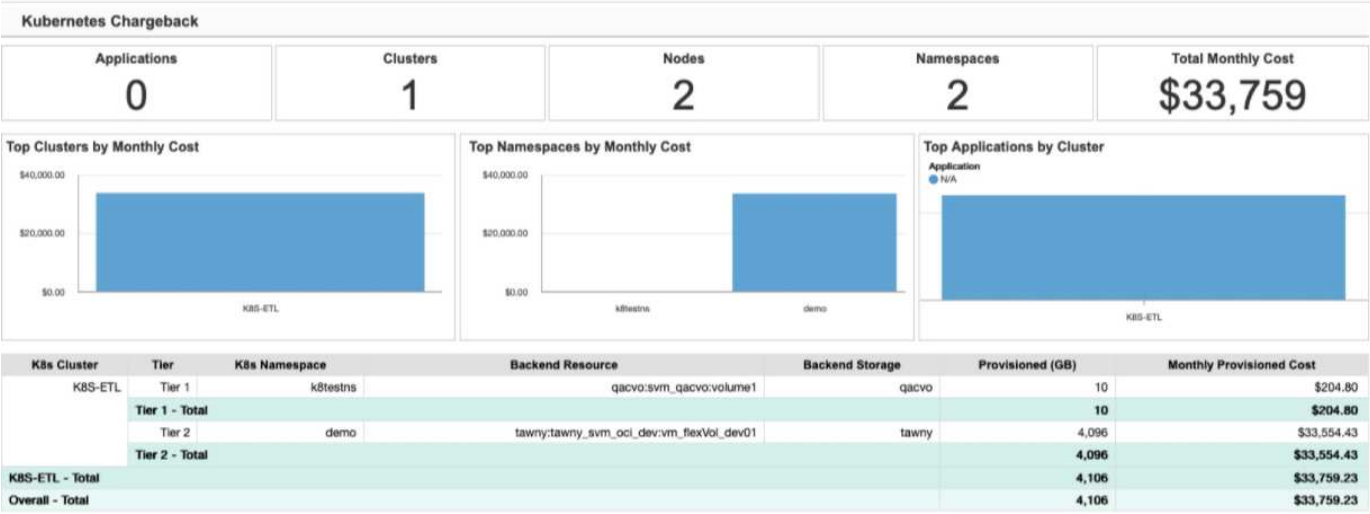
Filter auf K8S Explorer-Seiten

"Kubernetes Explorer"Seitenfilter geben Ihnen eine gezielte Kontrolle über die für Ihre Kubernetes-Cluster-, Knoten- und Pod-Erkundung angezeigten Daten.



K8s-Daten für die Berichterstattung

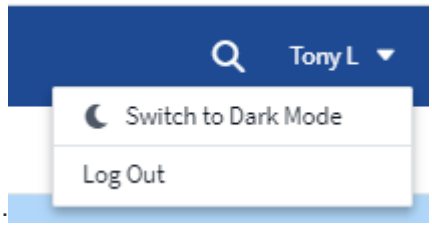
Kubernetes-Daten stehen jetzt für die Verwendung in der Berichterstattung zur Verfügung, sodass Sie Chargeback- oder andere Berichte erstellen können. Damit Kubernetes-Chargeback-Daten an Reporting übergeben werden können, müssen Sie über eine aktive Verbindung zu Ihrem Kubernetes-Cluster und seinem Back-End-Speicher verfügen und Cloud Insights muss Daten von diesem empfangen. Wenn keine Daten vom Back-End-Speicher empfangen werden, kann Cloud Insights keine Kubernetes-Objektdaten an Reporting senden.

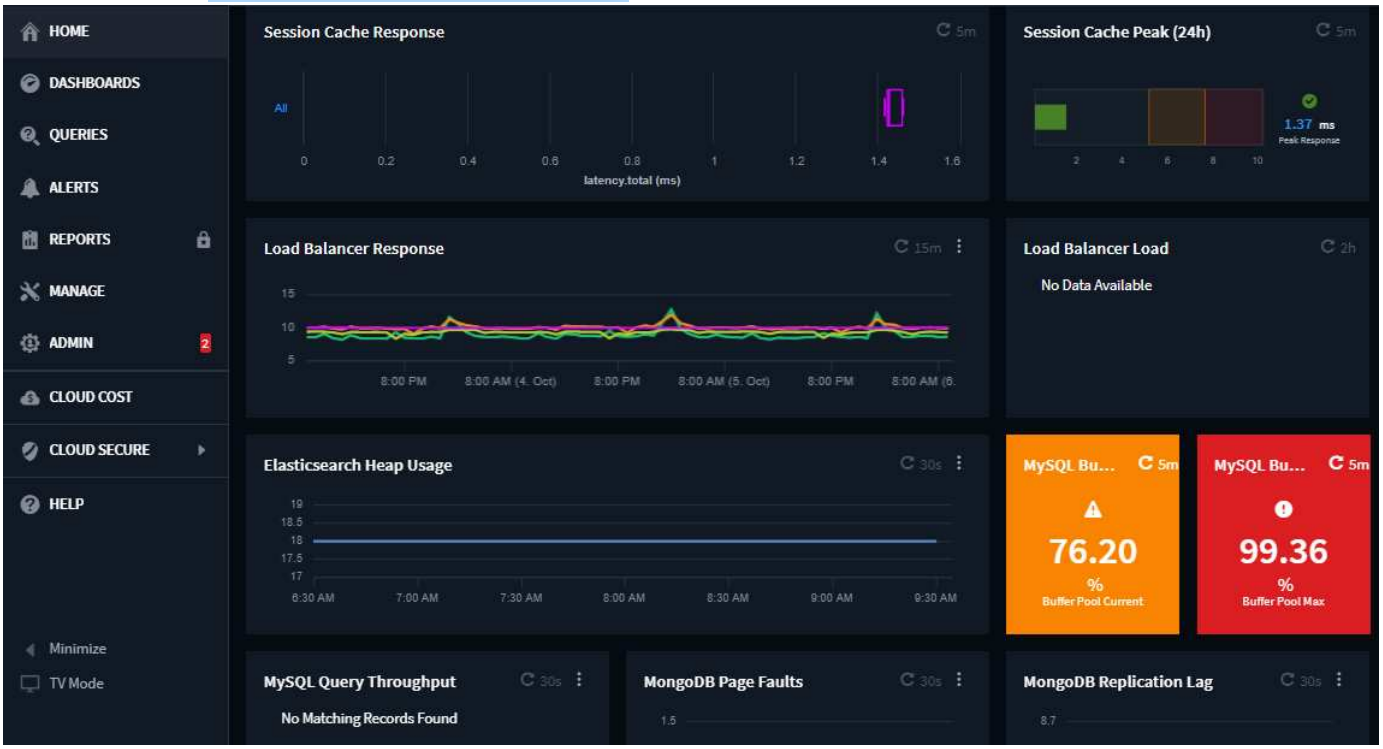


K8s Cluster	Tier	K8s Namespace	Backend Resource	Backend Storage	Provisioned (GB)	Monthly Provisioned Cost
K8S-ETL	Tier 1	k8testns	qacvo:svm_qacvo:volume1	qacvo	10	$204.80
	Tier 1 - Total				**10**	**$204.80**
	Tier 2	demo	tawny:tawny_svm_oci_dev:vm_flexVol_dev01	tawny	4,096	$33,554.43
	Tier 2 - Total				**4,096**	**$33,554.43**
K8S-ETL - Total					**4,106**	**$33,759.23**
Overall - Total					**4,106**	**$33,759.23**

Das dunkle Design ist da

Viele von Ihnen haben nach einem dunklen Design gefragt und Cloud Insights hat geantwortet. Um zwischen hellem und dunklem Design zu wechseln, klicken Sie auf das Dropdown-Menü neben Ihrem Benutzernamen.





Datensammler-Unterstützung

Wir haben einige Verbesserungen an den Cloud Insights Datensammlern vorgenommen. Hier sind einige Highlights:

- Neuer Collector für Amazon FSx für ONTAP

September 2021

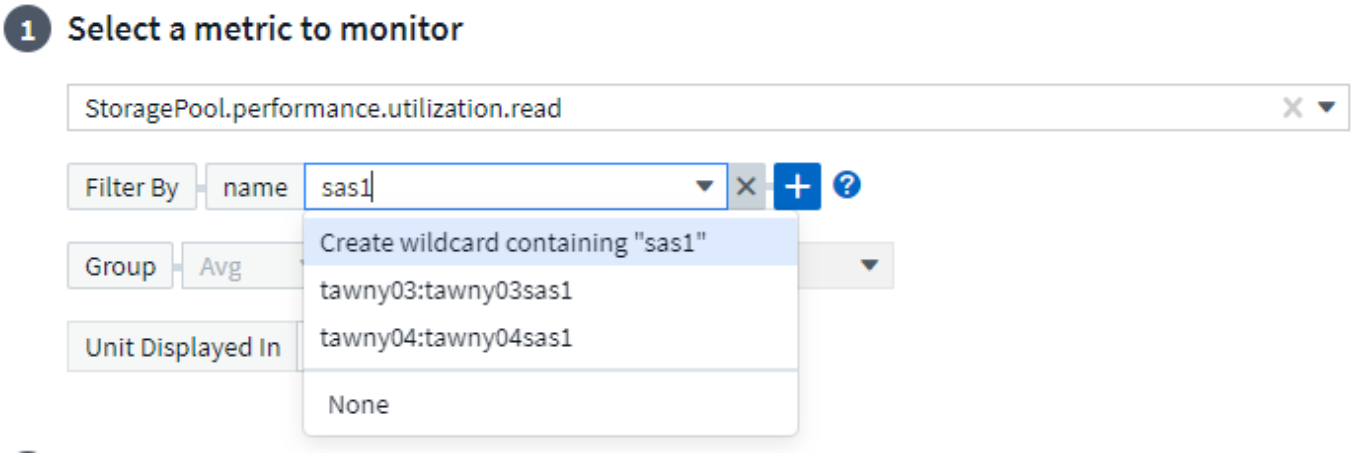
Leistungsrichtlinien sind jetzt Monitore

Monitore und Warnungen haben Leistungsrichtlinien und -verstöße in Cloud Insights ersetzt. "Alarmierung mit Monitoren" bietet mehr Flexibilität und Einblick in potenzielle Probleme oder Trends in Ihrer Umgebung.

Autovervollständigungsvorschläge, Platzhalter und Ausdrücke in Monitoren

Beim Erstellen eines Monitors für Warnmeldungen erfolgt die Eingabe eines Filters jetzt vorausschauend, sodass Sie die Metriken oder Attribute für Ihren Monitor einfach suchen und finden können. Darüber hinaus

haben Sie die Möglichkeit, basierend auf dem von Ihnen eingegebenen Text einen Platzhalterfilter zu erstellen.



Aktualisierter Telegraf-Agent

Der Agent für die Aufnahme von Telegraf-Integrationsdaten wurde auf Version **1.19.3** aktualisiert und bietet Leistungs- und Sicherheitsverbesserungen. Benutzer, die ein Update durchführen möchten, können sich auf den entsprechenden Upgrade-Abschnitt der"Agent-Installation" Dokumentation. Frühere Versionen des Agenten funktionieren weiterhin, ohne dass ein Eingreifen des Benutzers erforderlich ist.

Datensammler-Unterstützung

Wir haben einige Verbesserungen an den Cloud Insights Datensammlern vorgenommen. Hier sind einige Highlights:

- Microsoft Hyper-V Collector verwendet jetzt PowerShell anstelle von WMI
- Azure VMs und VHD Collector sind jetzt durch parallele Aufrufe bis zu 10-mal schneller
- HPE Nimble unterstützt jetzt föderierte und iSCSI-Konfigurationen

Und da wir die Datenerfassung ständig verbessern, sind hier einige weitere wichtige Änderungen:

- Neuer Kollektor für EMC Powerstore
- Neuer Collector für Hitachi Ops Center
- Neuer Collector für die Hitachi Content Platform
- Verbesserter ONTAP Collector zur Meldung von Fabric Pools
- Verbessertes ANF mit Speicherpool- und Volume-Leistung
- Verbessertes EMC ECS mit Storage Nodes und Storage-Performance sowie der Objektanzahl in Buckets
- Verbessertes EMC Isilon mit Storage Node- und Qtree-Metriken
- Verbesserte EMC Symetrix mit Volumen-QOS-Limitmetriken
- Verbesserter IBM SVC und EMC PowerStore mit übergeordneter Seriennummer für Storage Nodes

August 2021

Neue Benutzeroberfläche der Audit-Seite

Der"Audit-Seite" bietet eine übersichtlichere Benutzeroberfläche und ermöglicht jetzt den Export von Audit-Ereignissen in eine CSV-Datei.

Verbesserte Benutzerrollenverwaltung

Cloud Insights ermöglicht jetzt noch mehr Freiheit bei der Zuweisung von Benutzerrollen und Zugriffskontrollen. Benutzern können jetzt separat detaillierte Berechtigungen für Überwachung, Berichterstellung und Cloud Secure zugewiesen werden.

Dies bedeutet, dass Sie mehr Benutzern administrativen Zugriff auf Überwachungs-, Optimierungs- und Berichtsfunktionen gewähren und gleichzeitig den Zugriff auf Ihre vertraulichen Cloud Secure -Audit- und Aktivitätsdaten auf diejenigen beschränken können, die ihn benötigen.

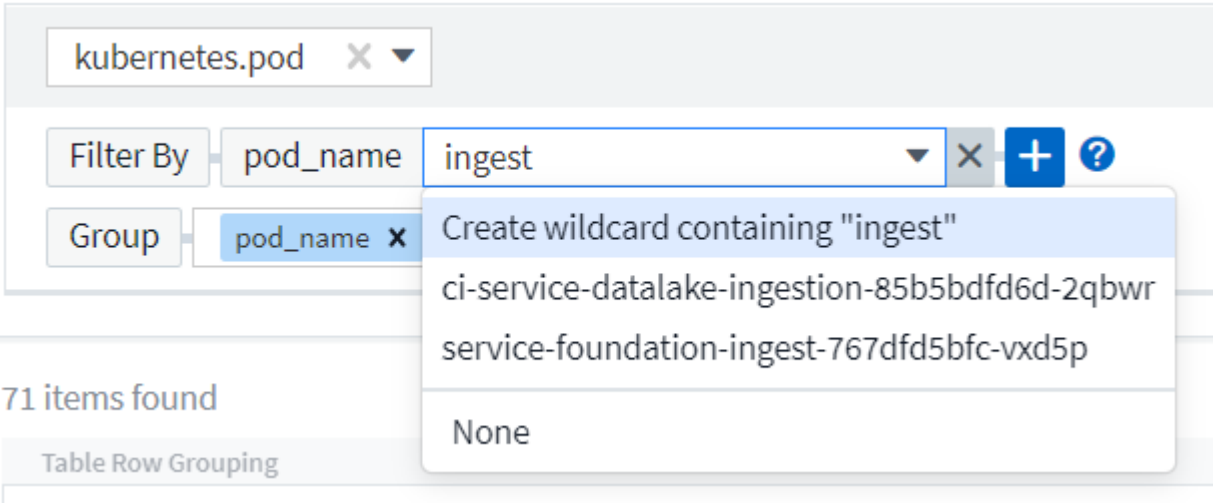
"Mehr erfahren"Informationen zu den verschiedenen Zugriffsebenen finden Sie in der Cloud Insights -Dokumentation.

Juni 2021

Autovervollständigungsvorschläge, Platzhalter und Ausdrücke in Filtern

Mit dieser Version von Cloud Insights müssen Sie nicht mehr alle möglichen Namen und Werte kennen, nach denen Sie in einer Abfrage oder einem Widget filtern können. Beim Filtern können Sie einfach mit der Eingabe beginnen und Cloud Insights schlägt Ihnen Werte basierend auf Ihrem Text vor. Sie müssen nicht mehr im Voraus nach Anwendungsnamen oder Kubernetes-Attributen suchen, nur um diejenigen zu finden, die Sie in Ihrem Widget anzeigen möchten.

Während Sie einen Filter eingeben, zeigt der Filter eine intelligente Liste mit Ergebnissen an, aus denen Sie auswählen können, sowie die Option, einen **Platzhalterfilter** basierend auf dem aktuellen Text zu erstellen. Wenn Sie diese Option auswählen, werden alle Ergebnisse zurückgegeben, die mit dem Platzhalterausdruck übereinstimmen. Natürlich können Sie auch mehrere Einzelwerte auswählen, die Sie dem Filter hinzufügen möchten.



Darüber hinaus können Sie mithilfe von NOT oder OR **Ausdrücke** in einem Filter erstellen oder die Option „Keine“ auswählen, um nach Nullwerten im Feld zu filtern.

Lesen Sie mehr über"Filteroptionen" in Abfragen und Widgets.

Verfügbare APIs nach Edition

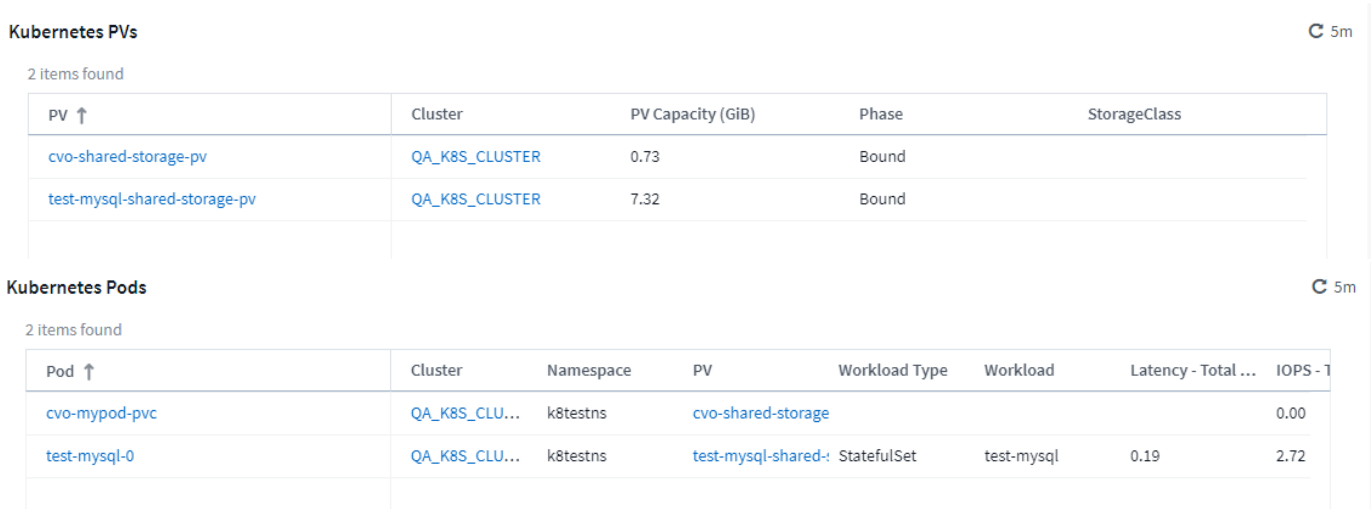
Die leistungsstarken APIs von Cloud Insights sind zugänglicher als je zuvor, da Alerts-APIs jetzt in der Standard- und Premium-Edition verfügbar sind. Für jede Edition sind die folgenden APIs verfügbar:

API-Kategorie	Basic	Standard	Prämie
Erfassungseinheit	✔	✔	✔
Datenerfassung	✔	✔	✔
Warnungen		✔	✔
Vermögenswerte		✔	✔
Datenaufnahme		✔	✔

Kubernetes PV und Pod-Sichtbarkeit

Cloud Insights bietet Einblick in den Back-End-Speicher Ihrer Kubernetes-Umgebungen und gibt Ihnen Einblick in Ihre Kubernetes-Pods und Persistent Volumes (PVs). Sie können jetzt PV-Zähler wie IOPS, Latenz und Durchsatz von der Nutzung eines einzelnen Pods über einen PV-Zähler bis hin zu einem PV und dem gesamten Weg zum Back-End-Speichergerät verfolgen.

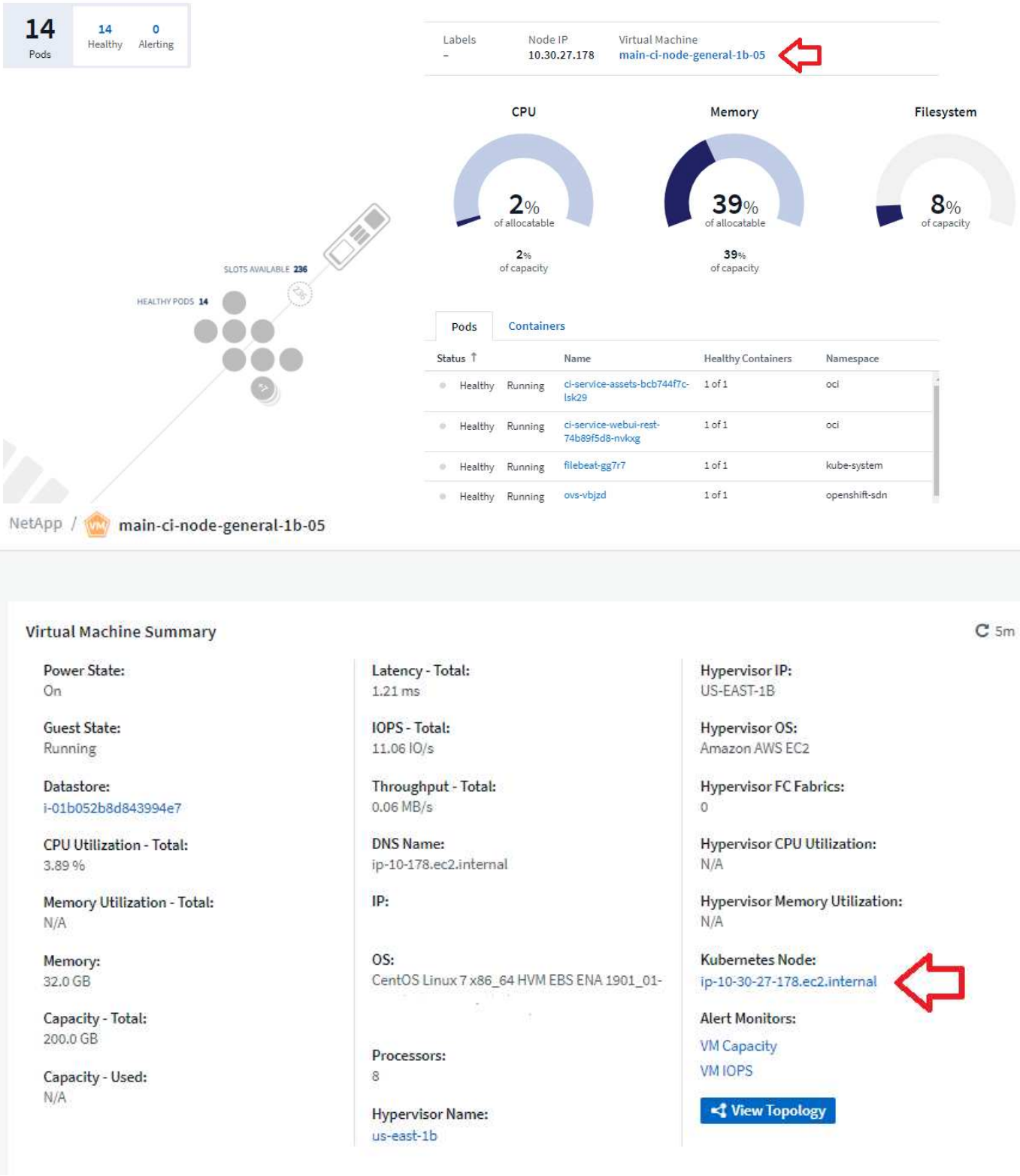
Auf einer Volume- oder Internal Volume-Landingpage werden zwei neue Tabellen angezeigt:



Beachten Sie, dass es zur Nutzung dieser neuen Tabellen empfohlen wird, Ihren aktuellen Kubernetes-Agenten zu deinstallieren und neu zu installieren. Sie müssen außerdem Kube-State-Metrics Version 2.1.0 oder höher installieren.

Kubernetes-Knoten-zu-VM-Links

Auf einer Kubernetes-Knotenseite können Sie jetzt klicken, um die VM-Seite des Knotens zu öffnen. Die VM-Seite enthält auch einen Link zurück zum Knoten selbst.



Alert-Monitore ersetzen Leistungsrichtlinien

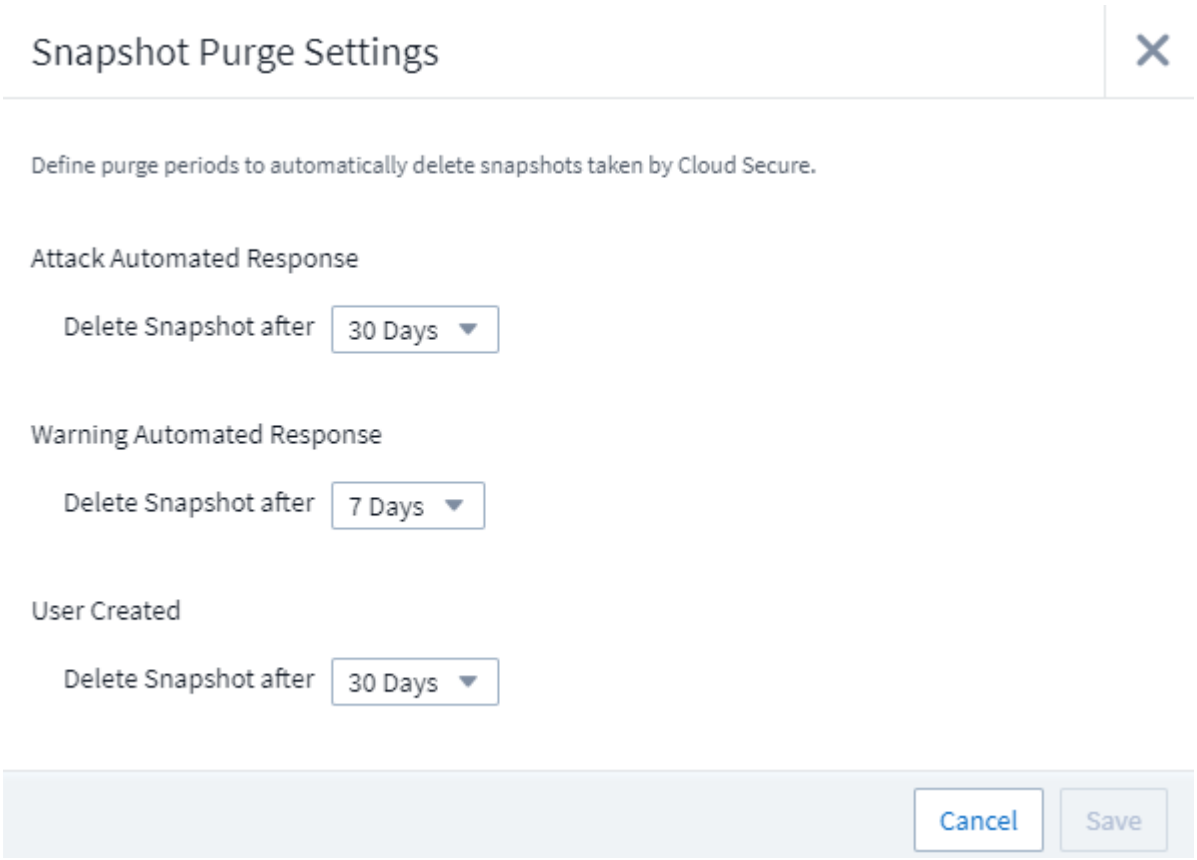
Um die zusätzlichen Vorteile mehrerer Schwellenwerte, der Zustellung von Webhook- und E-Mail-Benachrichtigungen, der Benachrichtigung zu allen Metriken über eine einzige Schnittstelle und mehr zu ermöglichen, wird Cloud Insights in den Monaten Juli und August 2021 Kunden der Standard- und Premium-Edition von **Leistungsrichtlinien** auf **Monitore** umstellen. Erfahren Sie mehr über"Warnungen und Monitore" , und bleiben Sie dran für diese aufregende Änderung.

Cloud Secure unterstützt NFS

Cloud Secure unterstützt jetzt NFS für die ONTAP Datenerfassung. Überwachen Sie den SMB- und NFS-Benutzerzugriff, um Ihre Daten vor Ransomware-Angriffen zu schützen. Darüber hinaus unterstützt Cloud Secure Active Directory- und LDAP-Benutzerverzeichnisse zum Sammeln von NFS-Benutzerattributen.

Cloud Secure -Snapshot-Bereinigung

Cloud Secure löscht Snapshots automatisch basierend auf den Snapshot-Bereinigungseinstellungen, um Speicherplatz zu sparen und die Notwendigkeit manueller Snapshot-Löschung zu reduzieren.



Geschwindigkeit der Cloud Secure Datenerfassung

Ein einzelnes Datenerfassungsagentensystem kann jetzt bis zu 20.000 Ereignisse pro Sekunde an Cloud Secure senden.

Juni 2021

Hier sind einige der Änderungen, die wir im April vorgenommen haben:

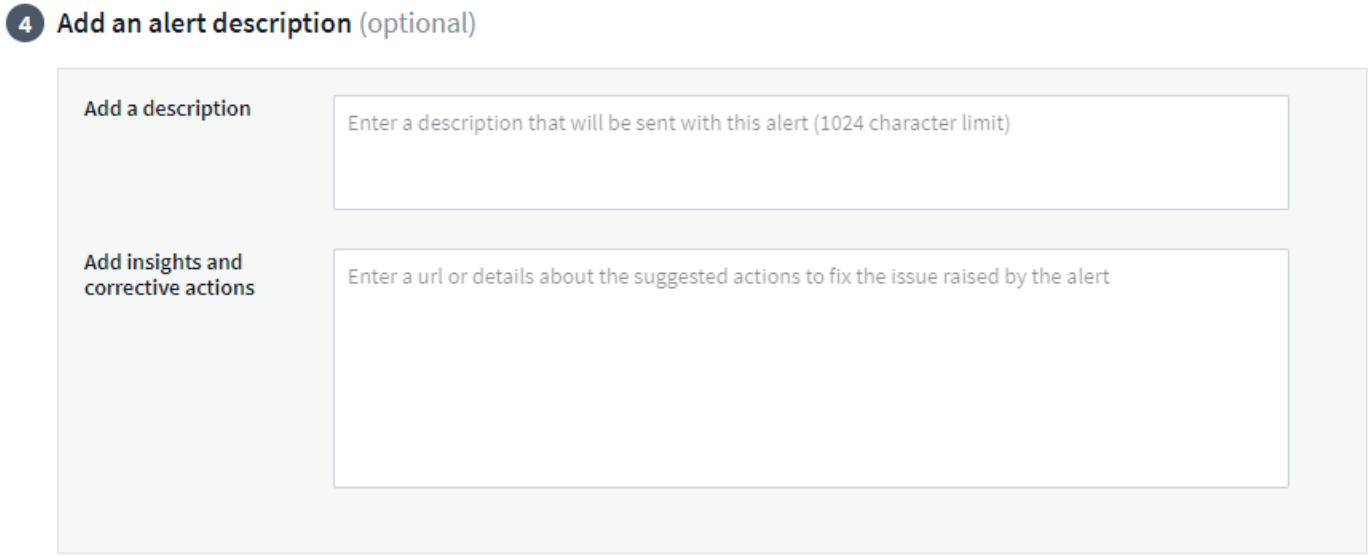
Aktualisierter Telegraf-Agent

Der Agent für die Aufnahme von Telegraf-Integrationsdaten wurde auf Version 1.17.3 aktualisiert und bietet Leistungs- und Sicherheitsverbesserungen. Benutzer, die ein Update durchführen möchten, können sich auf den entsprechenden Upgrade-Abschnitt der"Agent-Installation" Dokumentation. Frühere Versionen des

Agenten funktionieren weiterhin, ohne dass ein Eingreifen des Benutzers erforderlich ist.

Hinzufügen von Korrekturmaßnahmen zu einer Warnung

Sie können jetzt beim Erstellen oder Ändern eines Monitors eine optionale Beschreibung sowie zusätzliche Erkenntnisse und/oder Korrekturmaßnahmen hinzufügen, indem Sie den Abschnitt **Alarmbeschreibung hinzufügen** ausfüllen. Die Beschreibung wird mit der Benachrichtigung gesendet. Das Feld „Erkenntnisse und Korrekturmaßnahmen“ kann detaillierte Schritte und Anleitungen zum Umgang mit Warnungen bereitstellen und wird im Zusammenfassungsbereich der Zielseite der Warnung angezeigt.



Cloud Insights -APIs für alle Editionen

API-Zugriff ist jetzt in allen Editionen von Cloud Insights verfügbar. Benutzer der Basic Edition können jetzt Aktionen für Erfassungseinheiten und Datensammler automatisieren und Benutzer der Standard Edition können Metriken abfragen und benutzerdefinierte Metriken aufnehmen. Die Premium-Edition ermöglicht weiterhin die vollständige Nutzung aller API-Kategorien.

API-Kategorie	Basic	Standard	Prämie
Erfassungseinheit	✔	✔	✔
Datenerfassung	✔	✔	✔
Vermögenswerte		✔	✔
Datenaufnahme		✔	✔
Data Warehouse			✔

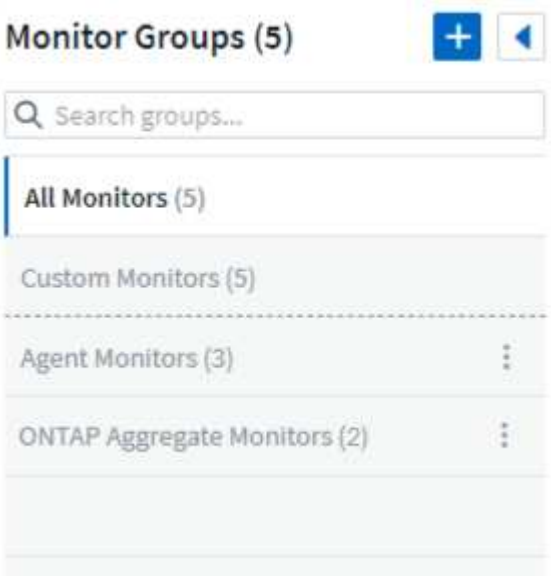
Einzelheiten zur API-Nutzung finden Sie im"API-Dokumentation" .

April 2021

Einfachere Verwaltung von Monitoren

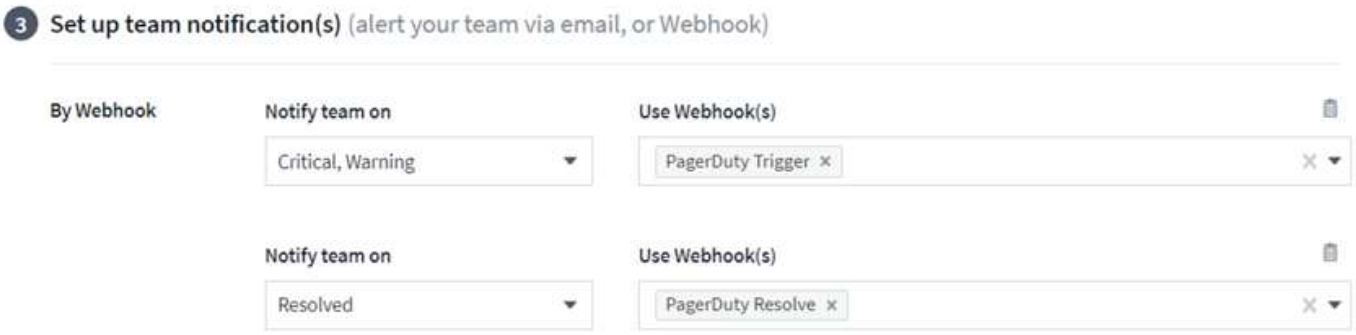
"Monitorgruppierung"vereinfacht die Verwaltung von Monitoren in Ihrer Umgebung. Mehrere Monitore können jetzt gruppiert und als einer angehalten werden. Wenn beispielsweise ein Update für einen Infrastrukturstapel durchgeführt wird, können Sie die Benachrichtigungen von allen diesen Geräten mit einem Klick anhalten.

Monitorgruppen sind der erste Teil einer spannenden neuen Funktion, die Cloud Insights eine verbesserte Verwaltung von ONTAP Geräten ermöglicht.



Erweiterte Warnoptionen durch Webhooks

Viele kommerzielle Anwendungen unterstützen"Webhooks" als Standard-Eingabeschnittstelle. Cloud Insights unterstützt jetzt viele dieser Bereitstellungskanäle und bietet Standardvorlagen für Slack, PagerDuty, Teams und Discord sowie anpassbare generische Webhooks zur Unterstützung vieler anderer Anwendungen.



Verbesserte Geräteidentifikation

Um die Überwachung und Fehlerbehebung zu verbessern und genaue Berichte zu liefern, ist es hilfreich, die Namen der Geräte zu kennen und nicht ihre IP-Adressen oder andere Kennungen. Cloud Insights bietet jetzt eine automatische Methode zur Identifizierung der Namen von Speicher- und physischen Hostgeräten in der Umgebung. Dabei kommt ein regelbasierter Ansatz namens**"Geräteauflösung"** , verfügbar im Menü **Verwalten**.

Sie haben nach mehr gefragt!

Eine häufige Anfrage unserer Kunden betraf mehr Standardoptionen zur Visualisierung des Datenbereichs. Daher haben wir die folgenden fünf neuen Auswahlmöglichkeiten hinzugefügt, die jetzt im gesamten Dienst über die Zeitbereichsauswahl verfügbar sind:

- Letzte 30 Minuten
- Letzte 2 Stunden
- Letzte 6 Stunden
- Letzte 12 Stunden
- Letzte 2 Tage

Mehrere Abonnements in einer Cloud Insights Umgebung

Ab dem 2. April unterstützt Cloud Insights mehrere Abonnements desselben Editionstyps für einen Kunden in einer einzigen Cloud Insights Instanz. Dadurch können Kunden Teile ihres Cloud Insights -Abonnements mit Infrastrukturkäufen zusammenlegen. Wenden Sie sich an den NetApp -Vertrieb, wenn Sie Unterstützung bei mehreren Abonnements benötigen.

Wähle deinen Weg

Beim Einrichten von Cloud Insights können Sie jetzt wählen, ob Sie mit Überwachung und Warnmeldungen oder mit der Erkennung von Ransomware und Insider-Bedrohungen beginnen möchten. Cloud Insights konfiguriert Ihre Startumgebung basierend auf dem von Ihnen gewählten Pfad. Den anderen Pfad können Sie jederzeit nachträglich konfigurieren.

Einfacheres, Cloud Secure -Onboarding

Und mit einer neuen Schritt-für-Schritt-Checkliste zur Einrichtung ist es einfacher denn je, mit der Nutzung von Cloud Secure zu beginnen.

Wie immer freuen wir uns über Ihre Vorschläge! Senden Sie sie an ng-cloudinsights-customerfeedback@netapp.com.

Februar 2021

Aktualisierter Telegraf-Agent

Der Agent für die Aufnahme von Telegraf-Integrationsdaten wurde auf Version 1.17.0 aktualisiert, die Schwachstellen- und Fehlerbehebungen enthält.

Cloud-Kostenanalysator

Erleben Sie die Leistungsfähigkeit von Spot by NetApp mit Cloud Cost, das eine detaillierte Kostenanalyse der vergangenen, aktuellen und geschätzten Ausgaben bietet und Ihnen Einblick in die Cloud-Nutzung in Ihrer Umgebung gewährt. Das Cloud-Kosten-Dashboard bietet eine klare Übersicht über die Cloud-Ausgaben und eine detaillierte Analyse einzelner Workloads, Konten und Dienste.

Cloud Cost kann bei diesen großen Herausforderungen helfen:

- Verfolgen und Überwachen Ihrer Cloud-Ausgaben
- Identifizierung von Verschwendung und Optimierungspotenzialen
- Bereitstellung ausführbarer Aktionselemente

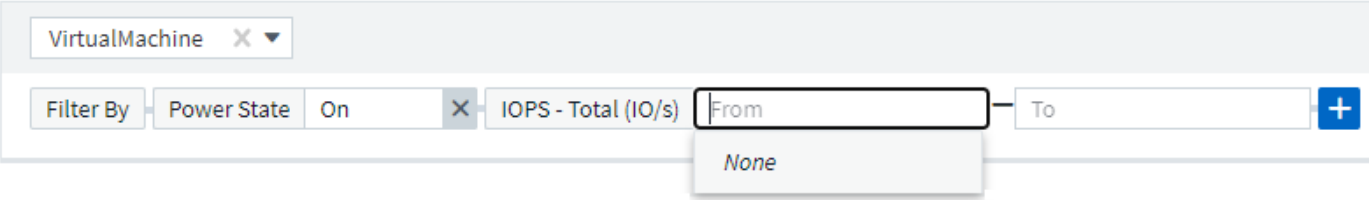
Der Schwerpunkt von Cloud Cost liegt auf der Überwachung. Führen Sie ein Upgrade auf das vollständige Spot by NetApp -Konto durch, um automatische Kosteneinsparungen und Umgebungsoptimierungen zu ermöglichen.

Abfragen von Objekten mit Nullwerten mithilfe von Filtern

Cloud Insights ermöglicht jetzt die Suche nach Attributen und Metriken mit Null-/Keine-Werten durch die Verwendung von Filtern. Sie können diese Filterung für beliebige Attribute/Metriken an den folgenden Stellen durchführen:

- Auf der Abfrageseite
- In Dashboard-Widgets und Seitenvariablen
- Auf der Seite „Warnungsliste“
- Beim Erstellen von Monitoren

Um nach Null-/Keine-Werten zu filtern, wählen Sie einfach die Option *Keine* aus, wenn sie im entsprechenden Filter-Dropdown-Menü angezeigt wird.



Unterstützung mehrerer Regionen

Ab heute bieten wir den Cloud Insights -Dienst in verschiedenen Regionen weltweit an, der die Leistung verbessert und die Sicherheit für Kunden außerhalb der USA erhöht. Cloud Insights/ Cloud Secure speichert Informationen entsprechend der Region, in der Ihre Umgebung erstellt wird.

Klicken"hier," für weitere Informationen.

Januar 2021

Zusätzliche ONTAP -Metriken umbenannt

Im Rahmen unserer kontinuierlichen Bemühungen, die Effizienz der Datenerfassung von ONTAP -Systemen zu verbessern, wurden die folgenden ONTAP -Metriken umbenannt.

Wenn Sie über vorhandene Dashboard-Widgets oder Abfragen verfügen, die eine dieser Metriken verwenden, müssen Sie sie bearbeiten oder neu erstellen, um die neuen Metriknamen zu verwenden.

Vorheriger Metrikname	Neuer Metrikname
netapp_ontap.disk_constituent.total_transfers	netapp_ontap.disk_constituent.total_iops
netapp_ontap.disk.total_transfers	netapp_ontap.disk.total_iops
netapp_ontap.fcp_lif.read_data	netapp_ontap.fcp_lif.read_throughput

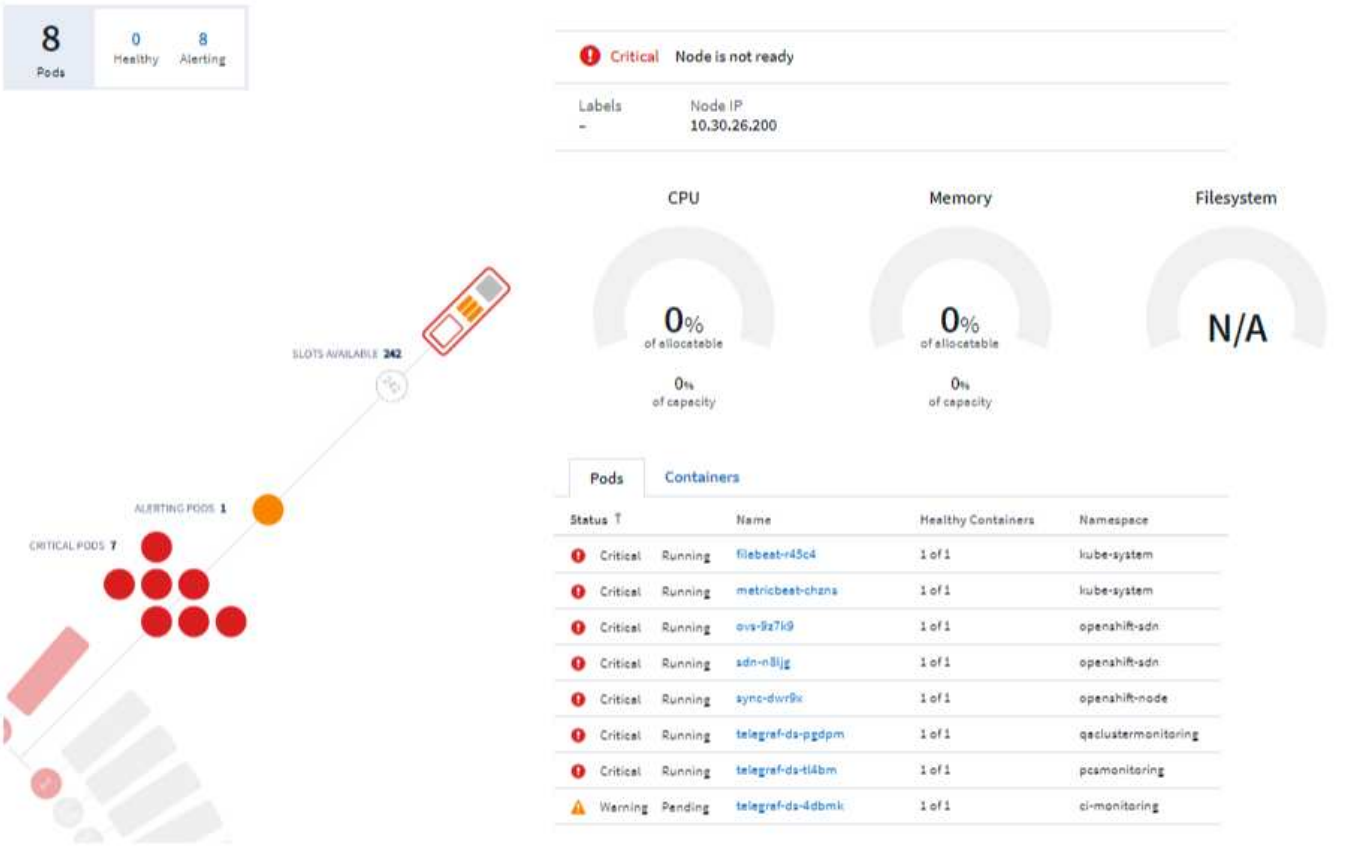
Vorheriger Metrikname	Neuer Metrikname
netapp_ontap.fcp_lif.write_data	netapp_ontap.fcp_lif.write_throughput
netapp_ontap.iscsi_lif.read_data	netapp_ontap.iscsi_lif.read_throughput
netapp_ontap.iscsi_lif.write_data	netapp_ontap.iscsi_lif.write_throughput
netapp_ontap.lif.recv_data	netapp_ontap.lif.recv_throughput
netapp_ontap.lif.sent_data	netapp_ontap.lif.sent_throughput
netapp_ontap.lun.read_data	netapp_ontap.lun.read_throughput
netapp_ontap.lun.write_data	netapp_ontap.lun.write_throughput
netapp_ontap.nic_common.rx_bytes	netapp_ontap.nic_common.rx_throughput
netapp_ontap.nic_common.tx_bytes	netapp_ontap.nic_common.tx_throughput
netapp_ontap.path.read_data	netapp_ontap.path.read_throughput
netapp_ontap.path.write_data	netapp_ontap.path.write_throughput
netapp_ontap.path.total_data	netapp_ontap.path.total_throughput
netapp_ontap.policy_group.read_data	netapp_ontap.policy_group.read_throughput
netapp_ontap.policy_group.write_data	netapp_ontap.policy_group.write_throughput
netapp_ontap.policy_group.other_data	netapp_ontap.policy_group.other_throughput
netapp_ontap.policy_group.total_data	netapp_ontap.policy_group.total_throughput
netapp_ontap.system_node.disk_data_read	netapp_ontap.system_node.disk_throughput_read
netapp_ontap.system_node.disk_data_written	netapp_ontap.system_node.disk_throughput_written
netapp_ontap.system_node.hdd_data_read	netapp_ontap.system_node.hdd_throughput_read
netapp_ontap.system_node.hdd_data_written	netapp_ontap.system_node.hdd_throughput_written
netapp_ontap.system_node.ssd_data_read	netapp_ontap.system_node.ssd_throughput_read
netapp_ontap.system_node.ssd_data_written	netapp_ontap.system_node.ssd_throughput_written
netapp_ontap.system_node.net_data_recv	netapp_ontap.system_node.net_throughput_recv
netapp_ontap.system_node.net_data_sent	netapp_ontap.system_node.net_throughput_sent
netapp_ontap.system_node.fcp_data_recv	netapp_ontap.system_node.fcp_throughput_recv
netapp_ontap.system_node.fcp_data_sent	netapp_ontap.system_node.fcp_throughput_sent
netapp_ontap.volume_node.cifs_read_data	netapp_ontap.volume_node.cifs_read_throughput
netapp_ontap.volume_node.cifs_write_data	netapp_ontap.volume_node.cifs_write_throughput
netapp_ontap.volume_node.nfs_read_data	netapp_ontap.volume_node.nfs_read_throughput
netapp_ontap.volume_node.nfs_write_data	netapp_ontap.volume_node.nfs_write_throughput
netapp_ontap.volume_node.iscsi_read_data	netapp_ontap.volume_node.iscsi_read_throughput
netapp_ontap.volume_node.iscsi_write_data	netapp_ontap.volume_node.iscsi_write_throughput
netapp_ontap.volume_node.fcp_read_data	netapp_ontap.volume_node.fcp_read_throughput

Vorheriger Metrikname	Neuer Metrikname
netapp_ontap.volume_node.fcp_write_data	netapp_ontap.volume_node.fcp_write_throughput
netapp_ontap.volume.read_data	netapp_ontap.volume.read_throughput
netapp_ontap.volume.write_data	netapp_ontap.volume.write_throughput
netapp_ontap.workload.read_data	netapp_ontap.workload.read_throughput
netapp_ontap.workload.write_data	netapp_ontap.workload.write_throughput
netapp_ontap.workload_volume.read_data	netapp_ontap.workload_volume.read_throughput
netapp_ontap.workload_volume.write_data	netapp_ontap.workload_volume.write_throughput

Neuer Kubernetes Explorer

Der"Kubernetes Explorer" bietet eine einfache Topologieansicht von Kubernetes-Clustern, sodass auch Nicht-Experten Probleme und Abhängigkeiten schnell erkennen können, von der Clusterebene bis hin zum Container und Speicher.

Mithilfe der Drilldown-Details des Kubernetes Explorers können Sie eine Vielzahl von Informationen zu Status, Nutzung und Integrität der Cluster, Knoten, Pods, Container und Speicher in Ihrer Kubernetes-Umgebung erkunden.



Dezember 2020

Einfachere Kubernetes-Installation

Die Installation des Kubernetes-Agenten wurde optimiert, sodass weniger Benutzerinteraktionen erforderlich sind. "Installieren des Kubernetes-Agenten" umfasst jetzt die Kubernetes-Datenerfassung.

November 2020

Zusätzliche Dashboards

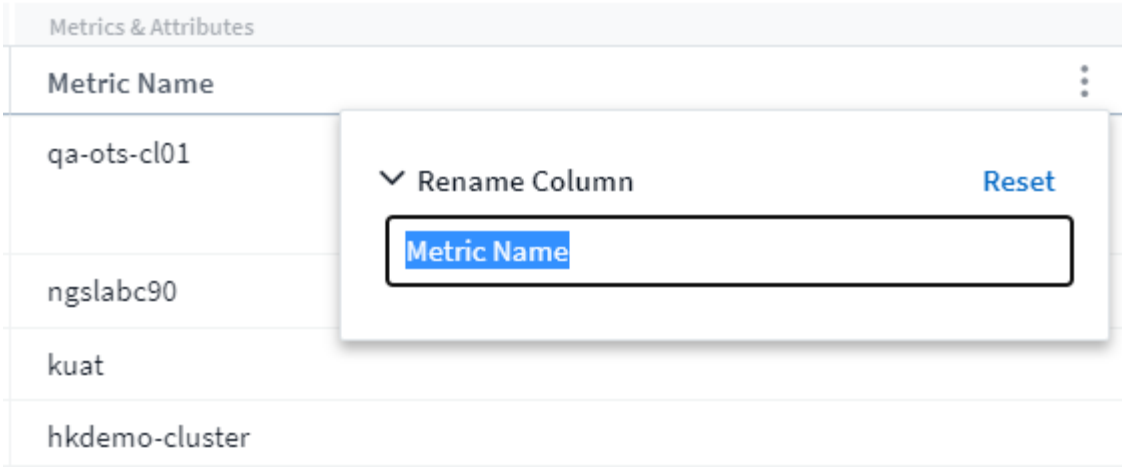
Die folgenden neuen ONTAP-fokussierten Dashboards wurden der Galerie hinzugefügt und stehen zum Importieren zur Verfügung:

- ONTAP: Gesamtleistung und -kapazität
- ONTAP FAS/ AFF – Kapazitätsauslastung
- ONTAP FAS/ AFF – Clusterkapazität
- ONTAP FAS/ AFF – Effizienz
- ONTAP FAS/ AFF – FlexVol -Leistung
- ONTAP FAS/ AFF – Knotenbetriebs-/Optimalpunkte
- ONTAP FAS/ AFF – PrePost-Kapazitätseffizienz
- ONTAP: Netzwerkportaktivität
- ONTAP: Leistung der Knotenprotokolle
- ONTAP: Knoten-Workload-Leistung (Frontend)
- ONTAP: Prozessor
- ONTAP: SVM-Workload-Leistung (Frontend)
- ONTAP: Leistung bei Volumen-Workloads (Frontend)

Spaltenumbenennung in Tabellen-Widgets

Sie können Spalten im Abschnitt „Metriken und Attribute“ eines Tabellen-Widgets umbenennen, indem Sie das Widget im Bearbeitungsmodus öffnen und auf das Menü oben in der Spalte klicken. Geben Sie den neuen Namen ein und klicken Sie auf *Speichern* oder klicken Sie auf *Zurücksetzen*, um die Spalte wieder auf den ursprünglichen Namen zurückzusetzen.

Beachten Sie, dass dies nur den Anzeigenamen der Spalte im Tabellen-Widget betrifft; der Metrik-/Attributname in den zugrunde liegenden Daten selbst ändert sich nicht.



Oktober 2020

Standarderweiterung von Integrationsdaten

Die Gruppierung von Tabellen-Widgets ermöglicht jetzt Standarderweiterungen von Kubernetes-, ONTAP Advanced Data- und Agent Node-Metriken. Wenn Sie beispielsweise Kubernetes-*Knoten* nach *Cluster* gruppieren, wird in der Tabelle für jeden Cluster eine Zeile angezeigt. Sie können dann jede Clusterzeile erweitern, um eine Liste der Knotenobjekte anzuzeigen.

Technischer Support für die Basic Edition

Technischer Support ist jetzt zusätzlich zu den Standard- und Premium-Editionen auch für Abonnenten der Cloud Insights Basic Edition verfügbar. Darüber hinaus hat Cloud Insights den Workflow zum Erstellen eines NetApp Supporttickets vereinfacht.

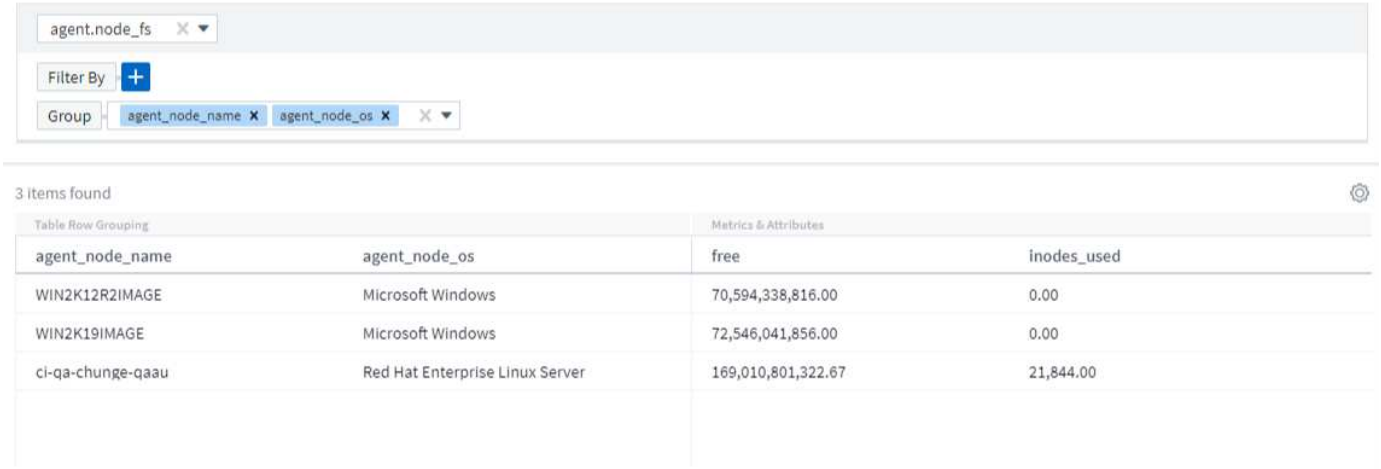
Cloud Secure -API

Cloud Secure unterstützt"REST-APIs" für den Zugriff auf Aktivitäts- und Alarminformationen. Dies wird durch die Verwendung von API-Zugriffstoken erreicht, die über die Cloud Secure Admin-Benutzeroberfläche erstellt und dann für den Zugriff auf die REST-APIs verwendet werden. Die Swagger-Dokumentation für diese REST-APIs ist in Cloud Secure integriert.

September 2020

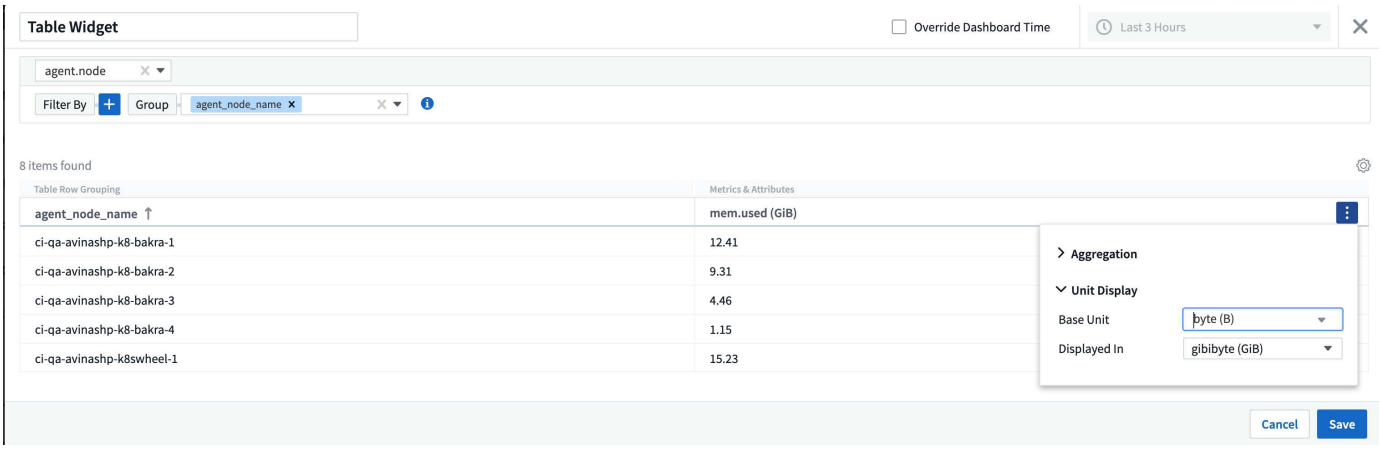
Abfrageseite mit Integrationsdaten

Die Cloud Insights -Abfrageseite unterstützt Integrationsdaten (z. B. von Kubernetes, ONTAP Advanced Metrics usw.). Beim Arbeiten mit Integrationsdaten wird in der Abfrageergebnistabelle eine „Split-Screen“-Ansicht angezeigt, mit Objekt/Gruppierung auf der linken Seite und Objektdaten (Attribute/Metriken) auf der rechten Seite. Sie können auch mehrere Attribute zum Gruppieren von Integrationsdaten auswählen.



Formatierung der Einheitenanzeige im Tabellen-Widget

Die Formatierung der Einheitenanzeige ist jetzt in Tabellen-Widgets für Spalten verfügbar, die Metrik-/Zählerdaten anzeigen (z. B. Gigabyte, MB/Sekunde usw.). Um die Anzeigeeinheit einer Metrik zu ändern, klicken Sie auf das Menü mit den drei Punkten in der Spaltenüberschrift und wählen Sie „Einheitenanzeige“. Sie können aus allen verfügbaren Einheiten wählen. Die verfügbaren Einheiten variieren je nach Art der metrischen Daten in der Anzeigespalte.



Detailseite der Erfassungseinheit

Akquisitionseinheiten verfügen jetzt über eine eigene Zielseite, die nützliche Details zu jeder AU sowie Informationen zur Fehlerbehebung bietet. Der"AU-Detailseite" bietet Links zu den Datensammlern der AU sowie hilfreiche Statusinformationen.

Cloud Secure Docker-Abhängigkeit entfernt

Die Abhängigkeit von Cloud Secure von Docker wurde entfernt. Docker ist für die Installation des Cloud Secure -Agenten nicht mehr erforderlich.

Berichterstellung für Benutzerrollen

Wenn Sie über Cloud Insights Premium Edition mit Reporting verfügen, verfügt jeder Cloud Insights Benutzer in Ihrer Umgebung auch über eine Single Sign-On (SSO)-Anmeldung bei der Reporting-Anwendung (z. B. Cognos). Durch Klicken auf den Link **Berichte** im Menü werden sie automatisch bei Reporting angemeldet.

Ihre Benutzerrolle in Cloud Insights bestimmt ihre"Berichterstellungsbenutzerrolle" :

Cloud Insights -Rolle	Berichtsrolle	Berichtsberechtigungen
Gast	Verbraucher	Kann Berichte anzeigen, planen und ausführen und persönliche Einstellungen wie Sprachen und Zeitzonen festlegen. Verbraucher können keine Berichte erstellen oder Verwaltungsaufgaben ausführen.
Benutzer	Autor	Kann alle Verbraucherfunktionen ausführen sowie Berichte und Dashboards erstellen und verwalten.
Administrator	Administrator	Kann alle Autorenfunktionen sowie alle Verwaltungsaufgaben ausführen, z. B. die Konfiguration von Berichten und das Herunterfahren und Neustarten von Berichtsaufgaben.

Cloud Insights Reporting ist für Umgebungen mit 500 MUs oder mehr verfügbar.

Wenn Sie bereits Premium Edition-Kunde sind und Ihre Berichte behalten möchten, lesen Sie dies"Wichtiger Hinweis für Bestandskunden" .

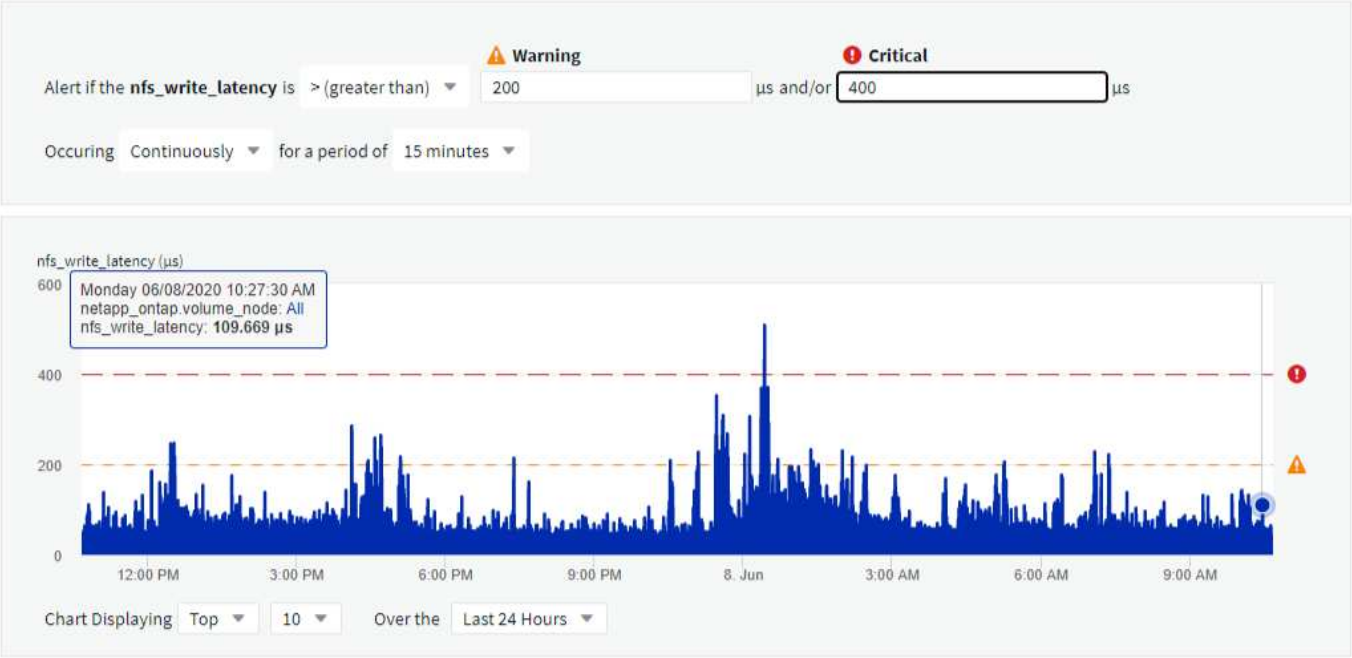
Neue API-Kategorie für die Datenaufnahme

Cloud Insights hat eine API-Kategorie **Data Ingestion** hinzugefügt, die Ihnen mehr Kontrolle über benutzerdefinierte Daten und Agenten gibt. Eine ausführliche Dokumentation zu dieser und anderen API-Kategorien finden Sie in Cloud Insights , indem Sie zu **Admin > API-Zugriff** navigieren und auf den Link *API-Dokumentation* klicken. Sie können der AU auch einen Kommentar im Feld „Notiz“ hinzufügen, der auf der AU-Detailseite sowie der AU-Listenseite angezeigt wird.

August 2020

Überwachung und Alarmierung

Zusätzlich zur aktuellen Möglichkeit, Leistungsrichtlinien für Speicherobjekte, VMs, EC2 und Ports festzulegen, bietet die Cloud Insights Standard Edition jetzt die Möglichkeit,"Monitore konfigurieren" für Schwellenwerte für Integrationsdaten für Kubernetes, erweiterte ONTAP -Metriken und Telegraf-Plugins. Sie erstellen einfach einen Monitor für jede Objektmetrik, für die Sie Warnungen auslösen möchten, legen die Bedingungen für Schwellenwerte auf Warn- oder kritischer Ebene fest und geben den/die gewünschten E-Mail-Empfänger für jede Ebene an. Sie können dann"Anzeigen und Verwalten von Warnungen" um Trends zu verfolgen oder Probleme zu beheben.



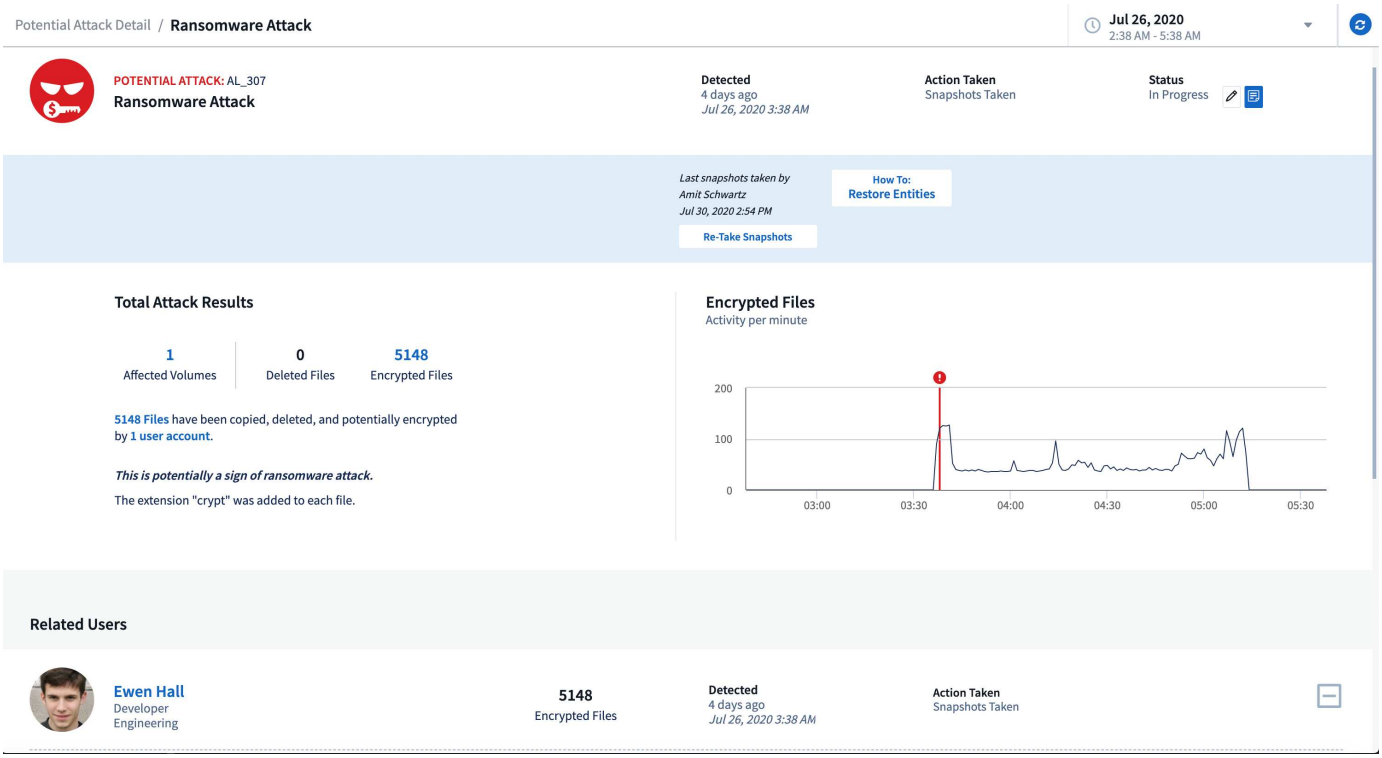
Juli 2020

Cloud Secure *Snapshot erstellen* Aktion

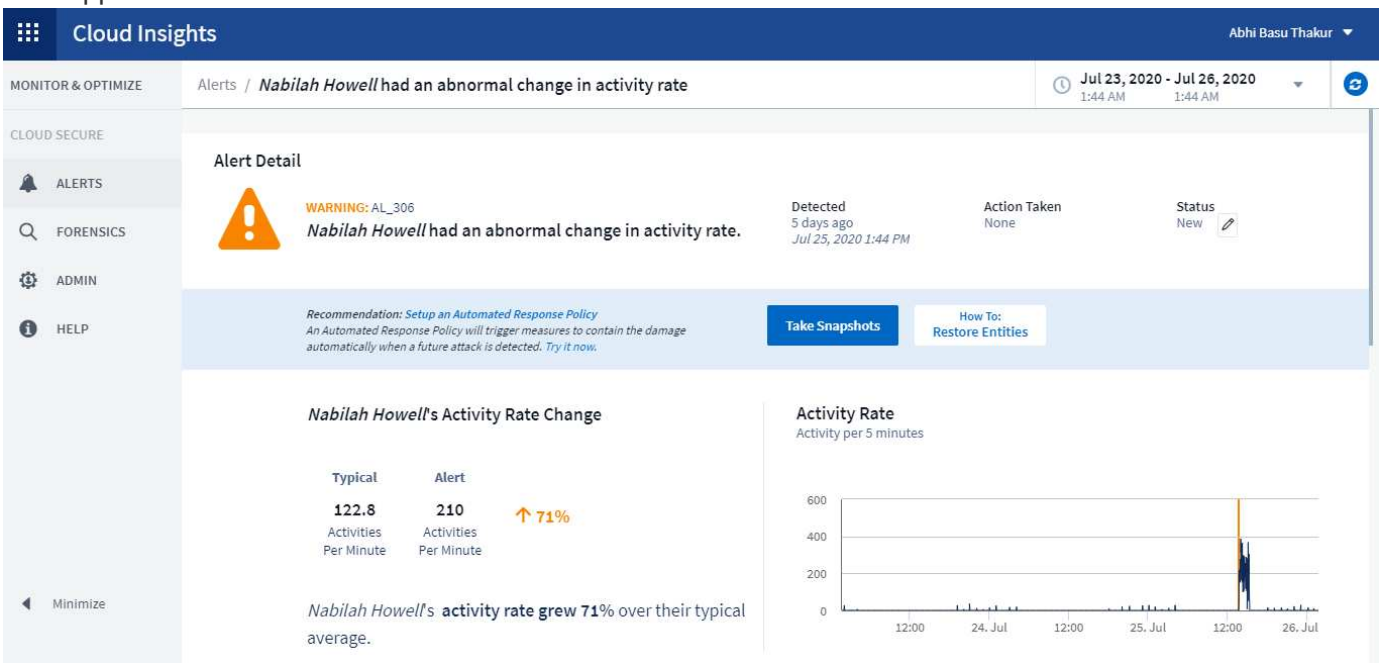
Cloud Secure schützt Ihre Daten, indem es automatisch einen Snapshot erstellt, wenn böswillige Aktivitäten erkannt werden, und so gewährleistet, dass Ihre Daten sicher gesichert werden.

Sie können automatisierte Reaktionsrichtlinien definieren, die einen Snapshot erstellen, wenn ein Ransomware-Angriff oder andere ungewöhnliche Benutzeraktivitäten erkannt werden. Sie können auch manuell einen Schnappschuss von der Warnseite aus erstellen.

Automatischer Schnappschuss
erstellt:



Manueller Schnappschuss:



Metrik-/Zähleraktualisierungen

Die folgenden Kapazitätszähler stehen zur Verwendung in der Cloud Insights -Benutzeroberfläche und der REST-API zur Verfügung. Bisher waren diese Zähler nur für das Data Warehouse/Reporting verfügbar.

Objekttyp	Schalter
Storage	Kapazität – freie Rohkapazität Kapazität – fehlgeschlagene Rohkapazität

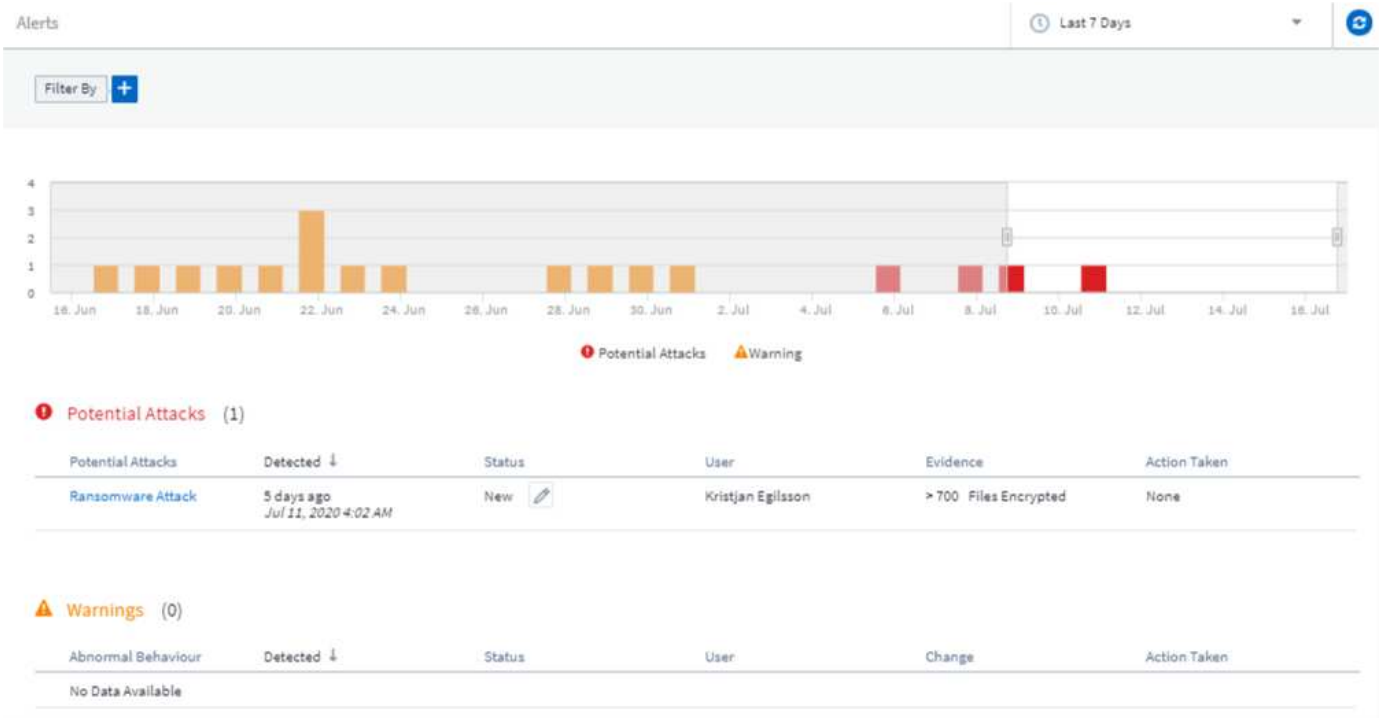
Objekttyp	Schalter
Speicherpool	Datenkapazität – Verwendete Datenkapazität – Gesamte sonstige Kapazität – Verwendete sonstige Kapazität – Gesamtkapazität – Rohkapazität – Weiches Limit
Internes Volumen	Datenkapazität – Verwendete Datenkapazität – Gesamt Andere Kapazität – Verwendete Andere Kapazität – Gesamt Gespeicherte Klonkapazität – Gesamt

Cloud Secure – Erkennung potenzieller Angriffe

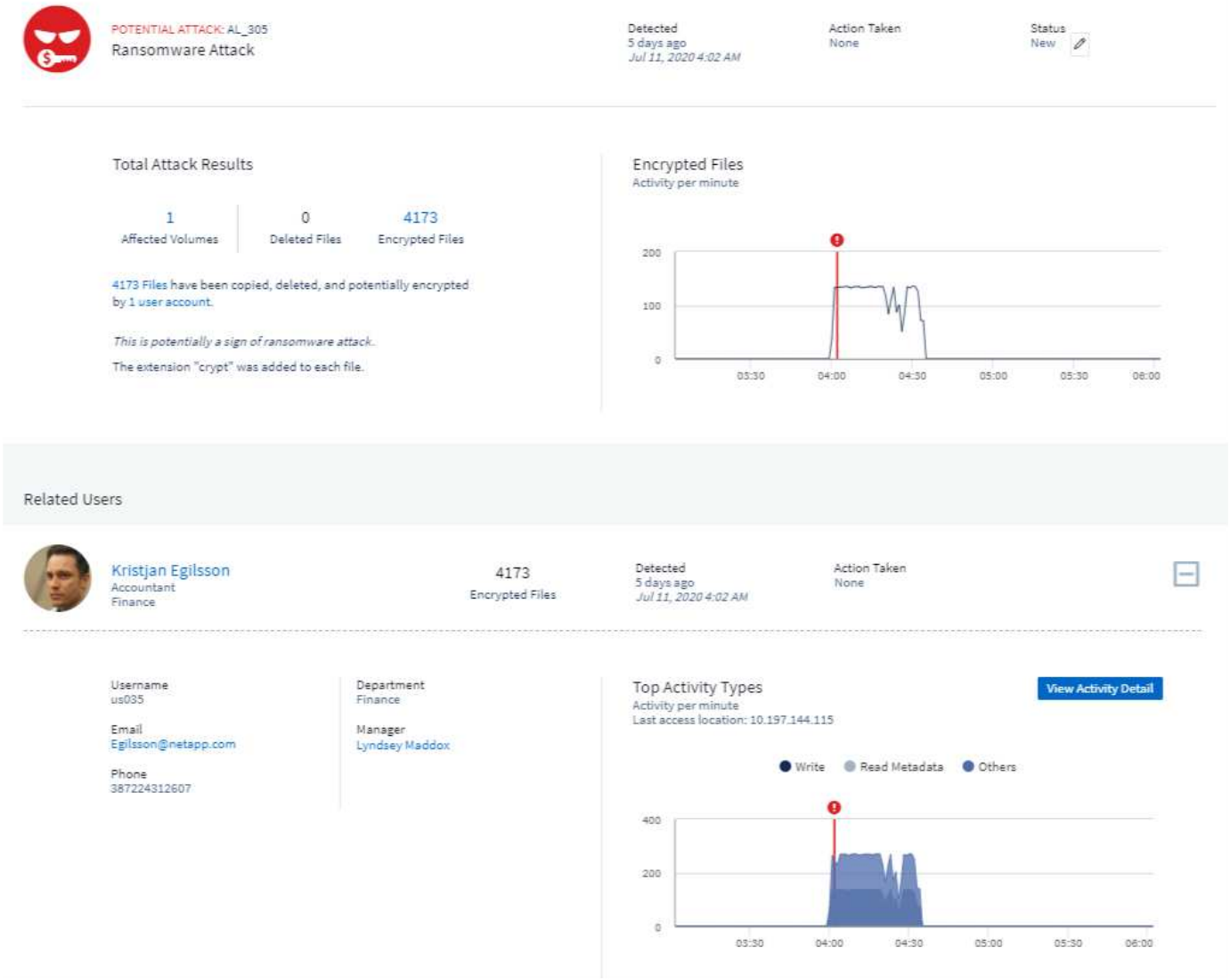
Cloud Secure erkennt jetzt potenzielle Angriffe wie Ransomware. Klicken Sie auf der Seite mit der Liste der Warnungen auf eine Warnung, um eine Detailseite mit folgendem Inhalt zu öffnen:

- Zeitpunkt des Angriffs
- Zugehörige Benutzer- und Dateiaktivität
- Ergriffene Maßnahmen
- Zusätzliche Informationen zur Unterstützung bei der Aufspürung möglicher Sicherheitsverletzungen

Warnseite mit Hinweis auf einen möglichen Ransomware-Angriff:



Detailseite zum potenziellen Ransomware-Angriff:



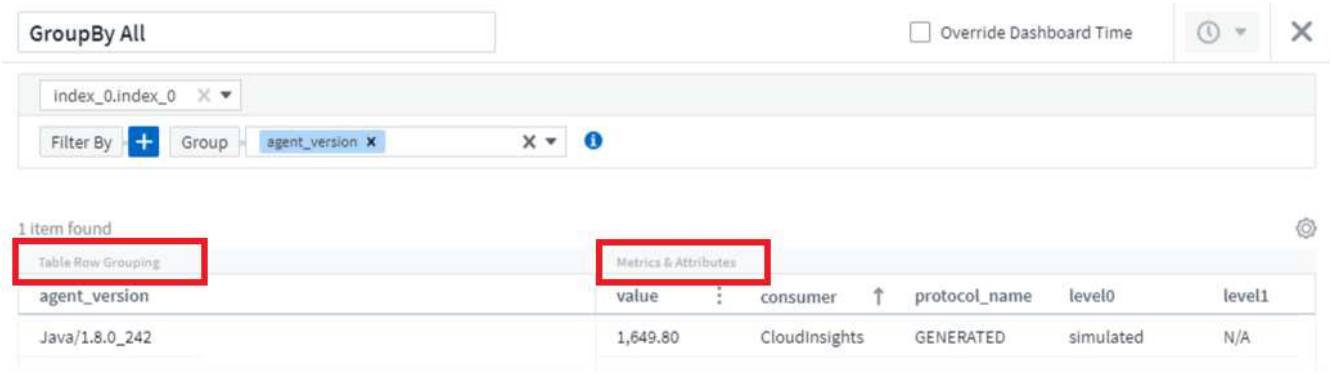
Abonnieren Sie die Premium Edition über AWS

Während Ihrer Testphase von Cloud Insights können Sie"Selbstabonnement" über AWS Marketplace entweder zur Cloud Insights Standard Edition oder Premium Edition. Bisher konnten Sie über AWS Marketplace nur ein Selbstabonnement für die Standard Edition abschließen.

Erweitertes Tabellen-Widget

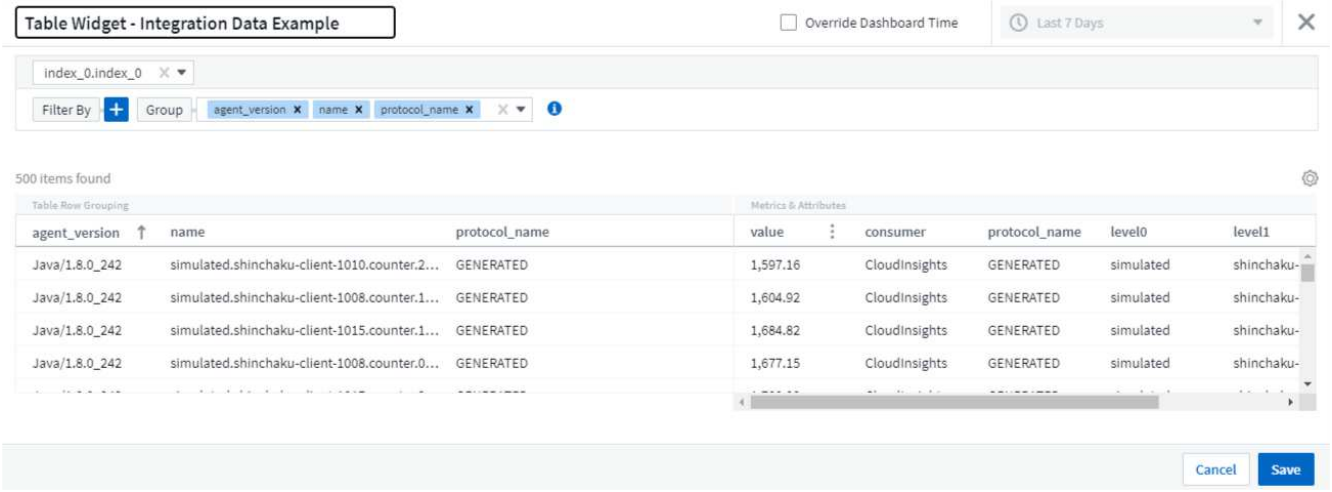
Das Tabellen-Widget der Dashboard-/Asset-Seite enthält die folgenden Verbesserungen:

- „Split-Screen“-Ansicht: Tabellen-Widgets zeigen das Objekt/die Gruppierung auf der linken Seite und die Objektdaten (Attribute/Metriken) auf der rechten Seite an.



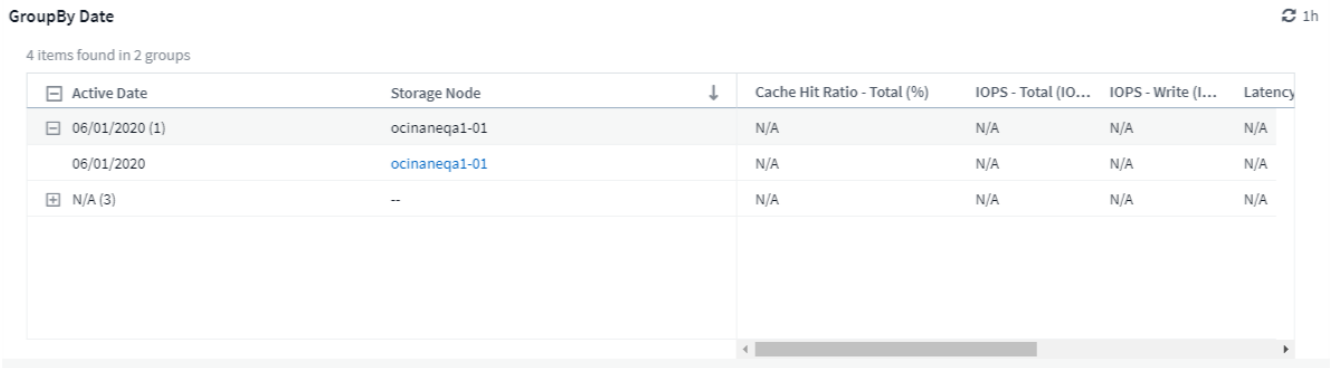
- Gruppierung mehrerer Attribute: Für Integrationsdaten (Kubernetes, ONTAP Advanced Metrics, Docker usw.) können Sie mehrere Attribute zur Gruppierung auswählen. Die Daten werden entsprechend den von Ihnen gewählten Gruppierungsattributen angezeigt.

  Gruppierung mit Integrationsdaten (im Bearbeitungsmodus angezeigt):



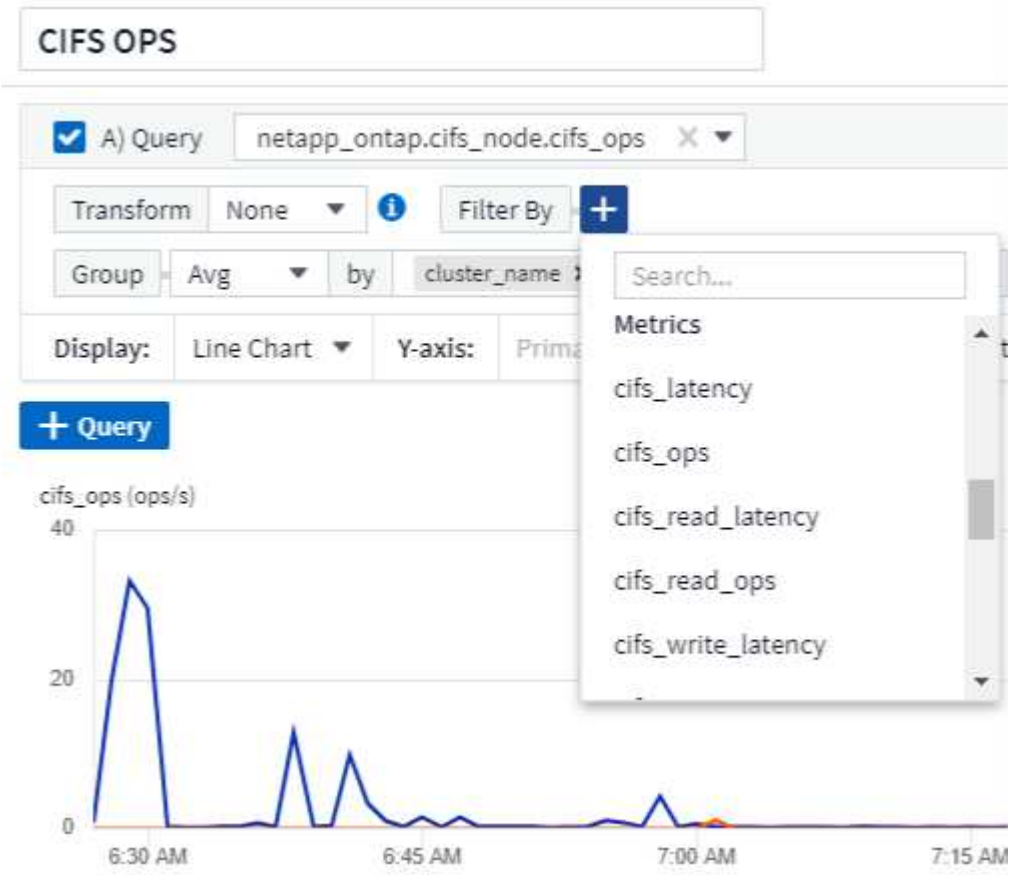
- Die Gruppierung von Infrastrukturdaten (Speicher, EC2, VM, Ports usw.) erfolgt wie zuvor über ein einzelnes Attribut. Beim Gruppieren nach einem Attribut, das nicht das Objekt ist, können Sie in der Tabelle die Gruppenzeile erweitern, um alle Objekte innerhalb der Gruppe anzuzeigen.

  Gruppierung mit Infrastrukturdaten (im Anzeigemodus angezeigt):

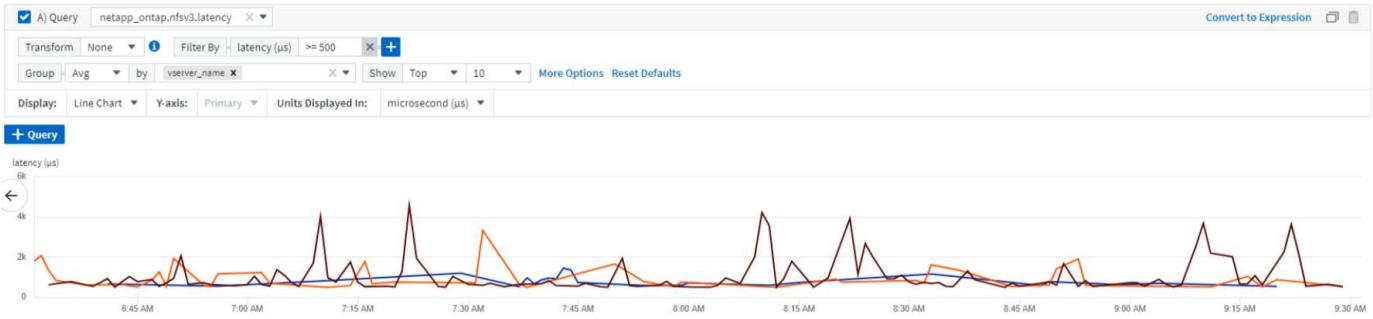


Metrikfilterung

Zusätzlich zum Filtern nach den Attributen eines Objekts in einem Widget können Sie jetzt auch nach Metriken filtern.



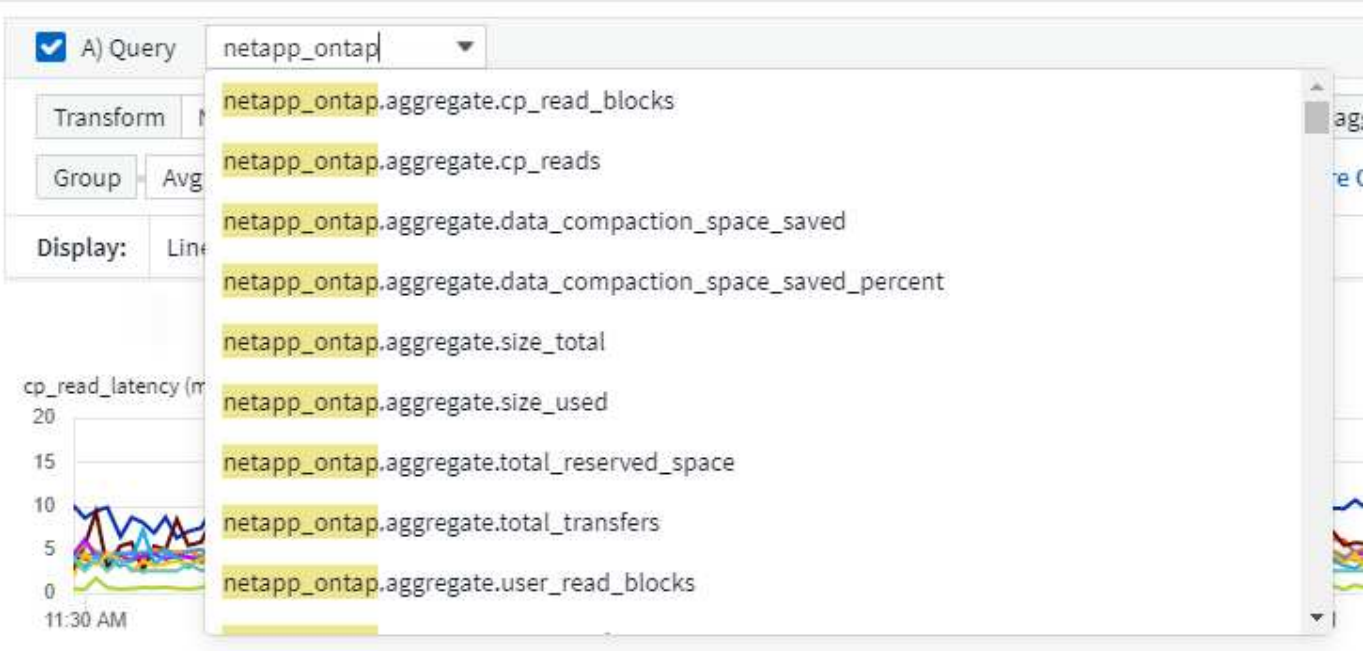
Beim Arbeiten mit Integrationsdaten (Kubernetes, ONTAP Advanced Data usw.) entfernt die Metrikfilterung die einzelnen/nicht übereinstimmenden Datenpunkte aus der dargestellten Datenreihe. Bei Infrastrukturdaten (Speicher, VM, Ports usw.) hingegen arbeiten Filter mit dem aggregierten Wert der Datenreihe und entfernen möglicherweise das gesamte Objekt aus dem Diagramm.



ONTAP Advanced Counter-Daten

Cloud Insights nutzt die ONTAP-spezifischen **Advanced Counter Data** von NetApp, die eine Vielzahl von Zählern und Metriken bereitstellen, die von ONTAP -Geräten erfasst wurden. ONTAP Advanced Counter Data ist für alle NetApp ONTAP -Kunden verfügbar. Diese Metriken ermöglichen eine benutzerdefinierte und umfassende Visualisierung in Cloud Insights -Widgets und Dashboards.

Sie können die erweiterten ONTAP -Zähler finden, indem Sie in der Abfrage des Widgets nach „netapp_ontap“ suchen und einen der Zähler auswählen.



Sie können Ihre Suche verfeinern, indem Sie zusätzliche Teile des Zählernamens eingeben. Beispiel:

- *Leben*
- *Aggregat*
- *offbox_vscan_server*
- und mehr

Bitte beachten Sie Folgendes:

- Die erweiterte Datenerfassung wird für neue ONTAP Datensammler standardmäßig aktiviert. Um die erweiterte Datenerfassung für Ihre vorhandenen ONTAP Datensammler zu aktivieren, bearbeiten Sie den Datensammler und erweitern Sie den Abschnitt „Erweiterte Konfiguration“.
- Die erweiterte Datenerfassung ist für 7-Mode ONTAP nicht verfügbar.

Erweiterte Zähler-Dashboards

Cloud Insights enthält eine Vielzahl vorgefertigter Dashboards, die Ihnen den Einstieg in die Visualisierung von ONTAP Advanced Counters für Themen wie *Aggregate Performance*, *Volume Workload*, *Prozessoraktivität* und mehr erleichtern. Wenn Sie mindestens einen ONTAP Datensammler konfiguriert haben, können diese aus der Dashboard-Galerie auf jeder Dashboard-Listenseite importiert werden.

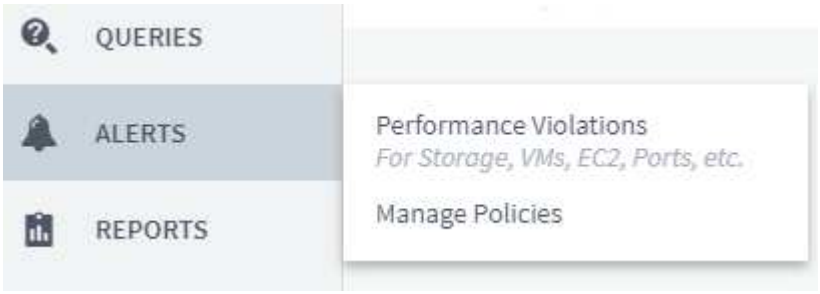
Weitere Informationen

Weitere Informationen zu ONTAP Advanced Data finden Sie unter den folgenden Links:

- https://mysupport.netapp.com/site/tools/tool-eula/netapp-harvest(Hinweis: Sie müssen sich beim NetApp -Support anmelden)
- https://nabox.org/faq/

Menü „Richtlinien und Verstöße“

Leistungsrichtlinien und -verstöße finden Sie jetzt im Menü **Warnungen**. Die Richtlinien- und Verstoßfunktionen bleiben unverändert.



Aktualisierter Telegraf-Agent

Der Agent für die Aufnahme von Telegraf-Integrationsdaten wurde aktualisiert auf"Version 1.14" , das Fehlerbehebungen, Sicherheitsfixes und neue Plugins enthält.

Hinweis: Beim Konfigurieren eines Kubernetes-Datensammlers auf der Kubernetes-Plattform wird im Protokoll möglicherweise der Fehler „HTTP-Status 403 Verboten“ angezeigt, da im Attribut „clusterrole“ keine ausreichenden Berechtigungen vorhanden sind.

Um dieses Problem zu umgehen, fügen Sie dem Abschnitt „*rules:*“ der Clusterrolle „Endpoint-Access“ die folgenden hervorgehobenen Zeilen hinzu und starten Sie dann die Telegraf-Pods neu.

```
rules:
- apiGroups:
  - ""
  - apps
  - autoscaling
  - batch
  - extensions
  - policy
  - rbac.authorization.k8s.io
  attributeRestrictions: null
  resources:
  - nodes/metrics
  - nodes/proxy     <== Add this line
  - nodes/stats
  - pods            <== Add this line
  verbs:
  - get
  - list            <== Add this line
```

Juni 2020

Vereinfachte Fehlerberichterstattung des Datensammlers

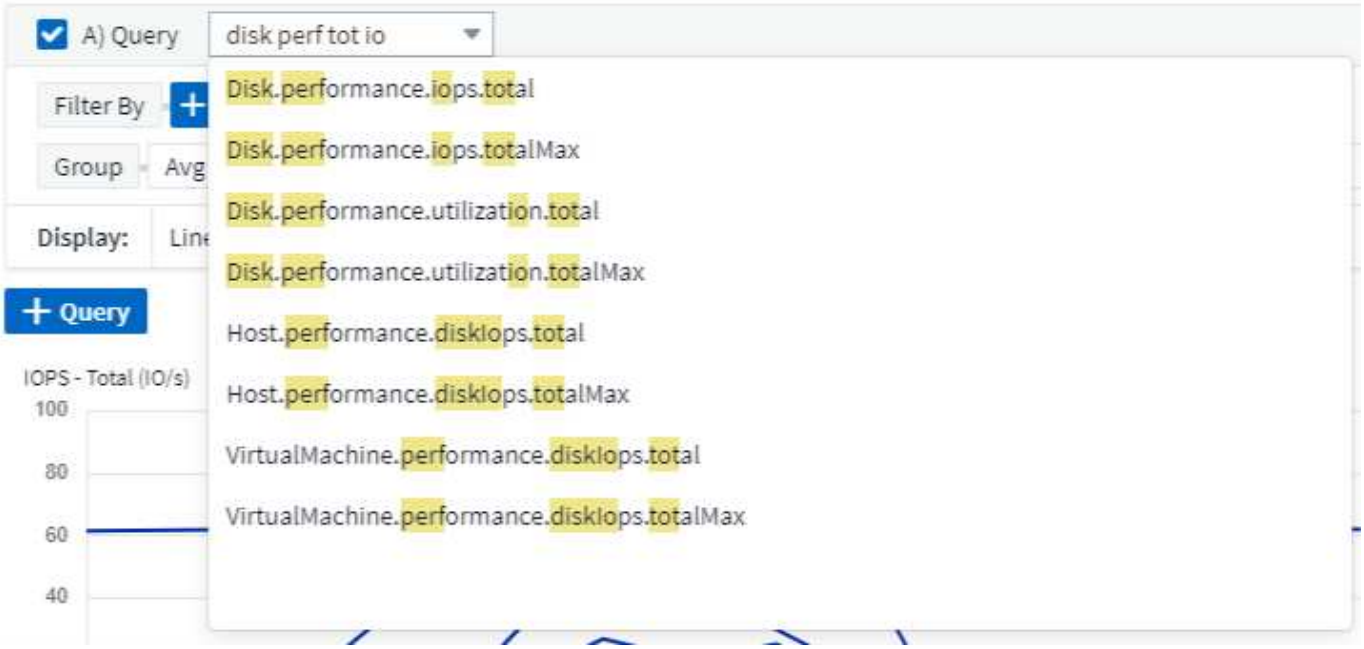
Das Melden eines Datensammlerfehlers ist mit der Schaltfläche *Fehlerbericht senden* auf der Datensammlerseite einfacher. Durch Klicken auf die Schaltfläche werden grundlegende Informationen zum Fehler an NetApp gesendet und eine Untersuchung des Problems veranlasst. Nach dem Drücken bestätigt Cloud Insights , dass NetApp benachrichtigt wurde, und die Schaltfläche „Fehlerbericht“ wird deaktiviert, um anzuzeigen, dass ein Fehlerbericht für diesen Datensammler gesendet wurde. Die Schaltfläche bleibt deaktiviert, bis die Browserseite aktualisiert wird.

Widget-Verbesserungen

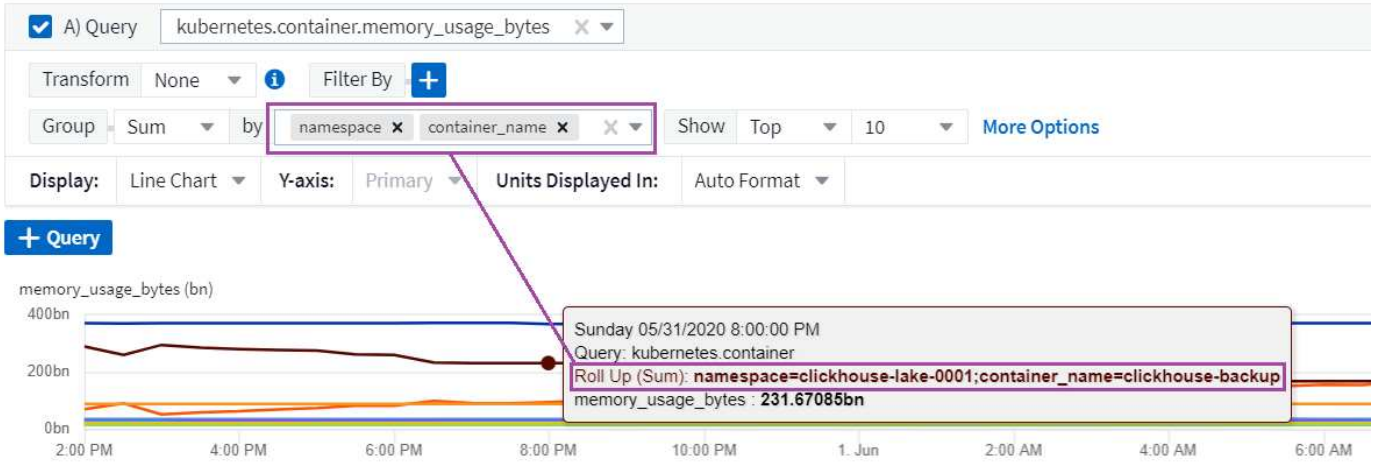
Die folgenden Verbesserungen wurden an Dashboard-Widgets vorgenommen. Diese Verbesserungen gelten als Vorschaufunktionen und sind möglicherweise nicht für alle Cloud Insights -Umgebungen verfügbar.

- Neue Objekt-/Metrikauswahl: Objekte (Speicher, Festplatte, Ports, Knoten usw.) und die zugehörigen Metriken (IOPS, Latenz, CPU-Anzahl usw.) sind jetzt in Widgets in einem einzigen umfassenden Dropdown-Menü mit leistungsstarker Suchfunktion verfügbar. Sie können mehrere Teilbegriffe in die

Dropdown-Liste eingeben und Cloud Insights listet alle Objektmetriken auf, die diesen Begriffen entsprechen.



- Gruppierung mehrerer Tags: Wenn Sie mit Integrationsdaten (Kubernetes usw.) arbeiten, können Sie die Daten nach mehreren Tags/Attributen gruppieren. Beispiel: Summieren Sie die Speichernutzung nach Kubernetes-Namespace und Containername.



Mai 2020

Berichterstellung für Benutzerrollen

Für die Berichterstattung wurden die folgenden Rollen hinzugefügt:

- Cloud Insights -Verbraucher: können Berichte ausführen und anzeigen
- Cloud Insights -Autoren: können die Consumer-Funktionen ausführen sowie Berichte und Dashboards erstellen und verwalten

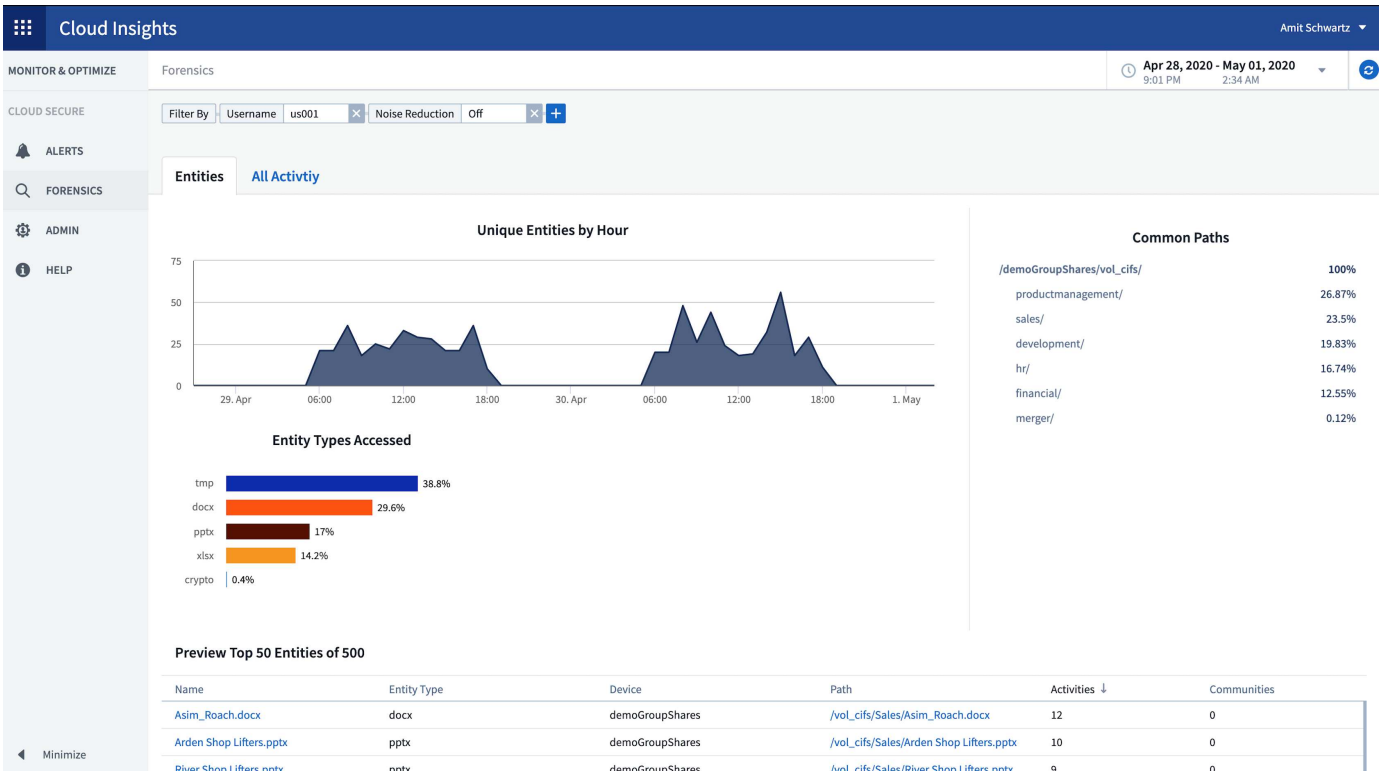
- Cloud Insights -Administratoren: können die Autorenfunktionen sowie alle administrativen Aufgaben ausführen

Cloud Secure -Sicherheitsupdates

Cloud Insights umfasst die folgenden aktuellen Cloud Secure -Änderungen.

Auf der Seite „Forensik > Aktivitätsforensik“ bieten wir zwei Ansichten zum Analysieren und Untersuchen der Benutzeraktivität:

- Aktivitätsansicht, konzentriert sich auf die Benutzeraktivität (Welche Operation? Wo wird es aufgeführt?)
- Entitätsansicht, mit Fokus auf den Dateien, auf die der Benutzer zugegriffen hat.

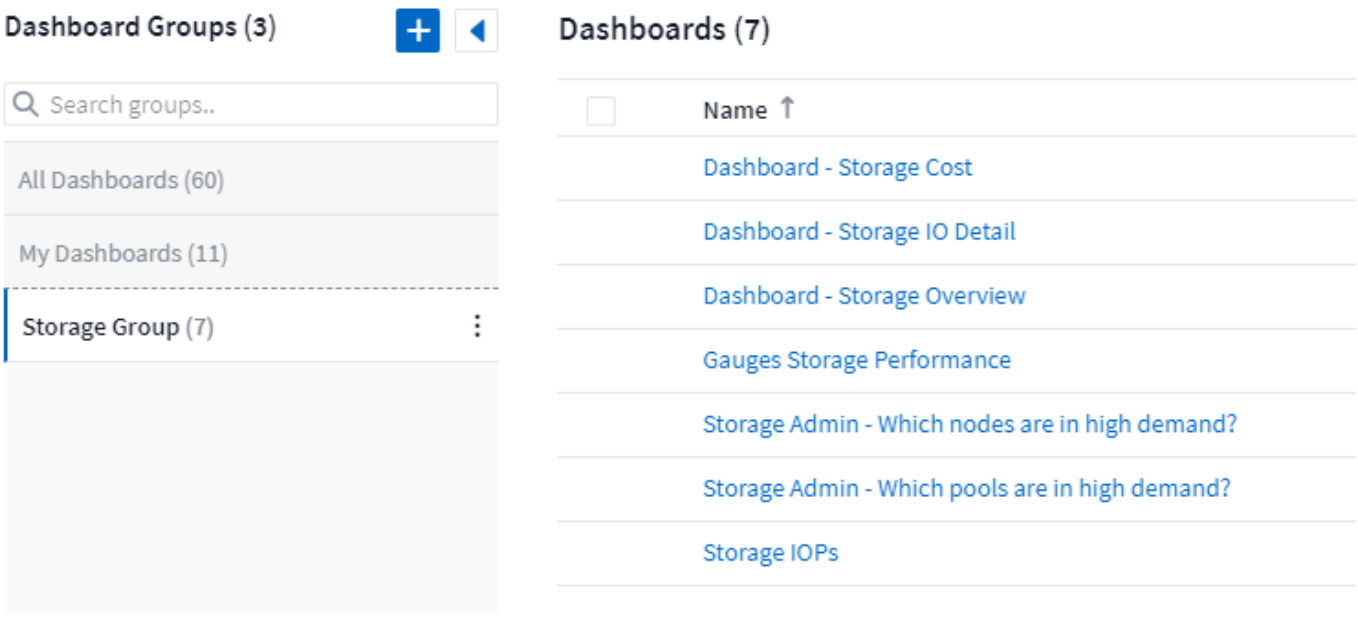


Darüber hinaus enthält die E-Mail-Benachrichtigung jetzt einen direkten Link zur Warnseite.

Dashboard-Gruppierung

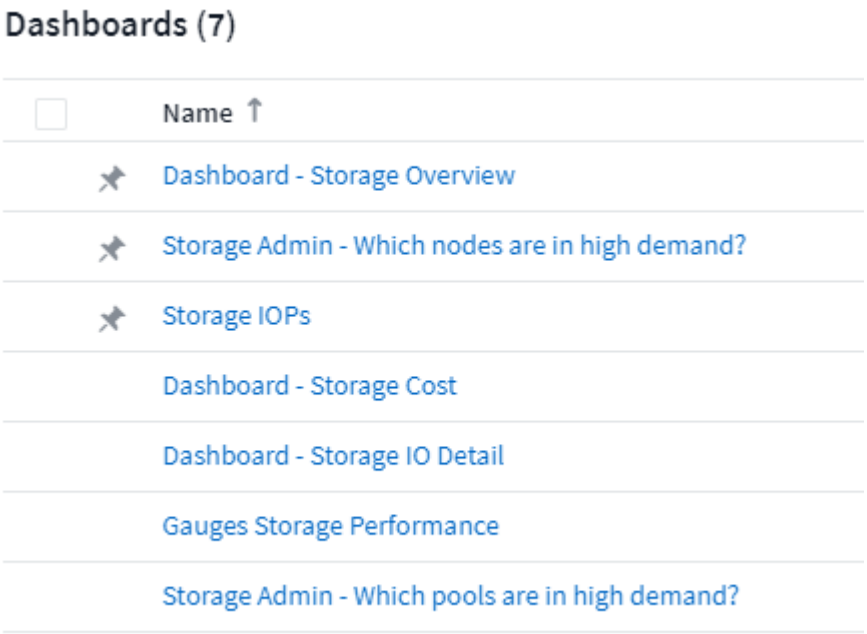
Dashboard-Gruppierung ermöglicht eine bessere"Verwaltung von Dashboards" die für Sie relevant sind. Sie können einer Gruppe verwandte Dashboards hinzufügen, um beispielsweise Ihren Speicher oder Ihre virtuellen Maschinen aus einer Hand zu verwalten.

Gruppen werden pro Benutzer individuell angepasst, sodass die Gruppen einer Person sich von denen einer anderen Person unterscheiden können. Sie können so viele Gruppen haben, wie Sie benötigen, mit so wenigen oder so vielen Dashboards in jeder Gruppe, wie Sie möchten.



Dashboard-Pinnung

Sie können Dashboards anheften, sodass Favoriten immer oben in der Liste angezeigt werden.



TV-Modus und automatische Aktualisierung

"TV-Modus und automatische Aktualisierung"ermöglichen die Anzeige von Daten nahezu in Echtzeit auf einem Dashboard oder einer Asset-Seite:

- Der **TV-Modus** bietet eine übersichtliche Anzeige; das Navigationsmenü ist ausgeblendet, sodass mehr Platz auf dem Bildschirm für die Anzeige Ihrer Daten zur Verfügung steht.
- Daten in Widgets auf Dashboards und Asset-Landingpages werden gemäß einem Aktualisierungsintervall (mindestens alle 10 Sekunden) **automatisch aktualisiert**, das durch den ausgewählten Dashboard-

Zeitbereich (oder den Widget-Zeitbereich, wenn dieser so eingestellt ist, dass er die Dashboard-Zeit überschreibt) bestimmt wird.

In Kombination bieten der TV-Modus und die automatische Aktualisierung eine Live-Ansicht Ihrer Cloud Insights -Daten, perfekt für nahtlose Demonstrationen oder die interne Überwachung.

April 2020

Neue Zeitbereichsauswahl im Dashboard

Die Zeitbereichsauswahl für Dashboards und andere Cloud Insights-Seiten umfasst jetzt *Letzte 1 Stunde* und *Letzte 15 Minuten*.

Cloud Secure -Sicherheitsupdates

Cloud Insights umfasst die folgenden aktuellen Cloud Secure -Änderungen.

- Bessere Erkennung von Änderungen an Datei- und Ordnermetadaten, um festzustellen, ob der Benutzer die Berechtigung, den Eigentümer oder die Gruppeneigentümerschaft geändert hat.
- Exportieren Sie den Benutzeraktivitätsbericht in CSV.

Cloud Secure überwacht und prüft alle Benutzerzugriffe auf Dateien und Ordner. Mithilfe der Aktivitätsüberwachung können Sie interne Sicherheitsrichtlinien einhalten, externe Compliance-Anforderungen wie PCI, DSGVO und HIPAA erfüllen und Untersuchungen zu Datenschutzverletzungen und Sicherheitsvorfällen durchführen.

Standard-Dashboard-Zeit

Der Standardzeitraum für Dashboards beträgt jetzt 3 Stunden statt 24 Stunden.

Optimierte Aggregationszeiten

Optimiert"Zeitaggregation" Intervalle in Zeitreihen-Widgets (Linien-, Spline-, Flächen- und gestapelte Flächendiagramme) sind für 3-Stunden- und 24-Stunden-Dashboard-/Widget-Zeiträume häufiger, was eine schnellere Diagrammerstellung der Daten ermöglicht.

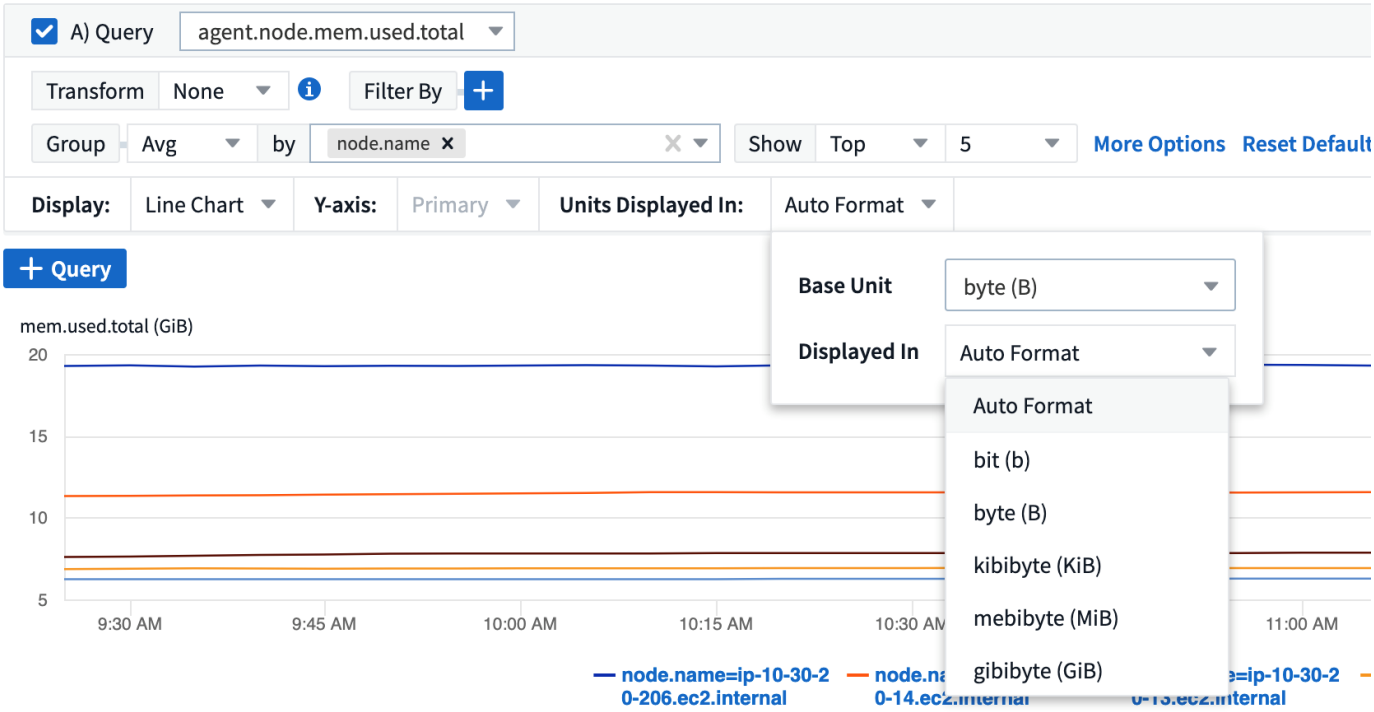
- Der 3-Stunden-Zeitraum wird auf ein 1-Minuten-Aggregationsintervall optimiert. Zuvor waren dies 5 Minuten.
- Der 24-Stunden-Zeitraum wird auf ein 30-Minuten-Aggregationsintervall optimiert. Zuvor war dies 1 Stunde.

Sie können die optimierte Aggregation weiterhin überschreiben, indem Sie ein benutzerdefiniertes Intervall festlegen.

Automatische Formatierung der Anzeigeeinheit

In den meisten Widgets kennt Cloud Insights die Basiseinheit, in der Werte angezeigt werden, zum Beispiel *Megabyte*, *Tausende*, *Prozent*, *Millisekunden (ms)* usw., und jetzt"formatiert automatisch" das Widget auf die am besten lesbare Einheit. Beispielsweise würde ein Datenwert von 1.234.567.890 Bytes automatisch auf 1,23 Gibibyte formatiert. In vielen Fällen kennt Cloud Insights das beste Format für die erfassten Daten. In Fällen, in

denen das beste Format nicht bekannt ist, oder in Widgets, bei denen Sie die automatische Formatierung überschreiben möchten, können Sie das gewünschte Format auswählen.

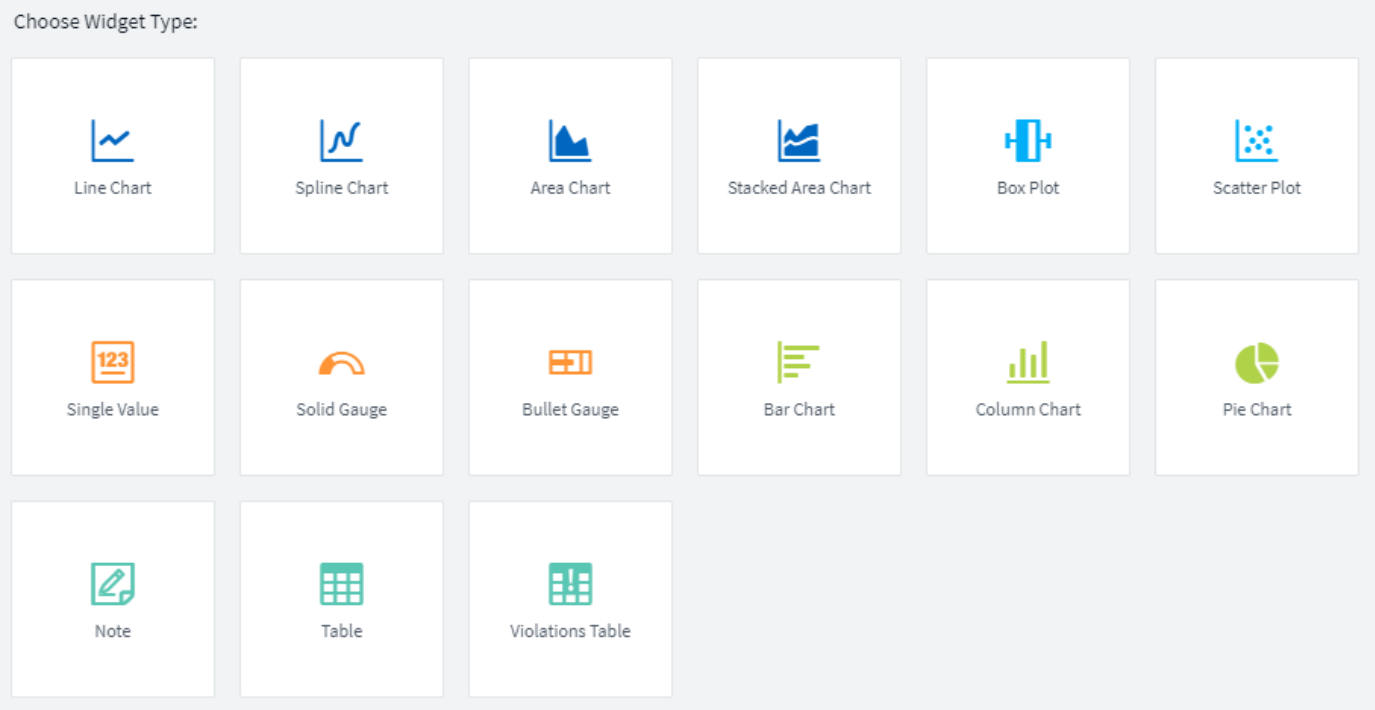


Anmerkungen mithilfe der API importieren

Mit der leistungsstarken API der Cloud Insights Premium Edition können Sie jetzt"Anmerkungen importieren" und weisen Sie sie mithilfe einer CSV-Datei Objekten zu. Auf die gleiche Weise können Sie auch Anwendungen importieren und Geschäftseinheiten zuweisen.

Einfacherer Widget-Selektor

Das Hinzufügen von Widgets zu Dashboards und Asset-Landingpages wird durch einen neuen Widget-Selektor vereinfacht, der alle Widget-Typen in einer einzigen Übersicht anzeigt. Der Benutzer muss also nicht mehr durch eine Liste von Widget-Typen scrollen, um den gewünschten Typ zu finden. Zusammengehörige Widgets werden im neuen Selektor farblich koordiniert und nach Nähe gruppiert.



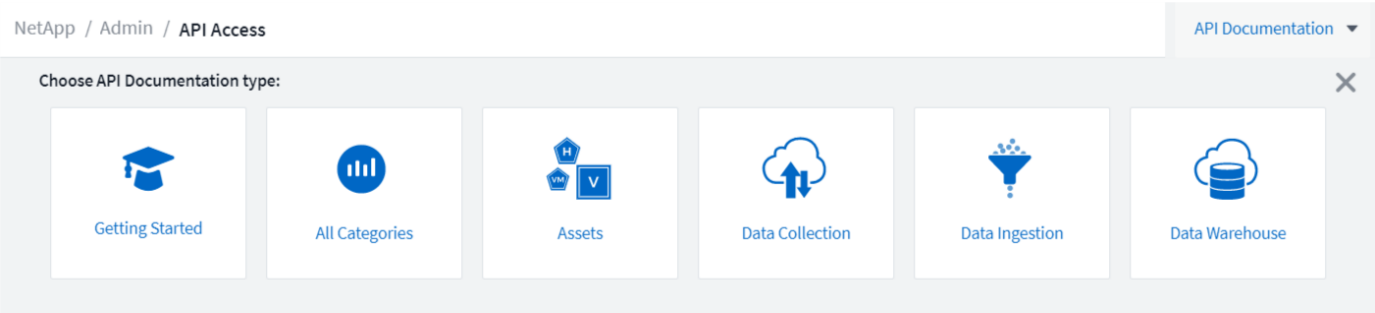
Februar 2020

API mit Premium Edition

Cloud Insights Premium Edition enthält eine"leistungsstarke API" die zur Integration von Cloud Insights in andere Anwendungen wie CMDBs oder andere Ticketsysteme verwendet werden können.

Detaillierte, Swagger-basierte Informationen finden Sie unter **Admin > API-Zugriff** unter dem Link **API-Dokumentation**. Swagger bietet eine kurze Beschreibung und Nutzungsinformationen für die API und ermöglicht Ihnen, jede API in Ihrer Umgebung auszuprobieren.

Die Cloud Insights -API verwendet Zugriffstoken, um berechtigungsbasierten Zugriff auf API-Kategorien wie ASSETS oder COLLECTION bereitzustellen.



Erste Abfrage nach dem Hinzufügen eines Datensammlers

Zuvor hat Cloud Insights nach der Konfiguration eines neuen Datensammlers den Datensammler sofort abgefragt, um *Inventar_daten zu sammeln, hat jedoch bis zum konfigurierten Leistungsabfrageintervall (normalerweise 15 Minuten) gewartet, um erste _Leistungs_daten zu sammeln. Anschließend wurde ein*

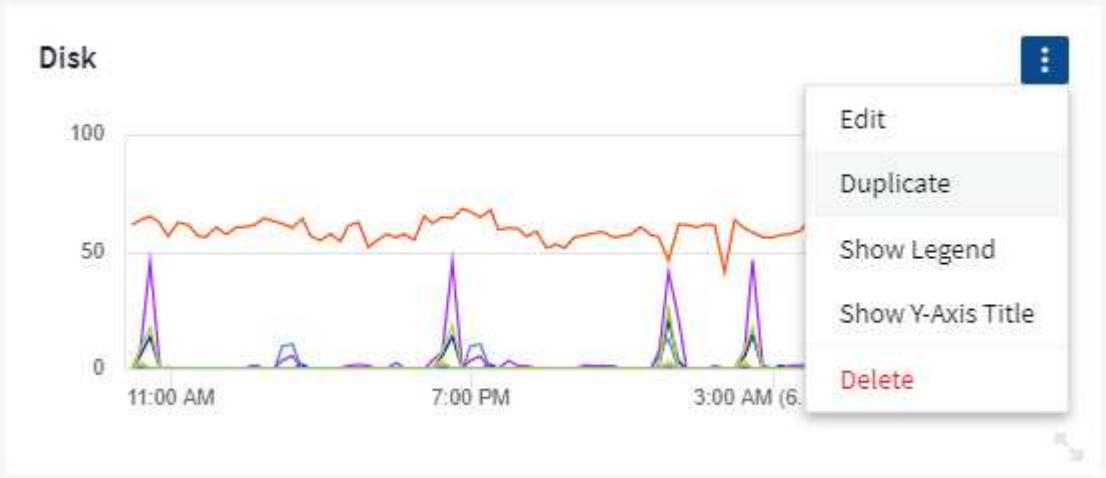
weiteres Intervall abgewartet, bevor die zweite Leistungsabfrage gestartet wurde. Dies bedeutete, dass es bis zu _30 Minuten dauern würde, bis aussagekräftige Daten von einem neuen Datensammler abgerufen wurden.

Datensammler"Umfrage" wurde erheblich verbessert, sodass die erste Leistungsabfrage unmittelbar nach der Inventarabfrage erfolgt und die zweite Leistungsabfrage innerhalb weniger Sekunden nach Abschluss der ersten Leistungsabfrage. Dadurch kann Cloud Insights innerhalb kürzester Zeit nützliche Daten auf Dashboards und Diagrammen anzeigen.

Dieses Polling-Verhalten tritt auch nach der Bearbeitung der Konfiguration eines vorhandenen Datensammlers auf.

Einfachere Widget-Duplizierung

Es ist einfacher denn je, eine Kopie eines Widgets auf einem Dashboard oder einer Zielseite zu erstellen. Klicken Sie im Dashboard-Bearbeitungsmodus auf das Menü im Widget und wählen Sie **Duplizieren**. Der Widget-Editor wird gestartet und ist bereits mit der Konfiguration des Original-Widgets und dem Suffix „Kopie“ im Widget-Namen ausgefüllt. Sie können problemlos alle erforderlichen Änderungen vornehmen und das neue Widget speichern. Das Widget wird unten in Ihrem Dashboard platziert und Sie können es nach Bedarf positionieren. Denken Sie daran, Ihr Dashboard zu speichern, wenn alle Änderungen abgeschlossen sind.



Einmaliges Anmelden (SSO)

Mit Cloud Insights Premium Edition können Administratoren Folgendes aktivieren: *"Einmaliges Anmelden" * (SSO) Zugriff auf Cloud Insights für alle Benutzer in ihrer Unternehmensdomäne, ohne sie einzeln einladen zu müssen. Wenn SSO aktiviert ist, kann sich jeder Benutzer mit derselben Domänen-E-Mail-Adresse mit seinen Unternehmensanmeldeinformationen bei Cloud Insights anmelden.

SSO ist nur in der Cloud Insights Premium Edition verfügbar und muss konfiguriert werden, bevor es für Cloud Insights aktiviert werden kann. Die SSO-Konfiguration umfasst"Identitätsföderation" über NetApp Cloud Central. Durch die Föderation können Single-Sign-On-Benutzer mit Anmeldeinformationen aus Ihrem Unternehmensverzeichnis auf Ihre NetApp Cloud Central-Konten zugreifen.

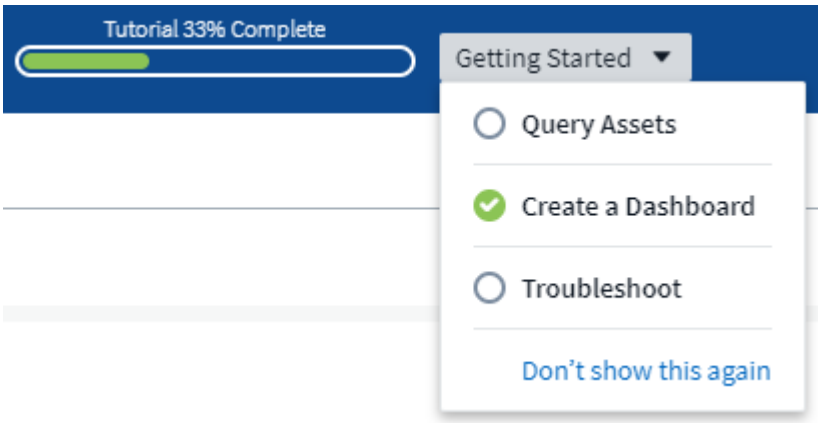
Januar 2020

Swagger-Dokumentation für REST-API

Swagger erklärt jede verfügbare REST-API in Cloud Insights sowie deren Verwendung und Syntax. Informationen zu Cloud Insights APIs finden Sie in"Dokumentation" .

Fortschrittsbalken für Feature-Tutorials

Die Checkliste für die Funktions-Tutorials wurde in das obere Banner verschoben und verfügt jetzt über eine Fortschrittsanzeige. Tutorials stehen jedem Benutzer zur Verfügung, bis sie geschlossen werden, und sind immer in Cloud Insights verfügbar."Dokumentation" .



Änderungen an der Erfassungseinheit

Wenn Sie eine Acquisition Unit (AU) auf einem Host oder einer VM installieren, die denselben Namen wie eine bereits installierte AU hat, stellt Cloud Insights einen eindeutigen Namen sicher, indem an den AU-Namen „_1“, „_2“ usw. angehängt wird. Dies ist auch der Fall, wenn Sie eine AU von derselben VM deinstallieren und neu installieren, ohne sie zuerst aus Cloud Insights zu entfernen. Möchten Sie einen ganz anderen AU-Namen? Kein Problem; AUs können nach der Installation umbenannt werden.

Optimierte Zeitaggregation in Widgets

In Widgets können Sie zwischen einem *optimierten* Zeitaggregationsintervall oder einem von Ihnen festgelegten *benutzerdefinierten* Intervall wählen. Durch die optimierte Aggregation wird automatisch das richtige Zeitintervall basierend auf dem ausgewählten Dashboard-Zeitbereich (oder Widget-Zeitbereich, wenn die Dashboard-Zeit überschrieben wird) ausgewählt. Das Intervall ändert sich dynamisch, wenn der Zeitbereich des Dashboards oder Widgets geändert wird.

Vereinfachter Prozess „Erste Schritte mit Cloud Insights“

Der Prozess für den Einstieg in die Verwendung von Cloud Insights wurde vereinfacht, um Ihre Ersteinrichtung reibungsloser und einfacher zu gestalten. Wählen Sie einfach einen ersten Datensammler aus und folgen Sie den Anweisungen. Cloud Insights führt Sie durch die Konfiguration des Datensammlers und aller erforderlichen Agenten oder Erfassungseinheiten. In den meisten Fällen werden sogar ein oder mehrere erste Dashboards importiert, sodass Sie schnell Einblicke in Ihre Umgebung gewinnen können (bitte rechnen Sie jedoch mit bis zu 30 Minuten, bis Cloud Insights aussagekräftige Daten erfasst hat).

Weitere Verbesserungen:

- Die Installation der Erfassungseinheit ist einfacher und läuft schneller.

- Die alphabetische Auswahl der Datensammler erleichtert Ihnen das Auffinden des gesuchten Datensammlers.
- Die Einrichtungsanweisungen für den verbesserten Datensammler sind leichter zu befolgen.
- Erfahrene Benutzer können den Einstiegsprozess mit einem Mausklick überspringen.
- Ein neuer Fortschrittsbalken zeigt Ihnen, wo Sie sich im Prozess befinden.

Onboarding von Data Infrastructure Insights

Bevor Sie mit der Arbeit mit Data Infrastructure Insights beginnen können, müssen Sie sich beim * NetApp Console*-Portal anmelden. Wenn Sie bereits über ein NetApp Console -Login verfügen, können Sie in wenigen Schritten eine kostenlose Testversion von Data Infrastructure Insights starten.

Erstellen Ihres NetApp Console

Um mit den Cloud-Diensten von NetApp zu beginnen, gehen Sie zu"* NetApp Console*" und klicken Sie auf **Erste Schritte**.

- Wenn Sie sich noch nicht angemeldet haben, wählen Sie **Anmelden**
- Geben Sie eine gültige geschäftliche E-Mail-Adresse ein und wählen Sie ein Passwort.
- Geben Sie Ihren Firmennamen und Ihren vollständigen Namen ein.
- Akzeptieren Sie die Allgemeinen Geschäftsbedingungen und wählen Sie **Weiter**.
- Die Konsole führt Sie durch die ersten Schritte.

Was ist, wenn ich bereits über eine NetApp Console verfüge?

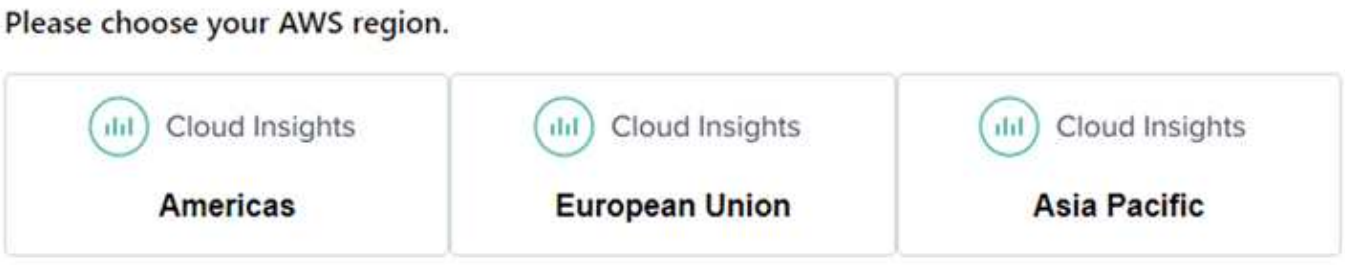
Sobald Sie ein NetApp Console -Konto haben, wählen Sie einfach **Anmelden** auf der"* NetApp Console*" Portalseite.

Geben Sie Ihre E-Mail-Adresse und Ihr Passwort ein. Sie werden dann zur Seite mit den Cloud-Angeboten von NetApp weitergeleitet.

Navigieren Sie zu **Analyse und Kontrolle > Beobachtbarkeit**, um mehr über Data Infrastructure Insights zu erfahren und/oder eine Demo anzufordern.

Starten Sie Ihre kostenlose Testversion von Data Infrastructure Insights

Wenn Sie sich zum ersten Mal bei Data Infrastructure Insights anmelden, klicken Sie unter dem Angebot von Data Infrastructure Insights auf **Kostenlose Testversion starten**. Data Infrastructure Insights führt Sie durch die Erstellung des Mandanten Ihres Unternehmens und wählt dabei auch die Region aus, in der sich Ihr Mandant befinden soll.



Sobald die Erstellung Ihres Mandanten abgeschlossen ist, melden Sie sich mit Ihren Konsolenanmeldeinformationen an und starten Sie Ihre kostenlose 30-Tage-Testversion von Data

Infrastructure Insights. Während dieser Testphase können Sie die Funktionen erkunden, die Data Infrastructure Insights zu bieten hat.

Während der kostenlosen Testphase können Sie"Starten Sie Ihr Abonnement" zu Data Infrastructure Insights jederzeit. Wenn Sie abonniert sind, können Sie die Data Infrastructure Insights -Funktionen basierend auf Ihrem aktuellen Abonnement nutzen.

Sign in und los gehts

Sobald Ihr Mandant erstellt wurde, können Sie sich jederzeit einfach beim NetApp Console Portal anmelden und zum"Cloud-Dienste" und wählen Sie **Zu Data Infrastructure Insights gehen**.

Sie können auch einen Browser direkt mit der URL Ihres Data Infrastructure Insights Mandanten öffnen, zum Beispiel:

```
 \https://<tenant-prefix>.c01.cloudinsights.netapp.com/
Die URL wird außerdem in die Einladungs-E-Mail jedes Benutzers
aufgenommen, um einen einfachen Zugriff und die Speicherung als
Lesezeichen zu ermöglichen.  Wenn der Benutzer noch nicht bei der Konsole
angemeldet ist, wird er aufgefordert, sich anzumelden.
```

Neue Benutzer müssen sich noch für den Zugriff auf die Konsole anmelden, bevor sie auf ihre Mandanten-URL zugreifen können.

Wenn Sie sich zum ersten Mal bei einem neuen Mandanten anmelden, werden Sie durch die Einrichtung geführt, um**"Beginne mit der Datenerfassung"** .

Abmelden

Um sich von Data Infrastructure Insights abzumelden, klicken Sie auf Ihren **Benutzernamen** und wählen Sie **Abmelden**. Sie werden zum Anmeldebildschirm der Konsole zurückgeleitet.

Wenn Sie sich von Data Infrastructure Insights abmelden, werden Sie auch von der Konsole abgemeldet. Sie werden auch von anderen NetApp Cloud-Diensten abgemeldet, die die Konsolenanmeldung verwenden.

Inaktivitäts-Timeout

Standardmäßig meldet die Konsole einen Benutzer ab, wenn sechs Stunden (360 Minuten) lang keine Aktivität stattfindet. Unabhängig von der Aktivität werden Benutzer nach sieben Tagen abgemeldet.

Sicherheit

Data Infrastructure Insights Sicherheit

Die Sicherheit von Produkt- und Kundendaten hat bei NetApp höchste Bedeutung. Data Infrastructure Insights befolgt während des gesamten Release-Lebenszyklus bewährte Sicherheitspraktiken, um sicherzustellen, dass Kundeninformationen und -daten bestmöglich geschützt sind.

Sicherheitsübersicht

Physische Sicherheit

Die Produktionsinfrastruktur von Data Infrastructure Insights wird in Amazon Web Services (AWS) gehostet. Physische und umweltbezogene sicherheitsrelevante Kontrollen für Data Infrastructure Insights Produktionsserver, zu denen Gebäude sowie an Türen verwendete Schlösser oder Schlüssel gehören, werden von AWS verwaltet. Laut AWS: „Der physische Zugang wird sowohl am Perimeter als auch an den Gebäudeeingängen von professionellem Sicherheitspersonal mithilfe von Videoüberwachung, Einbruchmeldeanlagen und anderen elektronischen Mitteln kontrolliert. Autorisierte Mitarbeiter nutzen Multi-Faktor-Authentifizierungsmechanismen, um auf die Etagen des Rechenzentrums zuzugreifen.“

Data Infrastructure Insights folgt den Best Practices der"Modell der geteilten Verantwortung" von AWS beschrieben.

Produktsicherheit

Data Infrastructure Insights folgt einem Entwicklungslebenszyklus im Einklang mit Agile-Prinzipien und ermöglicht uns so, sicherheitsrelevante Softwarefehler schneller zu beheben als bei Entwicklungsmethoden mit längeren Release-Zyklen. Durch den Einsatz kontinuierlicher Integrationsmethoden sind wir in der Lage, schnell auf funktionale und sicherheitsrelevante Änderungen zu reagieren. Die Verfahren und Richtlinien zum Änderungsmanagement definieren, wann und wie Änderungen erfolgen, und tragen dazu bei, die Stabilität der Produktionsumgebung aufrechtzuerhalten. Alle Änderungen mit Auswirkungen werden vor ihrer Veröffentlichung in der Produktionsumgebung formell kommuniziert, koordiniert, ordnungsgemäß überprüft und genehmigt.

Netzwerksicherheit

Der Netzwerkzugriff auf Ressourcen in der Data Infrastructure Insights Umgebung wird durch hostbasierte Firewalls gesteuert. Jede Ressource (z. B. ein Load Balancer oder eine Instanz einer virtuellen Maschine) verfügt über eine hostbasierte Firewall, die den eingehenden Datenverkehr auf die Ports beschränkt, die die Ressource zur Ausführung ihrer Funktion benötigt.

Data Infrastructure Insights verwendet verschiedene Mechanismen, darunter Intrusion Detection-Dienste, um die Produktionsumgebung auf Sicherheitsanomalien zu überwachen.

Risikobewertung

Das Data Infrastructure Insights -Team folgt einem formalisierten Risikobewertungsprozess, um eine systematische, wiederholbare Möglichkeit zur Identifizierung und Bewertung der Risiken bereitzustellen, sodass diese mithilfe eines Risikobehandlungsplans angemessen gemanagt werden können.

Datenschutz

Die Produktionsumgebung von Data Infrastructure Insights ist in einer hochredundanten Infrastruktur eingerichtet, die mehrere Verfügbarkeitszonen für alle Dienste und Komponenten nutzt. Neben der Nutzung einer hochverfügbaren und redundanten Computerinfrastruktur werden kritische Daten in regelmäßigen Abständen gesichert und Wiederherstellungen regelmäßig getestet. Formale Backup-Richtlinien und -Verfahren minimieren die Auswirkungen von Unterbrechungen der Geschäftstätigkeit, schützen Geschäftsprozesse vor den Auswirkungen von Ausfällen von Informationssystemen oder Katastrophen und gewährleisten ihre rechtzeitige und angemessene Wiederaufnahme.

Authentifizierung und Zugriffsverwaltung

Der gesamte Kundenzugriff auf Data Infrastructure Insights erfolgt über Browser-UI-Interaktionen über https. Die Authentifizierung erfolgt über den Drittanbieterdienst Auth0. NetApp hat dies als Authentifizierungsebene für alle Cloud-Datendienste zentralisiert.

Data Infrastructure Insights befolgt branchenübliche Best Practices, darunter „Least Privilege“ und „rollenbasierte Zugriffskontrolle“ für den logischen Zugriff auf die Data Infrastructure Insights -Produktionsumgebung. Der Zugriff wird streng nach Bedarf kontrolliert und nur ausgewählten autorisierten Mitarbeitern mithilfe von Multi-Faktor-Authentifizierungsmechanismen gewährt.

Erhebung und Schutz von Kundendaten

Alle Kundendaten werden während der Übertragung über öffentliche Netzwerke und im Ruhezustand verschlüsselt. Data Infrastructure Insights nutzt an verschiedenen Stellen im System Verschlüsselung, um Kundendaten mithilfe von Technologien wie Transport Layer Security (TLS) und dem Industriestandard-Algorithmus AES-256 zu schützen.

Kunden-Deprovisionierung

In unterschiedlichen Abständen werden E-Mail-Benachrichtigungen versendet, um den Kunden über den Ablauf seines Abonnements zu informieren. Nach Ablauf des Abonnements wird die Benutzeroberfläche eingeschränkt und es beginnt eine Schonfrist für die Datenerfassung. Der Kunde wird anschließend per E-Mail benachrichtigt. Für Testabonnements gilt eine Nachfrist von 14 Tagen und für kostenpflichtige Abonnementkonten eine Nachfrist von 28 Tagen. Nach Ablauf der Nachfrist wird der Kunde per E-Mail darüber informiert, dass das Konto in 2 Tagen gelöscht wird. Ein zahlender Kunde kann auch direkt die Abmeldung vom Dienst beantragen.

Abgelaufene Mandanten und alle zugehörigen Kundendaten werden vom Data Infrastructure Insights Operations (SRE)-Team am Ende der Nachfrist oder nach Bestätigung der Anfrage eines Kunden zur Kündigung seines Kontos gelöscht. In beiden Fällen führt das SRE-Team einen API-Aufruf aus, um das Konto zu löschen. Der API-Aufruf löscht die Mandanteninstanz und alle Kundendaten. Die Löschung des Kunden wird durch Aufrufen derselben API und Überprüfen, ob der Mandantenstatus des Kunden „GELÖSCHT“ lautet, überprüft.

Sicherheitsvorfallmanagement

Data Infrastructure Insights ist in den PSIRT-Prozess (Product Security Incident Response Team) von NetApp integriert, um bekannte Schwachstellen zu finden, zu bewerten und zu beheben. PSIRT bezieht Informationen zu Sicherheitslücken aus mehreren Kanälen, darunter Kundenberichte, interne Entwicklungsabteilungen und allgemein anerkannte Quellen wie die CVE-Datenbank.

Wenn das Data Infrastructure Insights Engineering-Team ein Problem erkennt, leitet das Team den PSIRT-Prozess ein, bewertet das Problem und behebt es möglicherweise.

Es ist auch möglich, dass ein Kunde oder Forscher von Data Infrastructure Insights ein Sicherheitsproblem mit dem Data Infrastructure Insights -Produkt erkennt und das Problem dem technischen Support oder direkt dem Incident Response Team von NetApp meldet. In diesen Fällen leitet das Data Infrastructure Insights -Team den PSIRT-Prozess ein, bewertet das Problem und behebt es möglicherweise.

Schwachstellen- und Penetrationstests

Data Infrastructure Insights befolgt die Best Practices der Branche und führt regelmäßig Schwachstellen- und Penetrationstests mithilfe interner und externer Sicherheitsexperten und -unternehmen durch.

Schulung zum Sicherheitsbewusstsein

Alle Mitarbeiter von Data Infrastructure Insights absolvieren ein Sicherheitstraining, das auf die jeweilige Rolle zugeschnitten ist, um sicherzustellen, dass jeder Mitarbeiter für die spezifischen sicherheitsbezogenen Herausforderungen seiner Rolle gerüstet ist.

Einhaltung

Data Infrastructure Insights führt unabhängige Audits und Validierungen seiner Sicherheit, Prozesse und Dienste durch externe lizenzierte CPA-Unternehmen durch, einschließlich der Durchführung des SOC 2-Audits.

NetApp Sicherheitshinweise

Sie können die verfügbaren Sicherheitshinweise von NetApp einsehen"hier," .

Informationen und Region

NetApp nimmt die Sicherheit von Kundeninformationen sehr ernst. Hier erfahren Sie, wie und wo Data Infrastructure Insights Ihre Informationen speichert.

Welche Informationen speichert Data Infrastructure Insights ?

Data Infrastructure Insights speichert die folgenden Informationen:

- Leistungsdaten

  Leistungsdaten sind Zeitreihendaten, die Informationen über die Leistung des überwachten Geräts/der überwachten Quelle liefern. Hierzu zählen beispielsweise die Anzahl der von einem Speichersystem bereitgestellten E/A-Vorgänge, der Durchsatz eines FibreChannel-Ports, die Anzahl der von einem Webserver bereitgestellten Seiten, die Antwortzeit einer Datenbank und mehr.

- Bestandsdaten

  Inventardaten bestehen aus Metadaten, die das überwachte Gerät/die überwachte Quelle und deren Konfiguration beschreiben. Hierzu gehören beispielsweise installierte Hardware- und Softwareversionen, Festplatten und LUNs in einem Speichersystem, CPU-Kerne, RAM und Festplatten einer virtuellen Maschine, die Tablespaces einer Datenbank, die Anzahl und Art der Ports auf einem SAN-Switch, Verzeichnis-/Dateinamen (wenn Storage Workload Security aktiviert ist) usw.

- Konfigurationsdaten

  Dies fasst die vom Kunden bereitgestellten Konfigurationsdaten zusammen, die zur Verwaltung des Kundenbestands und der Vorgänge verwendet werden, z. B. Hostnamen oder IP-Adressen der

überwachten Geräte, Abfrageintervalle, Timeout-Werte usw.

- Geheimnisse

  Geheimnisse bestehen aus den Anmeldeinformationen, die von der Data Infrastructure Insights Acquisition Unit für den Zugriff auf Kundengeräte und -dienste verwendet werden. Diese Anmeldeinformationen werden mithilfe einer starken asymmetrischen Verschlüsselung verschlüsselt und die privaten Schlüssel werden nur auf den Erfassungseinheiten gespeichert und verlassen nie die Kundenumgebung. Aufgrund dieses Designs können selbst privilegierte Data Infrastructure Insights SREs nicht auf Kundengeheimnisse im Klartext zugreifen.

- Funktionale Daten

  Dabei handelt es sich um Daten, die durch die Bereitstellung des Cloud Data Service durch NetApp generiert werden und die NetApp bei der Entwicklung, Bereitstellung, dem Betrieb, der Wartung und der Sicherung des Cloud Data Service unterstützen. Funktionale Daten enthalten keine Kundeninformationen oder personenbezogenen Daten.

- Benutzerzugriffsdaten

  Authentifizierungs- und Zugriffsinformationen, die es der NetApp Console ermöglichen, mit regionalen Data Infrastructure Insights -Sites zu kommunizieren, einschließlich Daten zur Benutzerautorisierung.

- Speicher-Workload-Sicherheit Benutzerverzeichnisdaten

  In Fällen, in denen die Workload-Sicherheitsfunktion aktiviert ist UND der Kunde den Benutzerverzeichnis-Collector aktiviert, speichert das System Benutzeranzeigenamen, Unternehmens-E-Mail-Adressen und andere aus Active Directory gesammelte Informationen.

> Benutzerverzeichnisdaten beziehen sich auf Benutzerverzeichnisinformationen, die vom Workload Security-Benutzerverzeichnis-Datensammler erfasst werden, und nicht auf Daten über die Benutzer von Data Infrastructure Insights/Workload Security selbst.

Es werden **keine expliziten personenbezogenen Daten** aus Infrastruktur- und Serviceressourcen erhoben. Die gesammelten Informationen bestehen nur aus Leistungsmesswerten, Konfigurationsinformationen und Infrastrukturmetadaten, ähnlich wie bei vielen Anbietern von Phone-Homes, einschließlich NetApp Auto-Support und ActiveIQ. Abhängig von den Namenskonventionen eines Kunden können Daten für Freigaben, Volumes, VMs, Qtrees, Anwendungen usw. jedoch personenbezogene Daten enthalten.

Wenn die Workload-Sicherheit aktiviert ist, prüft das System zusätzlich Datei- und Verzeichnisnamen auf SMB- oder anderen Freigaben, die möglicherweise personenbezogene Daten enthalten. Wenn Kunden den Workload Security User Directory Collector aktivieren (der im Wesentlichen Windows-SIDs über Active Directory Benutzernamen zuordnet), werden der Anzeigename, die Unternehmens-E-Mail-Adresse und alle weiteren ausgewählten Attribute von Data Infrastructure Insights erfasst und gespeichert.

Darüber hinaus werden Zugriffsprotokolle für Data Infrastructure Insights geführt, die die IP- und E-Mail-Adressen der Benutzer enthalten, die sie zum Anmelden beim Dienst verwendet haben.

Wo werden meine Informationen gespeichert?

Data Infrastructure Insights speichert Informationen entsprechend der Region, in der Ihre Umgebung erstellt wird.

Die folgenden Informationen werden in der Hostregion gespeichert:

- Telemetrie- und Asset-/Objektinformationen, einschließlich Zähler und Leistungsmetriken
- Informationen zur Erfassungseinheit
- Funktionale Daten
- Prüfinformationen zu Benutzeraktivitäten in Data Infrastructure Insights
- Informationen zur Workload-Sicherheit in Active Directory
- Informationen zum Workload-Sicherheitsaudit

Die folgenden Informationen befinden sich in den Vereinigten Staaten, unabhängig von der Region, in der Ihre Data Infrastructure Insights Umgebung gehostet wird:

- Informationen zur Umgebungssite (manchmal auch „Mandant“ genannt), z. B. Site-/Kontoinhaber.
- Informationen, die es der NetApp Console ermöglichen, mit regionalen Data Infrastructure Insights -Sites zu kommunizieren, einschließlich aller Informationen, die mit der Benutzerautorisierung zu tun haben.
- Informationen zur Beziehung zwischen dem Data Infrastructure Insights Benutzer und dem Mandanten.

Gastgeberregionen

Zu den Gastgeberregionen gehören:

- USA: us-east-1
- EMEA: eu-central-1
- APAC: ap-southeast-2

Weitere Informationen

Weitere Informationen zum Datenschutz und zur Sicherheit von NetApp finden Sie unter den folgenden Links:

- "Vertrauenszentrum"
- "Grenzüberschreitende Datenübertragungen"
- "Verbindliche Unternehmensregeln"
- "Antworten auf Datenanfragen von Drittanbietern"
- "NetApp Datenschutzgrundsätze"

SecurityAdmin-Tool

Data Infrastructure Insights umfasst Sicherheitsfunktionen, die einen Betrieb Ihrer Umgebung mit erhöhter Sicherheit ermöglichen. Zu den Funktionen gehören Verbesserungen bei der Verschlüsselung, beim Passwort-Hashing und die Möglichkeit, interne Benutzerpasswörter sowie Schlüsselpaare zum Ver- und Entschlüsseln von Passwörtern zu ändern.

Zum Schutz vertraulicher Daten empfiehlt NetApp , die Standardschlüssel und das *Acquisition* -Benutzerkennwort nach einer Installation oder einem Upgrade zu ändern.

Verschlüsselte Passwörter von Datenquellen werden in Data Infrastructure Insights gespeichert. Dabei wird ein öffentlicher Schlüssel zum Verschlüsseln von Passwörtern verwendet, wenn ein Benutzer sie auf einer Konfigurationsseite eines Datensammlers eingibt. Data Infrastructure Insights verfügt nicht über die privaten

Schlüssel, die zum Entschlüsseln der Kennwörter des Datensammlers erforderlich sind. Nur Acquisition Units (AUs) verfügen über den privaten Schlüssel des Datensammlers, der zum Entschlüsseln der Kennwörter des Datensammlers erforderlich ist.

Überlegungen zu Upgrades und Installationen

Wenn Ihr Insight-System nicht standardmäßige Sicherheitskonfigurationen enthält (d. h. Sie haben Passwörter neu verschlüsselt), müssen Sie Ihre Sicherheitskonfigurationen sichern. Durch die Installation neuer Software oder in einigen Fällen durch ein Software-Upgrade wird Ihr System auf die Standardsicherheitskonfiguration zurückgesetzt. Wenn Ihr System zur Standardkonfiguration zurückkehrt, müssen Sie die nicht standardmäßige Konfiguration wiederherstellen, damit das System ordnungsgemäß funktioniert.

Verwalten der Sicherheit auf der Erfassungseinheit

Mit dem Tool SecurityAdmin können Sie Sicherheitsoptionen für Data Infrastructure Insights verwalten. Es wird auf dem System der Erfassungseinheit ausgeführt. Zur Sicherheitsverwaltung gehört die Verwaltung von Schlüsseln und Passwörtern, das Speichern und Wiederherstellen der von Ihnen erstellten Sicherheitskonfigurationen oder das Zurücksetzen der Konfigurationen auf die Standardeinstellungen.

Bevor Sie beginnen

- Sie müssen über Administratorrechte auf dem AU-System verfügen, um die Acquisition Unit-Software (einschließlich des SecurityAdmin-Tools) zu installieren.
- Wenn Sie Benutzer ohne Administratorrechte haben, die später auf das SecurityAdmin-Tool zugreifen müssen, müssen diese der Gruppe *cisys* hinzugefügt werden. Die Gruppe *cisys* wird während der AU-Installation erstellt.

Nach der AU-Installation befindet sich das SecurityAdmin-Tool auf dem Erfassungseinheitssystem an einem der folgenden Orte:

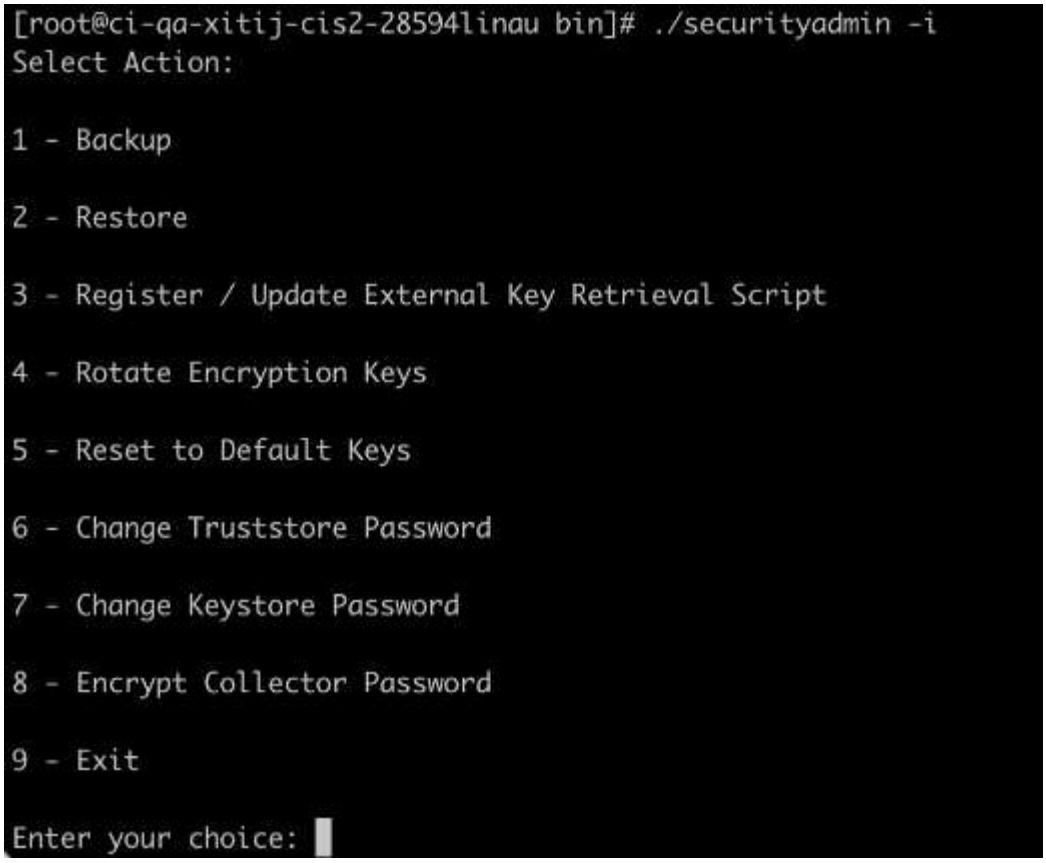
```
Windows - <install_path>\Cloud Insights\Acquisition
Unit\acq\securityadmin\bin\securityadmin.bat
Linux - /bin/oci-securityadmin.sh
```

Verwenden des SecurityAdmin-Tools

Starten Sie das SecurityAdmin-Tool im interaktiven Modus (-i).

> Es wird empfohlen, das SecurityAdmin-Tool im interaktiven Modus zu verwenden, um die Weitergabe von Geheimnissen über die Befehlszeile zu vermeiden, die in Protokollen erfasst werden können.

Die folgenden Optionen werden angezeigt:



1. **Sicherung**

   Erstellt eine ZIP-Sicherungsdatei des Tresors mit allen Passwörtern und Schlüsseln und speichert die Datei an einem vom Benutzer angegebenen Speicherort oder an den folgenden Standardspeicherorten:

   ```
   Windows - <install_path>\Cloud Insights\Acquisition
   Unit\acq\securityadmin\backup\vault
   Linux - /var/log/netapp/oci/backup/vault
   ```

   Es wird empfohlen, Tresor-Backups sicher aufzubewahren, da sie vertrauliche Informationen enthalten.

2. **Wiederherstellen**

   Stellt die erstellte ZIP-Sicherung des Tresors wieder her. Nach der Wiederherstellung werden alle Passwörter und Schlüssel auf die Werte zurückgesetzt, die zum Zeitpunkt der Sicherungserstellung gültig waren.

   Mit „Wiederherstellen“ können Sie Passwörter und Schlüssel auf mehreren Servern synchronisieren, beispielsweise mit diesen Schritten: 1) Ändern Sie die Verschlüsselungsschlüssel auf der AU. 2) Erstellen Sie eine Sicherungskopie des Tresors. 3) Stellen Sie die Tresorsicherung auf jeder der AUs wieder her.

3. **Skript zum Abrufen externer Schlüssel registrieren/aktualisieren**

   Verwenden Sie ein externes Skript, um die AU-Verschlüsselungsschlüssel zu registrieren oder zu ändern, die zum Verschlüsseln oder Entschlüsseln von Gerätekennwörtern verwendet werden.

   Wenn Sie Verschlüsselungsschlüssel ändern, sollten Sie Ihre neue Sicherheitskonfiguration sichern, damit

Sie sie nach einem Upgrade oder einer Installation wiederherstellen können.

Beachten Sie, dass diese Option nur unter Linux verfügbar ist.

Wenn Sie Ihr eigenes Schlüsselabrufskript mit dem SecurityAdmin-Tool verwenden, beachten Sie Folgendes:

- Der derzeit unterstützte Algorithmus ist RSA mit mindestens 2048 Bit.
- Das Skript muss den privaten und öffentlichen Schlüssel im Klartext zurückgeben. Das Skript darf keine verschlüsselten privaten und öffentlichen Schlüssel zurückgeben.
- Das Skript sollte unverarbeitete, codierte Inhalte zurückgeben (nur PEM-Format).
- Das externe Skript muss über Ausführungsberechtigungen verfügen.

4. **Rotierende Verschlüsselungsschlüssel**

   Rotieren Sie Ihre Verschlüsselungsschlüssel (melden Sie aktuelle Schlüssel ab und registrieren Sie neue Schlüssel). Um einen Schlüssel aus einem externen Schlüsselverwaltungssystem zu verwenden, müssen Sie die öffentliche und die private Schlüssel-ID angeben.

5. **Auf Standardtasten zurücksetzen**

   Setzt das Kennwort und die Verschlüsselungsschlüssel des Erwerbsbenutzers auf die Standardwerte zurück. Die Standardwerte sind diejenigen, die während der Installation bereitgestellt werden.

6. **Truststore-Passwort ändern**

   Ändern Sie das Passwort des Truststores.

7. **Keystore-Passwort ändern**

   Ändern Sie das Passwort des Schlüsselspeichers.

8. **Collector-Passwort verschlüsseln**

   Datensammlerkennwort verschlüsseln.

9. **Ausfahrt**

   Beenden Sie das SecurityAdmin-Tool.

Wählen Sie die Option, die Sie konfigurieren möchten, und folgen Sie den Anweisungen.

Festlegen eines Benutzers zum Ausführen des Tools

Wenn Sie sich in einer kontrollierten, sicherheitsbewussten Umgebung befinden, verfügen Sie möglicherweise nicht über die Gruppe *cisys*, möchten aber dennoch, dass bestimmte Benutzer das Tool SecurityAdmin ausführen.

Sie können dies erreichen, indem Sie die AU-Software manuell installieren und den Benutzer/die Gruppe angeben, für den/die Sie Zugriff wünschen.

- Laden Sie mithilfe der API das CI-Installationsprogramm auf das AU-System herunter und entpacken Sie es.

    - Sie benötigen ein einmaliges Autorisierungstoken. Sehen Sie sich die API Swagger-Dokumentation an (*Admin > API-Zugriff* und wählen Sie den Link *API-Dokumentation*) und suchen Sie den API-Abschnitt *GET /au/oneTimeToken*.
    - Sobald Sie das Token haben, verwenden Sie die API *GET /au/installers/{platform}/{version}*, um die Installationsdatei herunterzuladen. Sie müssen die Plattform (Linux oder Windows) sowie die Installationsversion angeben.
- Kopieren Sie die heruntergeladene Installationsdatei auf das AU-System und entpacken Sie sie.
- Navigieren Sie zu dem Ordner, der die Dateien enthält, und führen Sie das Installationsprogramm als Root aus, wobei Sie den Benutzer und die Gruppe angeben:

```
./cloudinsights-install.sh <User> <Group>
```

Wenn der angegebene Benutzer und/oder die angegebene Gruppe nicht vorhanden sind, werden sie erstellt. Der Benutzer hat Zugriff auf das SecurityAdmin-Tool.

Aktualisieren oder Entfernen des Proxys

Mit dem Tool SecurityAdmin können Sie Proxy-Informationen für die Erfassungseinheit festlegen oder entfernen, indem Sie das Tool mit dem Parameter *-pr* ausführen:

```
[root@ci-eng-linau bin]# ./securityadmin -pr
usage: securityadmin -pr -ap <arg> | -h | -rp | -upr <arg>

The purpose of this tool is to enable reconfiguration of security aspects
of the Acquisition Unit such as encryption keys, and proxy configuration,
etc. For more information about this tool, please check the Data
Infrastructure Insights
Documentation.

-ap,--add-proxy <arg>       add a proxy server.  Arguments: ip=ip
                             port=port user=user password=password
                             domain=domain
                             (Note: Always use double quote(") or single
                             quote(') around user and password to escape
                             any special characters, e.g., <, >, ~, `, ^,
                             !
                             For example: user="test" password="t'!<@1"
                             Note: domain is required if the proxy auth
                             scheme is NTLM.)
-h,--help
-rp,--remove-proxy          remove proxy server
-upr,--update-proxy <arg>   update a proxy.  Arguments: ip=ip port=port
                             user=user password=password domain=domain
                             (Note: Always use double quote(") or single
                             quote(') around user and password to escape
                             any special characters, e.g., <, >, ~, `, ^,
                             !
                             For example: user="test" password="t'!<@1"
                             Note: domain is required if the proxy auth
                             scheme is NTLM.)
```

Um beispielsweise den Proxy zu entfernen, führen Sie diesen Befehl aus:

```
 [root@ci-eng-linau bin]# ./securityadmin -pr -rp
Sie müssen die Erfassungseinheit nach der Ausführung des Befehls neu
starten.
```

Um einen Proxy zu aktualisieren, lautet der Befehl

```
./securityadmin -pr -upr <arg>
```

Externer Schlüsselabruf

Wenn Sie ein UNIX-Shell-Skript bereitstellen, kann es von der Erfassungseinheit ausgeführt werden, um den **privaten Schlüssel** und den **öffentlichen Schlüssel** aus Ihrem Schlüsselverwaltungssystem abzurufen.

Um den Schlüssel abzurufen, führt Data Infrastructure Insights das Skript aus und übergibt zwei Parameter: *Schlüssel-ID* und *Schlüsseltyp*. Mit der *Schlüssel-ID* können Sie den Schlüssel in Ihrem Schlüsselverwaltungssystem identifizieren. *Schlüsseltyp* ist entweder „öffentlich“ oder „privat“. Wenn der Schlüsseltyp „öffentlich“ ist, muss das Skript den öffentlichen Schlüssel zurückgeben. Wenn der Schlüsseltyp „privat“ ist, muss der private Schlüssel zurückgegeben werden.

Um den Schlüssel an die Erfassungseinheit zurückzusenden, muss das Skript den Schlüssel in der Standardausgabe drucken. Das Skript darf *nur* den Schlüssel in die Standardausgabe drucken. Es darf kein anderer Text in die Standardausgabe gedruckt werden. Sobald der angeforderte Schlüssel in der Standardausgabe gedruckt wird, muss das Skript mit einem Exitcode von 0 beendet werden; jeder andere Rückgabecode wird als Fehler betrachtet.

Das Skript muss mithilfe des SecurityAdmin-Tools bei der Erfassungseinheit registriert werden, das das Skript zusammen mit der Erfassungseinheit ausführt. Das Skript muss über Lese- und Ausführungsberechtigungen für den Root- und „cisys“-Benutzer verfügen. Wenn das Shell-Skript nach der Registrierung geändert wird, muss das geänderte Shell-Skript erneut bei der Erfassungseinheit registriert werden.

Eingabeparameter: Schlüssel-ID	Schlüsselkennung, die zur Identifizierung des Schlüssels im Schlüsselverwaltungssystem des Kunden verwendet wird.
Eingabeparameter: Schlüsseltyp	öffentlich oder privat.
Ausgabe	Der angeforderte Schlüssel muss auf der Standardausgabe ausgegeben werden. Derzeit wird ein 2048-Bit-RSA-Schlüssel unterstützt. Schlüssel müssen im folgenden Format codiert und gedruckt werden: Privates Schlüsselformat – PEM, DER-codiert PKCS8 PrivateKeyInfo RFC 5958 Öffentliches Schlüsselformat – PEM, DER-codiert X.509 SubjectPublicKeyInfo RFC 5280
Exitcode	Bei Erfolg ist der Exitcode Null. Alle anderen Exit-Werte gelten als Fehlschlag.
Skriptberechtigungen	Das Skript muss über Lese- und Ausführungsberechtigungen für den Root- und „cisys“-Benutzer verfügen.
Protokolle	Skriptausführungen werden protokolliert. Protokolle finden Sie unter - /var/log/netapp/cloudinsights/securityadmin/securityadmin.log /var/log/netapp/cloudinsights/acq/acq.log

Verschlüsseln eines Passworts zur Verwendung in der API

Option 8 ermöglicht Ihnen die Verschlüsselung eines Passworts, welches Sie dann per API an einen Datensammler weitergeben können.

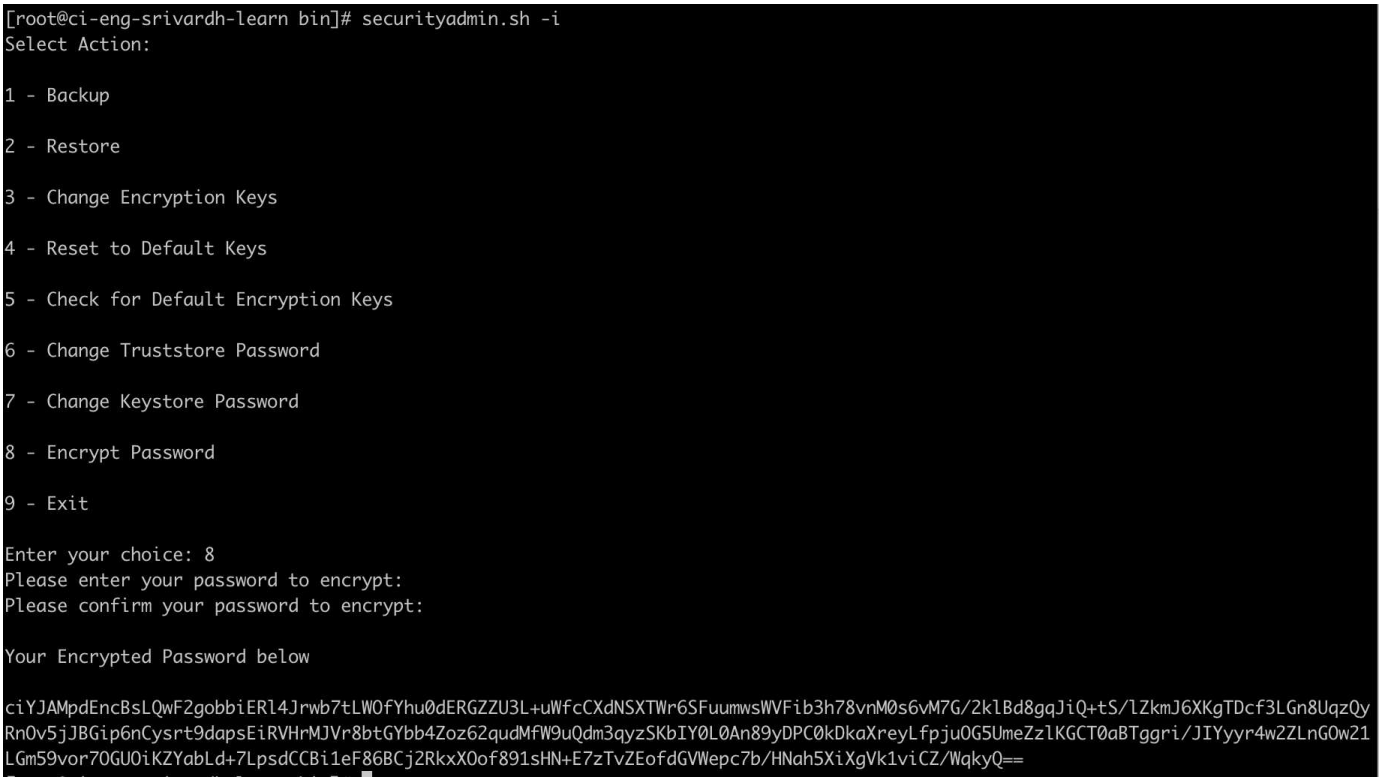
Starten Sie das SecurityAdmin-Tool im interaktiven Modus und wählen Sie Option 8: *Passwort verschlüsseln*.

```
 securityadmin.sh -i
Sie werden aufgefordert, das zu verschlüsselnde Kennwort einzugeben.
Beachten Sie, dass die von Ihnen eingegebenen Zeichen nicht auf dem
Bildschirm angezeigt werden.  Geben Sie das Passwort erneut ein, wenn Sie
dazu aufgefordert werden.
```

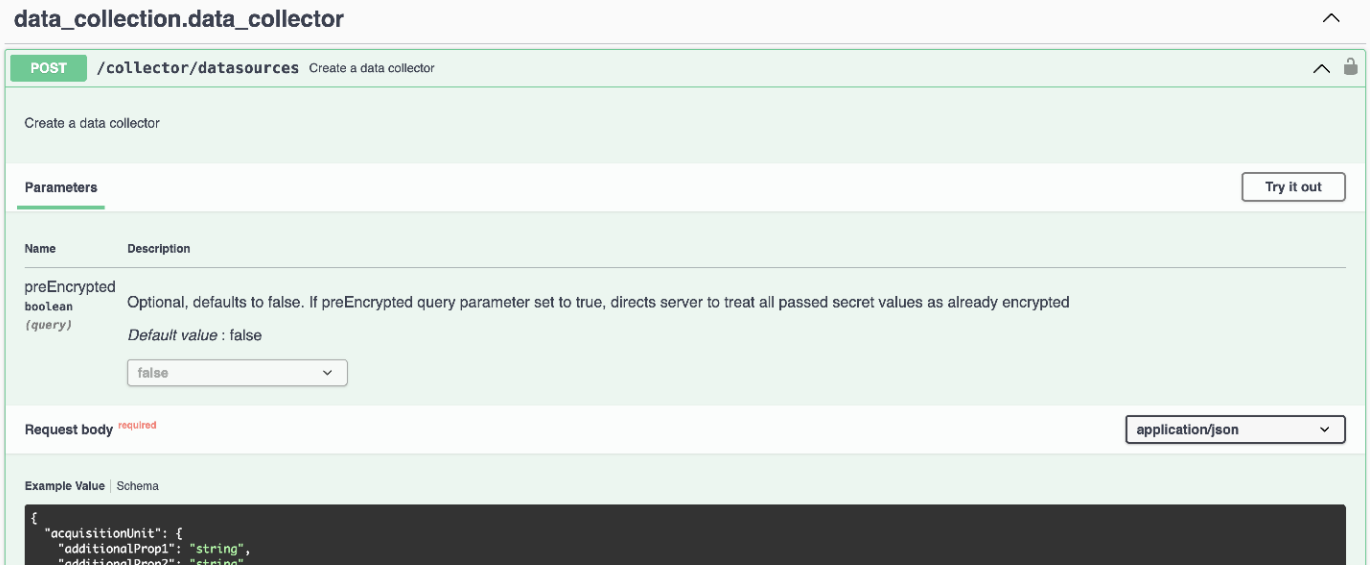
Wenn Sie den Befehl alternativ in einem Skript verwenden möchten, verwenden Sie in einer Befehlszeile *securityadmin.sh* mit dem Parameter „-enc“ und übergeben Sie Ihr unverschlüsseltes Kennwort:

```
 securityadmin -enc mypassword
image:SecurityAdmin_Encrypt_Key_API_CLI_Example.png["CLI-Beispiel"]
```

Das verschlüsselte Passwort wird auf dem Bildschirm angezeigt. Kopieren Sie die gesamte Zeichenfolge einschließlich aller führenden oder nachfolgenden Symbole.



Um das verschlüsselte Passwort an einen Datensammler zu senden, können Sie die Datensammlungs-API verwenden. Den Swagger für diese API finden Sie unter **Admin > API-Zugriff**. Klicken Sie auf den Link „API-Dokumentation“. Wählen Sie den API-Typ „Datenerfassung“ aus. Wählen Sie unter der Überschrift *data_collection.data_collector* die POST-API */collector/datasources* für dieses Beispiel aus.



Wenn Sie die Option *preEncrypted* auf *True* setzen, wird jedes Kennwort, das Sie über den API-Befehl übergeben, als **bereits verschlüsselt** behandelt. Die API verschlüsselt das/die Kennwort(e) nicht erneut. Fügen Sie beim Erstellen Ihrer API einfach das zuvor verschlüsselte Passwort an der entsprechenden Stelle ein.

https://<TENANT URL>/rest/v1/collector/datasources?preEncrypted=true


```
{
"name": "cdot-aaaaa",
  "config": {
    "dsTypeId": "93",
    "vendorModelId": "1",
    "packages": [
      {
        "id": "foundation",
        "displayName": "Inventory",
        "isMandatory": true,
        "attributes": {
          "RELEASESTATUS": "OFFICIAL",
          "enabled": true,
          "ip": "10.62.219.30",
          "user": "admin",
          "password":
"J8bepjwz9oNknfs6mcqbz3zuEThZQp1VyTk+1wE05gWwmmj1u0CB688nfOnB1xnlBVsAWyLmORxFAw
vcDCvGbTraqp/+nT0k94LO8Z7Q04I5KqhHfTvINGU54S4IVLWiMIFj8kSU4RhMvNNNq5Tarz0gJZhWR+
4RoNF+84R/uFFGwKeblrwfHxWZZMoW7pEJ2kzLFBtBzx2mUvRP0kn6AFbyS4+DM2YTPQkSk3W2Gzc
+nfPDDyH8Tq6AM5WsVCKqnZAa2ZlY1FxMkKT7iFt5oiYnl93ka7OrQlmM9QAyPoyw/JT0nXHDuf683uE
K32yn9CgxNGXy5NcNzRurdFNb5w=="
        }
      },
      {
        "id": "storageperformance",
        "displayName": "Array Performance",
        "isMandatory": false,
        "attributes": {
          "password": "this will not be encrypted on the server side"
        }
      }
    ]
  },
  "acquisitionUnit": {
    "id": "1"
  }
}
```

Erste Schritte

Daten sammeln

Erste Schritte beim Sammeln von Daten

Nachdem Sie sich für Data Infrastructure Insights angemeldet und sich zum ersten Mal bei Ihrer Umgebung angemeldet haben, werden Sie durch die folgenden Schritte geführt, um mit dem Sammeln und Verwalten von Daten zu beginnen.

Datensammler ermitteln Informationen aus Ihren Datenquellen, beispielsweise Speichergeräten, Netzwerk-Switches und virtuellen Maschinen. Die gesammelten Informationen werden zur Analyse, Validierung, Überwachung und Fehlerbehebung verwendet.

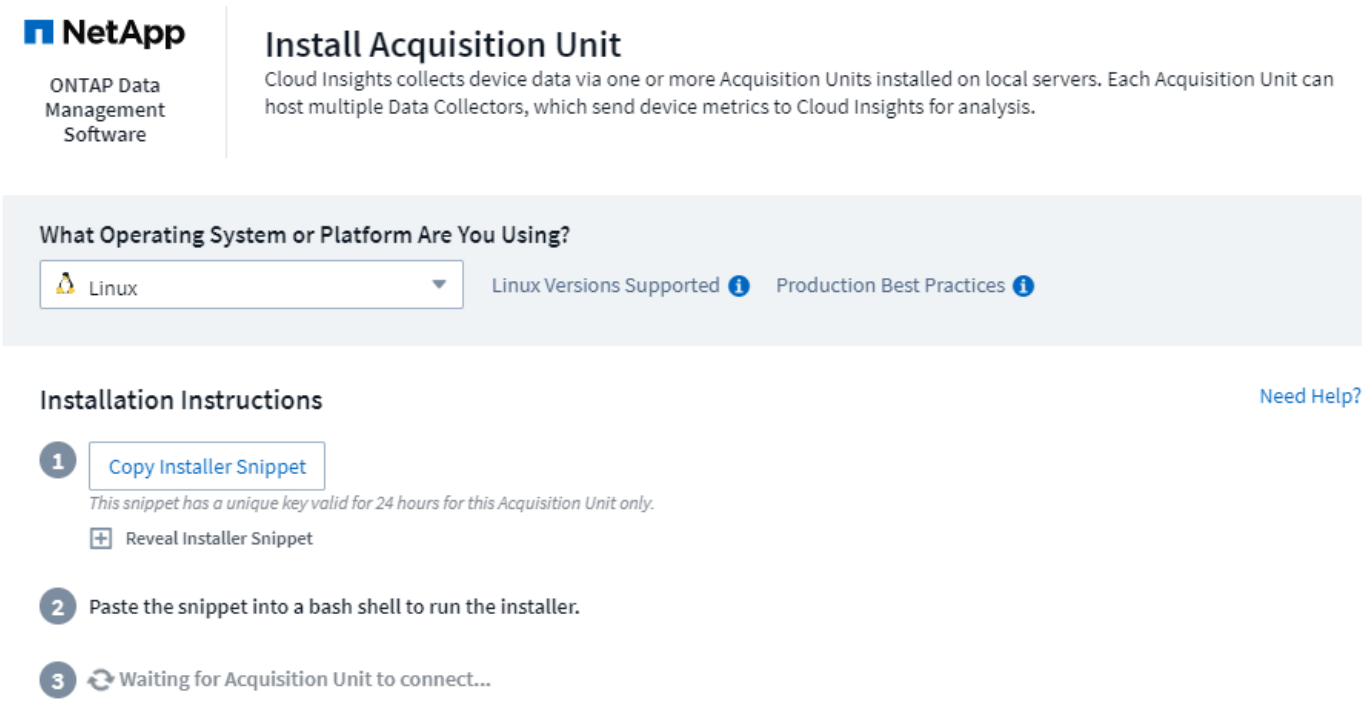
Data Infrastructure Insights bietet drei Arten von Datensammlern:

- Infrastruktur (Speichergeräte, Netzwerk-Switches, Computerinfrastruktur)
- Betriebssysteme (wie VMware oder Windows)
- Dienste (wie Kafka)

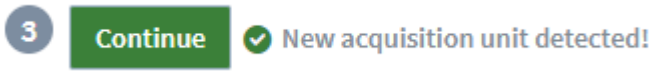
Wählen Sie Ihren ersten Datensammler aus den verfügbaren unterstützten Anbietern und Modellen aus. Sie können später problemlos weitere Datensammler hinzufügen.

Installieren einer Erfassungseinheit

Wenn Sie einen *Infrastruktur*-Datensammler ausgewählt haben, ist eine Erfassungseinheit erforderlich, um Daten in Data Infrastructure Insights einzuspeisen. Sie müssen die Acquisition Unit-Software herunterladen und auf einem Server oder einer VM im Rechenzentrum installieren, von dem Sie die Daten erfassen. Eine einzelne Erfassungseinheit kann für mehrere Datensammler verwendet werden.



- Folgen Sie den"Anweisungen" wird angezeigt, um Ihre Erfassungseinheit zu installieren. Sobald die Software der Erfassungseinheit installiert ist, wird die Schaltfläche „Weiter“ angezeigt und Sie können mit dem nächsten Schritt fortfahren.



Bei Bedarf können Sie später weitere Erfassungseinheiten einrichten. Beispielsweise möchten Sie möglicherweise, dass verschiedene Erfassungseinheiten Informationen aus Rechenzentren in unterschiedlichen Regionen sammeln.

Konfigurieren des Datensammlers – Infrastruktur

Bei *Infrastruktur*-Datensammlern werden Sie aufgefordert, die angezeigten Datensammlerfelder auszufüllen:

- Geben Sie dem Datensammler einen eindeutigen und aussagekräftigen Namen.
- Geben Sie die Anmeldeinformationen (Benutzername und Kennwort) ein, um gegebenenfalls eine Verbindung mit dem Gerät herzustellen.
- Füllen Sie alle anderen Pflichtfelder in den Abschnitten *Konfiguration* und *Erweiterte Konfiguration* aus.
- Klicken Sie auf **Sammler hinzufügen**, um den Datensammler zu speichern.

Sie können später weitere Datensammler konfigurieren.

Konfigurieren des Datensammlers – Betriebssysteme und Dienste

Betriebssystem:

Wählen Sie für Datensammler vom Typ „Betriebssystem“ eine Plattform (Linux, Windows) aus, um einen Data Infrastructure Insights Agent zu installieren. Sie müssen mindestens einen Agenten haben, um Daten von Diensten zu sammeln. Der Agent sammelt auch Daten vom Host selbst zur Verwendung in Data Infrastructure Insights. Diese Daten werden in Widgets usw. als „Knoten“-Daten kategorisiert.

- Öffnen Sie ein Terminal- oder Befehlsfenster auf dem Agent-Host oder der VM und fügen Sie den angezeigten Befehl ein, um den Agent zu installieren.
- Wenn die Installation abgeschlossen ist, klicken Sie auf **Setup abschließen**.

Leistungen:

Klicken Sie bei *Service*-Datensammlern auf eine Kachel, um die Anleitungsseite für diesen Service zu öffnen.

- Wählen Sie eine Plattform und einen Agent-Zugriffsschlüssel.
- Wenn auf dieser Plattform kein Agent installiert ist, befolgen Sie die Anweisungen zum Installieren des Agenten.
- Klicken Sie auf **Weiter**, um die Anleitungsseite zum Datensammler zu öffnen.
- Befolgen Sie die Anweisungen zum Konfigurieren des Datensammlers.
- Wenn die Konfiguration abgeschlossen ist, klicken Sie auf **Setup abschließen**.

Dashboards hinzufügen

Abhängig vom Typ des anfänglichen Datensammlers, den Sie zur Konfiguration ausgewählt haben (Speicher,

Switch usw.), werden ein oder mehrere relevante Dashboards importiert. Wenn Sie beispielsweise einen Speicherdatensammler konfiguriert haben, wird eine Reihe speicherbezogener Dashboards importiert und eines davon als Ihre Data Infrastructure Insights Startseite festgelegt. Sie können die Startseite über die Liste **Dashboards > Alle Dashboards anzeigen** ändern.

Sie können später weitere Dashboards importieren oder"Erstellen Sie Ihre eigenen" .

Das ist alles, was dazu gehört

Nachdem Sie den anfänglichen Einrichtungsprozess abgeschlossen haben, beginnt Ihre Umgebung mit der Datenerfassung.

Wenn Ihr anfänglicher Einrichtungsvorgang unterbrochen wird (z. B. wenn Sie das Browserfenster schließen), müssen Sie die Schritte manuell ausführen:

- Wählen Sie einen Datensammler
- Installieren Sie einen Agenten oder eine Erfassungseinheit, wenn Sie dazu aufgefordert werden
- Konfigurieren des Datensammlers

Nützliche Definitionen

Die folgenden Definitionen können hilfreich sein, wenn es um Datensammler oder Funktionen von Data Infrastructure Insights geht:

- Lebenszyklus des Kollektors: Ein Kollektor befindet sich in seinem Lebenszyklus in einem der folgenden Zustände:
  - **Vorschau**: In begrenzter Kapazität oder für ein begrenztes Publikum verfügbar. "Vorschaufunktionen" und es wird erwartet, dass die Datensammler nach der Vorschauphase allgemein verfügbar werden. Die Vorschauzeiträume variieren je nach Zielgruppe oder Funktionalität.
  - **GA**: Eine Funktion oder ein Datensammler, der basierend auf der Edition oder dem Funktionsumfang allgemein für alle Kunden verfügbar ist.
  - **Veraltet**: Gilt für Datensammler, deren Funktion nicht mehr aufrechterhalten werden kann oder voraussichtlich nicht mehr aufrechterhalten werden kann. Veraltete Datensammler werden häufig durch neuere, funktional aktualisierte Datensammler ersetzt.
  - **Gelöscht**: Ein Datensammler, der entfernt wurde und nicht mehr verfügbar ist.
- Erfassungseinheit: Ein Computer, der ausschließlich zum Hosten von Datensammlern dient, normalerweise eine virtuelle Maschine. Dieser Computer befindet sich normalerweise im selben Rechenzentrum/VPC wie die überwachten Elemente.
- Datenquelle: Ein Modul zur Kommunikation mit einem Hardware- oder Software-Stack. Es besteht aus einer Konfiguration und einem Code, der auf dem AU-Computer ausgeführt wird, um mit dem Gerät zu kommunizieren.

Anforderungen an die Erfassungseinheit

Sie müssen eine Acquisition Unit (AU) installieren, um Informationen von Ihren Infrastrukturdatensammlern (Speicher, VM, Port, EC2 usw.) zu erfassen. Bevor Sie die Erfassungseinheit installieren, sollten Sie sicherstellen, dass Ihr Mandant die Anforderungen an Betriebssystem, CPU, Speicher und Festplattenspeicher erfüllt.

Anforderungen

Komponente	Linux-Anforderungen	Windows-Anforderung
Betriebssystem	Ein Computer, auf dem eine lizenzierte Version eines der folgenden Betriebssysteme ausgeführt wird: * AlmaLinux 9.3 bis 9.5 * Centos (64-Bit): 7.2 bis 7.9, 8.1 bis 8.4, Stream 8, Stream 9 * Debian (64-Bit): 9 bis 12 * OpenSUSE Leap 15.1 bis 15.6 * Oracle Enterprise Linux (64-Bit): 7.5 bis 7.9, 8.1 bis 8.10, 9.3 bis 9.6 * Red Hat (64-Bit): 7.2 bis 7.9, 8.1 bis 8.10, 9.1 bis 9.6 * Rocky 9.0 bis 9.5 * SUSE Linux Enterprise Server 15, 15 SP2 bis 15 SP6 * Ubuntu Server: 18.04, 20.04, 22.04, 24.04 LTS * SELinux auf dem über Plattformen Auf diesem Computer sollte keine andere Software auf Anwendungsebene ausgeführt werden. Ein dedizierter Server wird empfohlen. Wenn Sie mit SELinux arbeiten, wird empfohlen, die folgenden Befehle auf dem Erfassungseinheitssystem auszuführen: sudo semanage fcontext -a -t usr_t "/opt/netapp/cloudinsights(/.*)?" sudo restorecon -R /opt/netapp/cloudinsights	Ein Computer, auf dem eine lizenzierte Version eines der folgenden Programme ausgeführt wird: * Microsoft Windows 10 64-Bit * Microsoft Windows 11 * Microsoft Windows Server 2012 * Microsoft Windows Server 2012 R2 * Microsoft Windows Server 2016 * Microsoft Windows Server 2019 * Microsoft Windows Server 2022 * Microsoft Windows Server 2025 Auf diesem Computer sollte keine andere Software auf Anwendungsebene ausgeführt werden. Ein dedizierter Server wird empfohlen.
CPU	2 CPU-Kerne	Dasselbe
Erinnerung	8 GB RAM	Dasselbe
Verfügbarer Speicherplatz	50 GB (100 GB empfohlen) Für Linux sollte der Speicherplatz folgendermaßen zugewiesen werden: /opt/netapp 10 GB (20 GB für große Umgebungen) /var/log/netapp 40 GB (80 GB für große Umgebungen) /tmp mindestens 1 GB während der Installation verfügbar	50 GB

Netzwerk	Erforderlich sind eine Ethernet-Verbindung mit 100 Mbit/s/1 Gbit/s, eine statische IP-Adresse und Port 80 oder 443 (ausgehend) für die Konnektivität von der Erfassungseinheit zu *.cloudinsights.netapp.com oder Ihrem Data Infrastructure Insights Mandanten (d. h. https://<tenant_id>.c01.cloudinsights.netapp.com). Informationen zu den Anforderungen zwischen der Erfassungseinheit und den einzelnen Datensammlern finden Sie in den Anweisungen für die"Datensammler" . Wenn Ihre Organisation die Verwendung eines Proxys für den Internetzugang erfordert, müssen Sie möglicherweise das Proxy-Verhalten Ihrer Organisation verstehen und nach bestimmten Ausnahmen suchen, damit Data Infrastructure Insights funktioniert. Blockiert Ihre Organisation beispielsweise standardmäßig den Zugriff und erlaubt den Zugriff auf bestimmte Websites/Domänen nur ausnahmsweise? In diesem Fall müssen Sie die folgende Domäne zur Ausnahmeliste hinzufügen: *.cloudinsights.netapp.com. Weitere Informationen finden Sie unter Proxies."hier (Linux)" oder"hier (Windows)" . Beachten Sie, dass Port 443 von der AU zu Data Infrastructure Insights„ausgehend“ geöffnet sein muss.	Dasselbe
Berechtigungen	Sudo-Berechtigungen auf dem Acquisition Unit-Server. /tmp muss mit Exec-Funktionen gemountet werden.	Administratorberechtigungen auf dem Acquisition Unit-Server
Virenscan		Während der Installation müssen Sie alle Virenscanner vollständig deaktivieren. Nach der Installation müssen die von der Acquisition Unit-Software verwendeten Pfade vom Virenscan ausgeschlossen werden.

Zusätzliche Empfehlungen

- Für eine genaue Prüfung und Datenberichterstattung wird dringend empfohlen, die Zeit auf dem Computer der Erfassungseinheit mithilfe des **Network Time Protocol (NTP)** oder des **Simple Network Time Protocol (SNTP)** zu synchronisieren.

Zur Größenbestimmung

Sie können mit einer Data Infrastructure Insights Acquisition Unit mit nur 8 GB Speicher und 50 GB Festplattenspeicher beginnen. Bei größeren Umgebungen sollten Sie sich jedoch die folgenden Fragen stellen:

Erwarten Sie:

- Entdecken Sie mehr als 2500 virtuelle Maschinen oder 10 große (> 2 Knoten) ONTAP Cluster, Symmetrix oder HDS/HPE VSP/XP-Arrays auf dieser Erfassungseinheit?
- Sollen insgesamt 75 oder mehr Datensammler auf dieser Erfassungseinheit eingesetzt werden?

Für jede der oben aufgeführten „Ja“-Antworten wird empfohlen, der AU 8 GB Arbeitsspeicher und 50 GB Festplattenspeicher hinzuzufügen. Wenn Sie beispielsweise beide Fragen mit „Ja“ beantwortet haben, sollten Sie ein 24-GB-Speichersystem mit 150 GB oder mehr Festplattenspeicher einsetzen. Unter Linux der Speicherplatz, der dem Protokollspeicherort hinzugefügt werden soll.

Wenden Sie sich bei weiteren Fragen zur Dimensionierung an den NetApp Support.

Konfigurieren von Erfassungseinheiten

Data Infrastructure Insights sammelt Gerätedaten mithilfe einer oder mehrerer auf lokalen Servern installierter Erfassungseinheiten. Jede Erfassungseinheit kann mehrere Datensammler hosten, die Gerätemetriken zur Analyse an Data Infrastructure Insights senden.

In diesem Thema wird beschrieben, wie Sie Erfassungseinheiten hinzufügen, und es werden zusätzliche Schritte beschrieben, die erforderlich sind, wenn Ihre Umgebung einen Proxy verwendet.

> Für eine genaue Prüfung und Datenberichterstattung wird dringend empfohlen, die Zeit auf dem Computer der Erfassungseinheit mithilfe des **Network Time Protocol (NTP)** oder des **Simple Network Time Protocol (SNTP)** zu synchronisieren.

Lesen Sie mehr über die Sicherheit von Data Infrastructure Insights"hier," .

Hinzufügen einer Linux-Erfassungseinheit

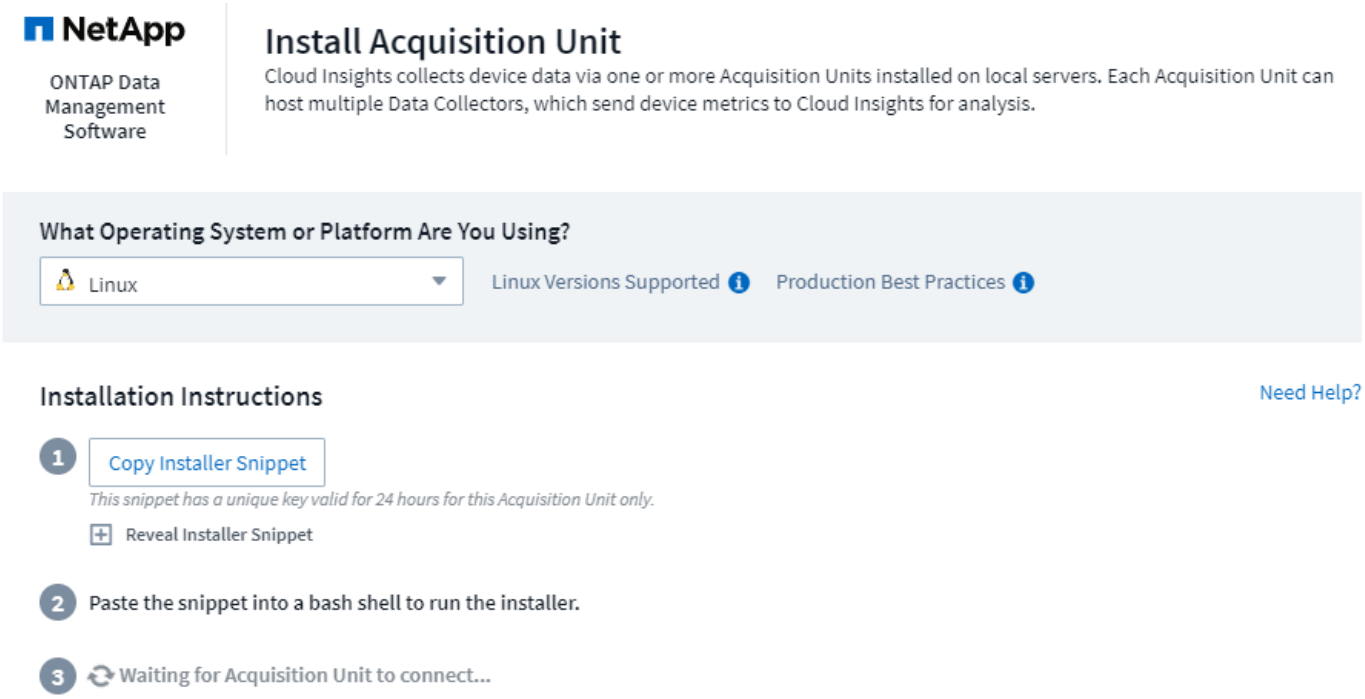
Bevor Sie beginnen

- Wenn Ihr System einen Proxy verwendet, müssen Sie die Proxy-Umgebungsvariablen festlegen, bevor die Erfassungseinheit installiert wird. Weitere Informationen finden Sie unter Festlegen von Proxy-Umgebungsvariablen .

Schritte zur Installation der Linux Acquisition Unit

1. Melden Sie sich als Administrator oder Kontoinhaber bei Ihrer Data Infrastructure Insights Umgebung an.
2. Klicken Sie auf **Beobachtbarkeit > Sammler > Erfassungseinheiten > +Erfassungseinheit**

   Das System zeigt das Dialogfeld „Erfassungseinheit installieren“ an. Wählen Sie Linux.



1. Überprüfen Sie, ob der Server oder die VM, auf dem/der die Erfassungseinheit gehostet wird, die empfohlenen Systemanforderungen erfüllt.
2. Stellen Sie sicher, dass auf dem Server eine unterstützte Linux-Version ausgeführt wird. Klicken Sie auf *Unterstützte Betriebssystemversionen (i)*, um eine Liste der unterstützten Versionen anzuzeigen.
3. Kopieren Sie den Installationsbefehlsausschnitt im Dialogfeld in ein Terminalfenster auf dem Server oder der VM, auf dem/der die Erfassungseinheit gehostet wird.
4. Fügen Sie den Befehl in die Bash-Shell ein und führen Sie ihn aus.

Nach Abschluss

- Klicken Sie auf **Beobachtbarkeit > Sammler > Erfassungseinheiten**, um den Status der Erfassungseinheiten zu überprüfen.
- Sie können auf die Protokolle der Erfassungseinheit unter /var/log/netapp/cloudinsights/acq/acq.log zugreifen.
- Verwenden Sie das folgende Skript, um die Erfassungseinheit zu steuern:
  - cloudinsights-service.sh (Stoppen, Starten, Neustarten, Status prüfen)
- Verwenden Sie das folgende Skript, um die Erfassungseinheit zu deinstallieren:
  - cloudinsights-uninstall.sh

Festlegen von Proxy-Umgebungsvariablen

Für Umgebungen, die einen Proxy verwenden, müssen Sie die Proxy-Umgebungsvariablen festlegen, bevor Sie die Erfassungseinheit hinzufügen. Die Anweisungen zum Konfigurieren des Proxys finden Sie im Dialogfeld „Erfassungseinheit hinzufügen“.

1. Klicken Sie auf + in *Haben Sie einen Proxyserver?*
2. Kopieren Sie die Befehle in einen Texteditor und legen Sie Ihre Proxyvariablen nach Bedarf fest.

   Hinweis: Beachten Sie die Einschränkungen für Sonderzeichen in den Feldern für Proxy-Benutzernamen

und -Passwörter: „%“ und „!“ sind im Feld „Benutzername“ zulässig. Im Kennwortfeld sind die Zeichen „:“, „%“ und „!“ zulässig.

3. Führen Sie den bearbeiteten Befehl in einem Terminal mithilfe der Bash-Shell aus.
4. Installieren Sie die Software der Erfassungseinheit.

Proxy-Konfiguration

Die Acquisition Unit verwendet eine 2-Wege-/gegenseitige Authentifizierung, um eine Verbindung zum Data Infrastructure Insights -Server herzustellen. Zur Authentifizierung muss das Client-Zertifikat an den Data Infrastructure Insights -Server übergeben werden. Um dies zu erreichen, muss der Proxy so eingerichtet werden, dass er die https-Anfrage an den Data Infrastructure Insights -Server weiterleitet, ohne die Daten zu entschlüsseln.

Am einfachsten ist es, in Ihrem Proxy/Ihrer Firewall eine Platzhalterkonfiguration für die Kommunikation mit Data Infrastructure Insights anzugeben, zum Beispiel:

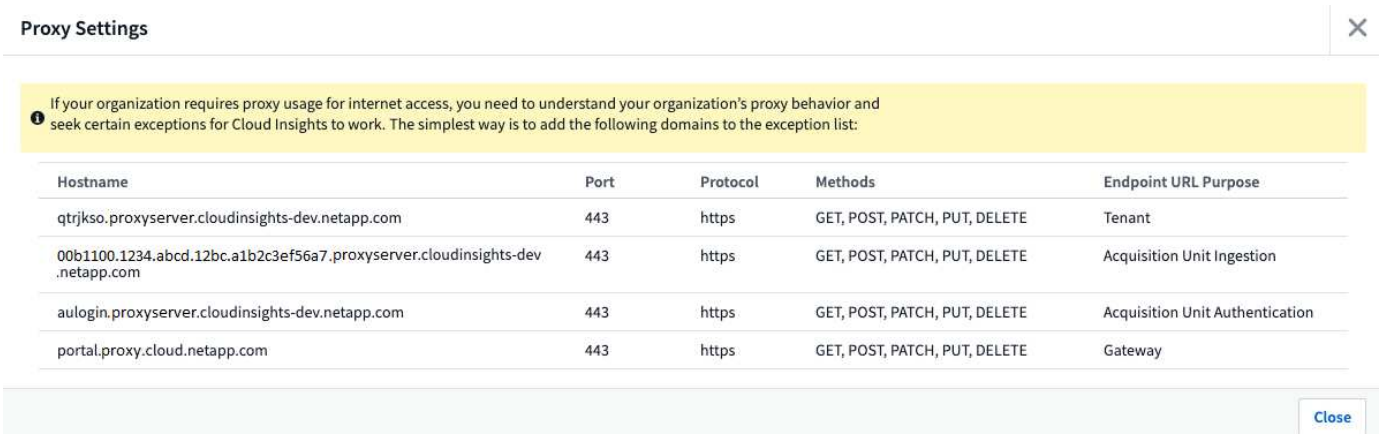
```
*.cloudinsights.netapp.com
```

Die Verwendung eines Sternchens (*) als Platzhalter ist üblich, Ihre Proxy-/Firewall-Konfiguration verwendet jedoch möglicherweise ein anderes Format. Überprüfen Sie anhand der Proxy-Dokumentation, ob die Platzhalterspezifikation in Ihrer Umgebung korrekt ist.

Weitere Informationen zur Proxy-Konfiguration finden Sie in der NetApp"Wissensdatenbank" .

Anzeigen von Proxy-URLs

Sie können die URLs Ihres Proxy-Endpunkts anzeigen, indem Sie beim Auswählen eines Datensammlers während des Onboardings auf den Link **Proxy-Einstellungen** oder auf der Seite **Hilfe > Support** auf den Link unter *Proxy-Einstellungen* klicken. Es wird eine Tabelle wie die folgende angezeigt.



Wenn Sie Workload Security auf Ihrem Mandanten haben, werden die konfigurierten Endpunkt-URLs auch in dieser Liste angezeigt.

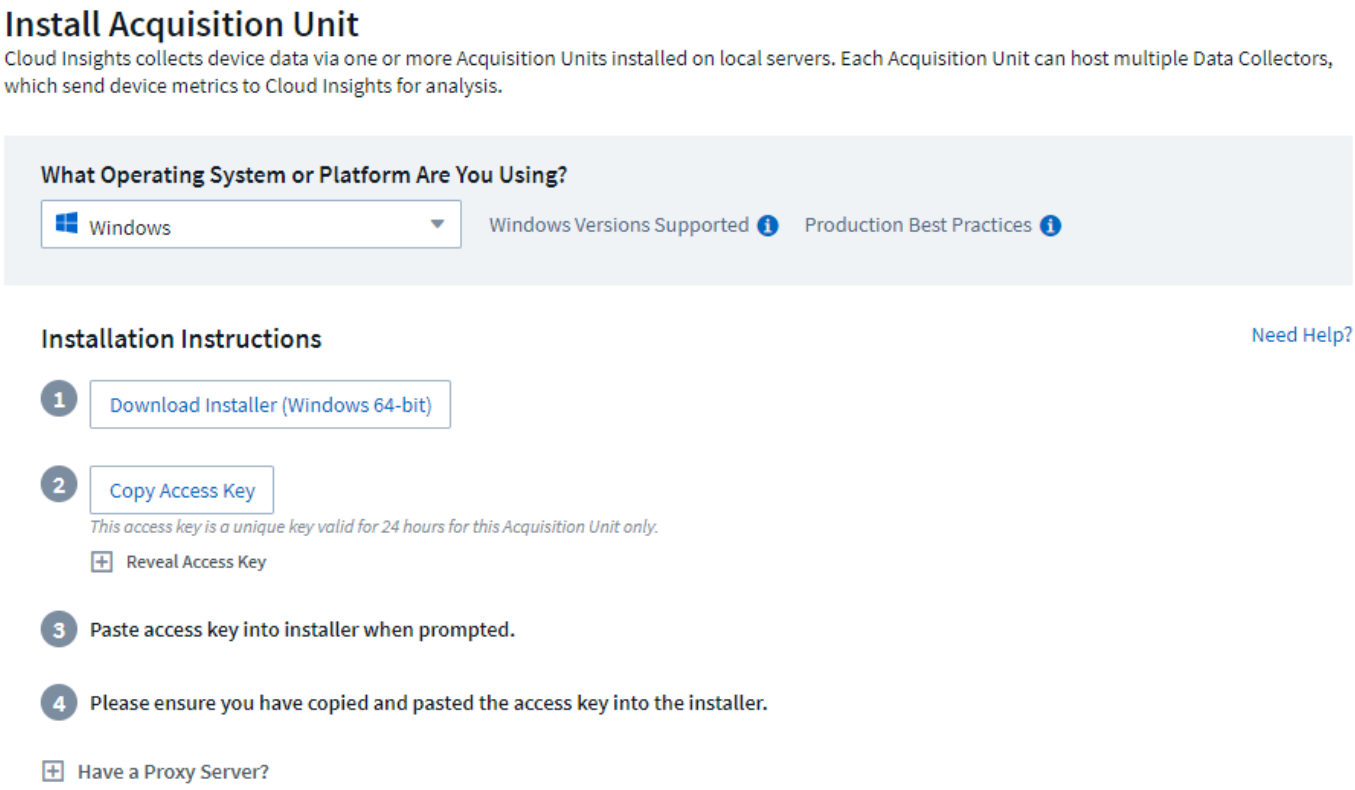
Hinzufügen einer Windows-Erfassungseinheit

Schritte zur Installation der Windows-Erfassungseinheit

1. Melden Sie sich beim Acquisition Unit-Server/VM als Benutzer mit Administratorberechtigungen an.

2. Öffnen Sie auf diesem Server ein Browserfenster und melden Sie sich als Administrator oder Kontoinhaber bei Ihrer Data Infrastructure Insights Umgebung an.
3. Klicken Sie auf **Beobachtbarkeit > Sammler > Erfassungseinheiten > +Erfassungseinheit**.

   Das System zeigt das Dialogfeld „Erfassungseinheit installieren“ an. Wählen Sie Windows.



1. Überprüfen Sie, ob der Server oder die VM, auf dem/der die Erfassungseinheit gehostet wird, die empfohlenen Systemanforderungen erfüllt.
2. Stellen Sie sicher, dass auf dem Server eine unterstützte Windows-Version ausgeführt wird. Klicken Sie auf *Unterstützte Betriebssystemversionen (i)*, um eine Liste der unterstützten Versionen anzuzeigen.
3. Klicken Sie auf die Schaltfläche **Installer herunterladen (Windows 64-Bit)**.
4. Kopieren Sie den Zugriffsschlüssel. Sie benötigen dies während der Installation.
5. Führen Sie auf dem Server/der VM der Acquisition Unit das heruntergeladene Installationsprogramm aus.
6. Fügen Sie den Zugriffsschlüssel bei entsprechender Aufforderung in den Installationsassistenten ein.
7. Während der Installation wird Ihnen die Möglichkeit geboten, Ihre Proxyserver-Einstellungen anzugeben.

Nach Abschluss

- Klicken Sie auf * > Observability > Collectors > Acquisition Units*, um den Status der Acquisition Units zu überprüfen.
- Sie können auf das Acquisition Unit-Protokoll unter <Installationsverzeichnis>\ Cloud Insights\Acquisition Unit\log\acq.log zugreifen.
- Verwenden Sie das folgende Skript, um die Erfassungseinheit zu stoppen, zu starten, neu zu starten oder ihren Status zu überprüfen:

```
cloudinsights-service.sh
```

Proxy-Konfiguration

Die Acquisition Unit verwendet eine 2-Wege-/gegenseitige Authentifizierung, um eine Verbindung zum Data Infrastructure Insights -Server herzustellen. Zur Authentifizierung muss das Client-Zertifikat an den Data Infrastructure Insights -Server übergeben werden. Um dies zu erreichen, muss der Proxy so eingerichtet werden, dass er die https-Anfrage an den Data Infrastructure Insights -Server weiterleitet, ohne die Daten zu entschlüsseln.

Am einfachsten ist es, in Ihrem Proxy/Ihrer Firewall eine Platzhalterkonfiguration für die Kommunikation mit Data Infrastructure Insights anzugeben, zum Beispiel:

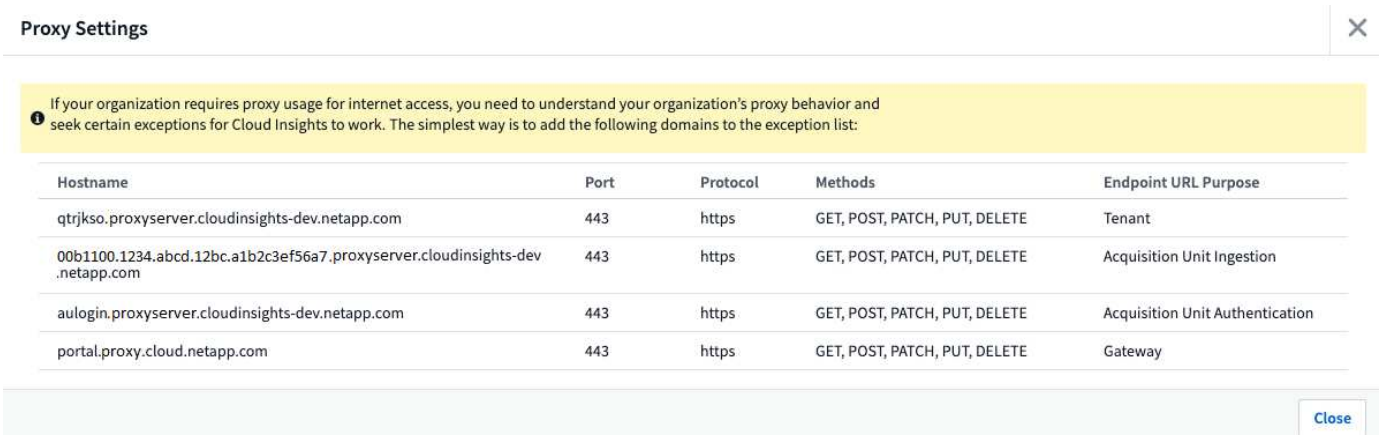
```
*.cloudinsights.netapp.com
```

Die Verwendung eines Sternchens (*) als Platzhalter ist üblich, Ihre Proxy-/Firewall-Konfiguration verwendet jedoch möglicherweise ein anderes Format. Überprüfen Sie anhand der Proxy-Dokumentation, ob die Platzhalterspezifikation in Ihrer Umgebung korrekt ist.

Weitere Informationen zur Proxy-Konfiguration finden Sie in der NetApp"Wissensdatenbank" .

Anzeigen von Proxy-URLs

Sie können die URLs Ihres Proxy-Endpunkts anzeigen, indem Sie beim Auswählen eines Datensammlers während des Onboardings auf den Link **Proxy-Einstellungen** oder auf der Seite **Hilfe > Support** auf den Link unter *Proxy-Einstellungen* klicken. Es wird eine Tabelle wie die folgende angezeigt.



Wenn Sie Workload Security auf Ihrem Mandanten haben, werden die konfigurierten Endpunkt-URLs auch in dieser Liste angezeigt.

Deinstallieren einer Erfassungseinheit

Um die Software der Erfassungseinheit zu deinstallieren, gehen Sie wie folgt vor:

Windows:

Wenn Sie eine **Windows**-Erfassungseinheit deinstallieren:

1. Öffnen Sie auf dem Server/der VM der Erfassungseinheit die Systemsteuerung und wählen Sie **Programm deinstallieren**. Wählen Sie das Data Infrastructure Insights Acquisition Unit-Programm zum Entfernen aus.
2. Klicken Sie auf „Deinstallieren“ und folgen Sie den Anweisungen.

Linux:

Wenn Sie eine **Linux**-Erfassungseinheit deinstallieren:

1. Führen Sie auf dem Server/der VM der Acquisition Unit den folgenden Befehl aus:

```
 sudo cloudinsights-uninstall.sh -p
. Um Hilfe bei der Deinstallation zu erhalten, führen Sie Folgendes aus:
```

```
sudo cloudinsights-uninstall.sh --help
```

Windows und Linux:

Nach der Deinstallation der AU:

1. Gehen Sie in Data Infrastructure Insights zu **Observability > Collectors und wählen Sie die Registerkarte *Acquisition Units** aus.
2. Klicken Sie rechts neben der Erfassungseinheit, die Sie deinstallieren möchten, auf die Schaltfläche „Optionen“ und wählen Sie „Löschen“ aus. Sie können eine Erfassungseinheit nur löschen, wenn ihr keine Datensammler zugewiesen sind.

> ⓘ Sie können keine Erfassungseinheit (AU) löschen, an die Datensammler angeschlossen sind. Verschieben Sie alle Datensammler der AU in eine andere AU (bearbeiten Sie den Sammler und wählen Sie einfach eine andere AU aus), bevor Sie die ursprüngliche AU löschen.

Zur Geräteauflösung wird eine Erfassungseinheit mit einem Stern daneben verwendet. Bevor Sie diese AU entfernen, müssen Sie eine andere AU zur Verwendung für die Geräteauflösung auswählen. Bewegen Sie den Mauszeiger über eine andere AU und öffnen Sie das Menü mit den drei Punkten, um „Für Geräteauflösung verwenden“ auszuwählen.

Neuinstallation einer Erfassungseinheit

Um eine Erfassungseinheit auf demselben Server/derselben VM neu zu installieren, müssen Sie die folgenden Schritte ausführen:

Bevor Sie beginnen

Sie müssen eine temporäre Erfassungseinheit auf einem separaten Server/VM konfiguriert haben, bevor Sie eine Erfassungseinheit neu installieren.

Schritte

1. Melden Sie sich beim Acquisition Unit-Server/VM an und deinstallieren Sie die AU-Software.
2. Melden Sie sich bei Ihrer Data Infrastructure Insights Umgebung an und gehen Sie zu **Observability > Collectors**.
3. Klicken Sie für jeden Datensammler rechts auf das Optionsmenü und wählen Sie *Bearbeiten*. Weisen Sie den Datensammler der temporären Erfassungseinheit zu und klicken Sie auf **Speichern**.

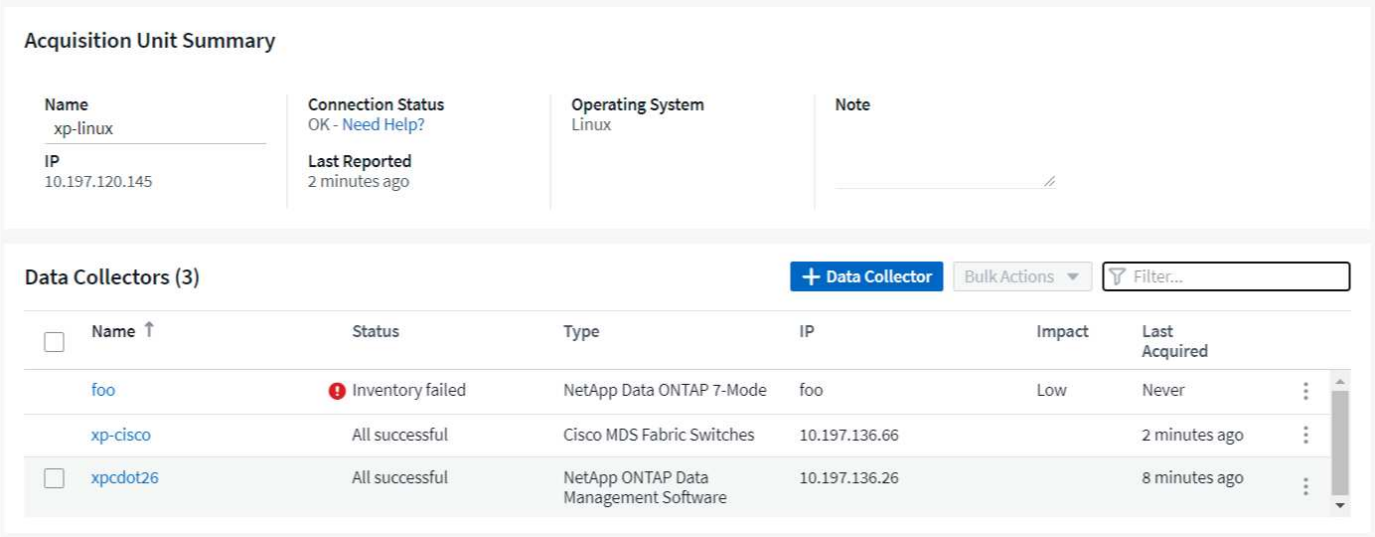
   Sie können auch mehrere Datensammler desselben Typs auswählen und auf die Schaltfläche **Massenaktionen** klicken. Wählen Sie *Bearbeiten* und weisen Sie die Datensammler der temporären Erfassungseinheit zu.

4. Nachdem alle Datensammler in die temporäre Erfassungseinheit verschoben wurden, gehen Sie zu **Beobachtbarkeit > Sammler** und wählen Sie die Registerkarte **Erfassungseinheiten** aus.
5. Klicken Sie auf die Schaltfläche „Optionen“ rechts neben der Erfassungseinheit, die Sie neu installieren möchten, und wählen Sie „Löschen“ aus. Sie können eine Erfassungseinheit nur löschen, wenn ihr keine Datensammler zugewiesen sind.
6. Sie können die Acquisition Unit-Software jetzt auf dem ursprünglichen Server/der ursprünglichen VM neu installieren. Klicken Sie auf **+Erfassungseinheit** und befolgen Sie die obigen Anweisungen, um die Erfassungseinheit zu installieren.
7. Nachdem die Erfassungseinheit neu installiert wurde, weisen Sie Ihre Datensammler wieder der Erfassungseinheit zu.

Anzeigen von AU-Details

Die Detailseite der Erfassungseinheit (AU) bietet nützliche Einzelheiten zu einer AU sowie Informationen zur Fehlerbehebung. Die AU-Detailseite enthält die folgenden Abschnitte:

- Ein **Zusammenfassungsabschnitt** mit folgendem Inhalt:
  - **Name** und **IP** der Erfassungseinheit
  - Aktueller Verbindungsstatus der AU
  - **Zuletzt gemeldet** erfolgreiche Datensammler-Abfragezeit
  - Das **Betriebssystem** der AU-Maschine
  - Alle aktuellen **Hinweise** für die AU. Verwenden Sie dieses Feld, um einen Kommentar für die AU einzugeben. Das Feld zeigt die zuletzt hinzugefügte Notiz an.
- Eine Tabelle der **Datensammler** der AU, die für jeden Datensammler Folgendes anzeigt:
  - **Name** - Klicken Sie auf diesen Link, um zur Detailseite des Datensammlers mit zusätzlichen Informationen zu gelangen
  - **Status** – Erfolgs- oder Fehlerinformationen
  - **Typ** – Anbieter/Modell
  - **IP**-Adresse des Datensammlers
  - Aktuelles **Auswirkungsniveau**
  - **Letzte Erfassung** - Zeitpunkt der letzten erfolgreichen Abfrage des Datensammlers



Sie können bei jedem Datensammler auf das Menü mit den drei Punkten klicken, um den Datensammler zu klonen, zu bearbeiten, abzufragen oder zu löschen. Sie können in dieser Liste auch mehrere Datensammler auswählen, um Massenaktionen für sie auszuführen.

Um die Erfassungseinheit neu zu starten, klicken Sie oben auf der Seite auf die Schaltfläche **Neustart**. Klicken Sie auf diese Schaltfläche, um im Falle eines Verbindungsproblems zu versuchen, die **Verbindung wiederherzustellen**.

Konfigurieren eines Agenten zum Sammeln von Daten (Windows/Linux)

Data Infrastructure Insights verwendet"Telegraf" als dessen Agent für die Erfassung von Integrationsdaten. Telegraf ist ein Plugin-gesteuerter Server-Agent, der zum Sammeln und Melden von Metriken, Ereignissen und Protokollen verwendet werden kann. Eingabe-Plugins werden verwendet, um die gewünschten Informationen im Agenten zu sammeln, indem direkt auf das System/Betriebssystem zugegriffen wird, APIs von Drittanbietern aufgerufen werden oder konfigurierte Streams abgehört werden (z. B. Kafka, statsD usw.). Ausgabe-Plugins werden verwendet, um die gesammelten Metriken, Ereignisse und Protokolle vom Agenten an Data Infrastructure Insights zu senden.

Informationen zur Installation auf Kubernetes finden Sie im"NetApp Kubernetes Monitoring Operator" Seite.

Für eine genaue Prüfung und Datenberichterstattung wird dringend empfohlen, die Zeit auf dem Agent-Computer mithilfe von **Network Time Protocol (NTP)** oder **Simple Network Time Protocol (SNTP)** zu synchronisieren.

Wenn Sie die Installationsdateien vor der Installation des Agenten überprüfen möchten, lesen Sie den Abschnitt weiter unten aufÜberprüfen der Prüfsummen von Telegraf-Paketen .

Installieren eines Agenten

Wenn Sie einen Service-Datensammler installieren und noch keinen Agenten konfiguriert haben, werden Sie aufgefordert, zuerst einen Agenten für das entsprechende Betriebssystem zu installieren. Dieses Thema enthält Anweisungen zur Installation des Telegraf-Agenten auf den folgenden Betriebssystemen:

- Windows
- RHEL und CentOS
- Ubuntu und Debian

Um einen Agenten zu installieren, müssen Sie unabhängig von der verwendeten Plattform zunächst Folgendes tun:

1. Melden Sie sich bei dem Host an, den Sie für Ihren Agenten verwenden möchten.
2. Melden Sie sich bei Ihrer Data Infrastructure Insights Umgebung an und navigieren Sie zu **Observability > Collectors**.
3. Klicken Sie auf **+Datensammler** und wählen Sie einen zu installierenden Datensammler aus.
4. Wählen Sie die passende Plattform für Ihren Host (Windows, Linux)
5. Befolgen Sie die verbleibenden Schritte für jede Plattform.

Nachdem Sie einen Agenten auf einem Host installiert haben, müssen Sie auf diesem Host keinen weiteren Agenten installieren.

Sobald Sie einen Agenten auf einem Server/einer VM installiert haben, sammelt Data Infrastructure Insights zusätzlich zu den von Ihnen konfigurierten Datensammlern auch Metriken von diesem System. Diese Kennzahlen werden wie folgt erfasst:"„Knoten“-Metriken" .

Wenn Sie einen Proxy verwenden, lesen Sie die Proxy-Anweisungen für Ihre Plattform, bevor Sie den Telegraf-Agenten installieren.

Protokollspeicherorte

Telegraf-Protokollnachrichten werden standardmäßig von stdout in die folgenden Protokolldateien umgeleitet:

- RHEL/CentOS: /var/log/telegraf/telegraf.log
- Ubuntu/Debian: /var/log/telegraf/telegraf.log
- Windows: C:\Programme\telegraf\telegraf.log

Windows

Voraussetzungen:

- PowerShell muss installiert sein
- Wenn Sie sich hinter einem Proxy befinden, müssen Sie die Anweisungen im Abschnitt **Proxy-Unterstützung für Windows konfigurieren** befolgen.

Konfigurieren der Proxy-Unterstützung für Windows

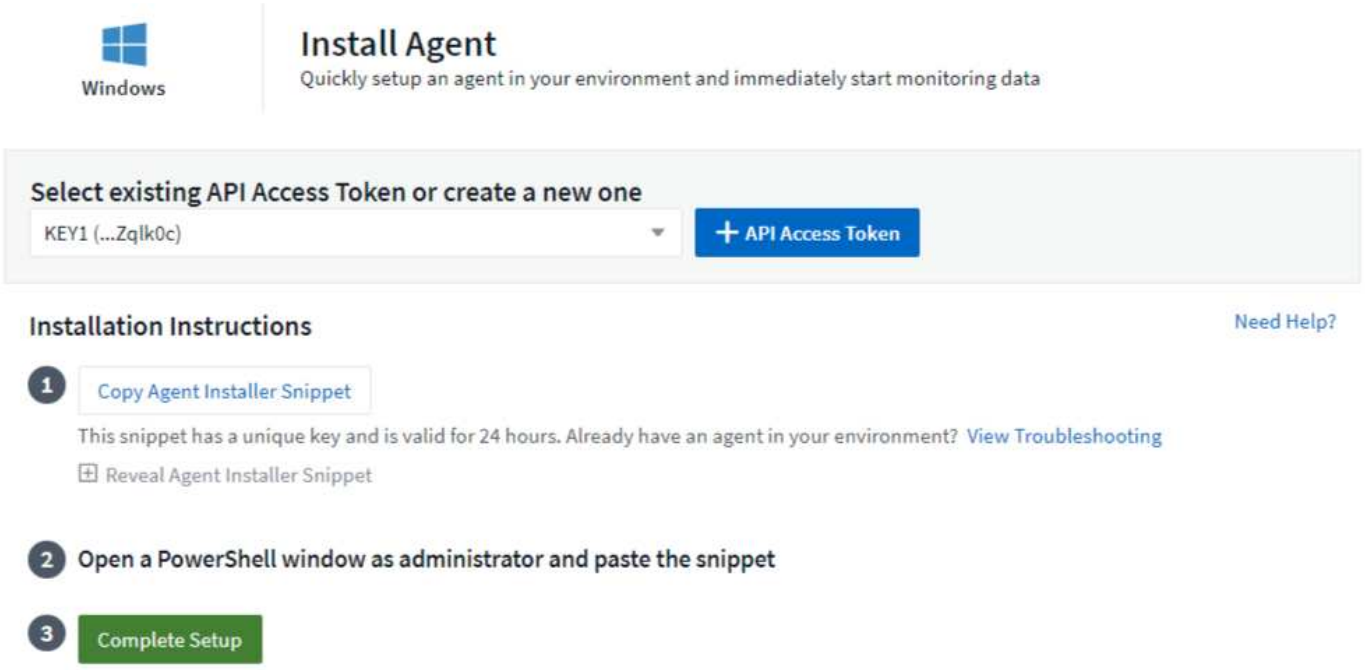
Wenn Ihre Umgebung einen Proxy verwendet, lesen Sie diesen Abschnitt vor der Installation.

Die folgenden Schritte beschreiben die Aktionen, die zum Festlegen der Umgebungsvariablen *http_proxy/https_proxy* erforderlich sind. Für einige Proxy-Umgebungen müssen Benutzer möglicherweise auch die Umgebungsvariable *no_proxy* festlegen.

Führen Sie bei Systemen, die sich hinter einem Proxy befinden, Folgendes aus, um die Umgebungsvariable(n) *https_proxy* und/oder *http_proxy* **VOR** der Installation des Telegraf-Agenten festzulegen:

```
[System.Environment]:SetEnvironmentVariable("https_proxy",
"<proxy_server>:<proxy_port>", [System.EnvironmentVariableTarget]:Machine)
```

Installieren des Agenten



Schritte zum Installieren des Agenten unter Windows:

1. Wählen Sie einen Agent-Zugriffsschlüssel.
2. Kopieren Sie den Befehlsblock aus dem Agent-Installationsdialog. Sie können auf das Zwischenablagesymbol klicken, um den Befehl schnell in die Zwischenablage zu kopieren.
3. Öffnen Sie ein PowerShell-Fenster
4. Fügen Sie den Befehl in das PowerShell-Fenster ein und drücken Sie die Eingabetaste.
5. Der Befehl lädt das entsprechende Agent-Installationsprogramm herunter, installiert es und legt eine Standardkonfiguration fest. Wenn der Vorgang abgeschlossen ist, wird der Agentendienst neu gestartet. Der Befehl hat einen eindeutigen Schlüssel und ist 24 Stunden gültig.
6. Klicken Sie auf **Fertig** oder **Weiter**

Nachdem der Agent installiert wurde, können Sie den Dienst mit den folgenden Befehlen starten/stoppen:

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

Deinstallation des Agenten

Um den Agenten unter Windows zu deinstallieren, führen Sie in einem PowerShell-Fenster die folgenden

Schritte aus:

1. Stoppen und löschen Sie den Telegraf-Dienst:

```
Stop-Service telegraf
sc.exe delete telegraf
```

2. Entfernen Sie das Zertifikat aus dem Truststore:

```
cd Cert:\CurrentUser\Root
//rm E5FB7B68C08B1CA902708584C274F8EFC7BE8ABC
rm 1A918038E8E127BB5C87A202DF173B97A05B4996
```

3. Löschen Sie den Ordner *C:\Programme\telegraf*, um die Binär-, Protokoll- und Konfigurationsdateien zu entfernen
4. Entfernen Sie den Schlüssel *SYSTEM\CurrentControlSet\Services\EventLog\Application\telegraf* aus der Registrierung

Aktualisieren des Agenten

Um den Telegraf-Agenten zu aktualisieren, gehen Sie wie folgt vor:

1. Stoppen und löschen Sie den Telegraf-Dienst:

```
Stop-Service telegraf
sc.exe delete telegraf
```

2. Löschen Sie den Schlüssel *SYSTEM\CurrentControlSet\Services\EventLog\Application\telegraf* aus der Registrierung
3. Löschen Sie *C:\Programme\telegraf\telegraf.conf*
4. Löschen Sie *C:\Programme\telegraf\telegraf.exe*
5. "Installieren des neuen Agenten" .

RHEL und CentOS

Voraussetzungen:

- Die folgenden Befehle müssen verfügbar sein: curl, sudo, ping, sha256sum, openssl und dmidecode
- Wenn Sie sich hinter einem Proxy befinden, müssen Sie die Anweisungen im Abschnitt **Proxy-Unterstützung für RHEL/CentOS konfigurieren** befolgen.

Konfigurieren der Proxy-Unterstützung für RHEL/CentOS

Wenn Ihre Umgebung einen Proxy verwendet, lesen Sie diesen Abschnitt vor der Installation.

Die folgenden Schritte beschreiben die Aktionen, die zum Festlegen der Umgebungsvariablen *http_proxy/https_proxy* erforderlich sind. Für einige Proxy-Umgebungen müssen Benutzer möglicherweise auch die Umgebungsvariable *no_proxy* festlegen.

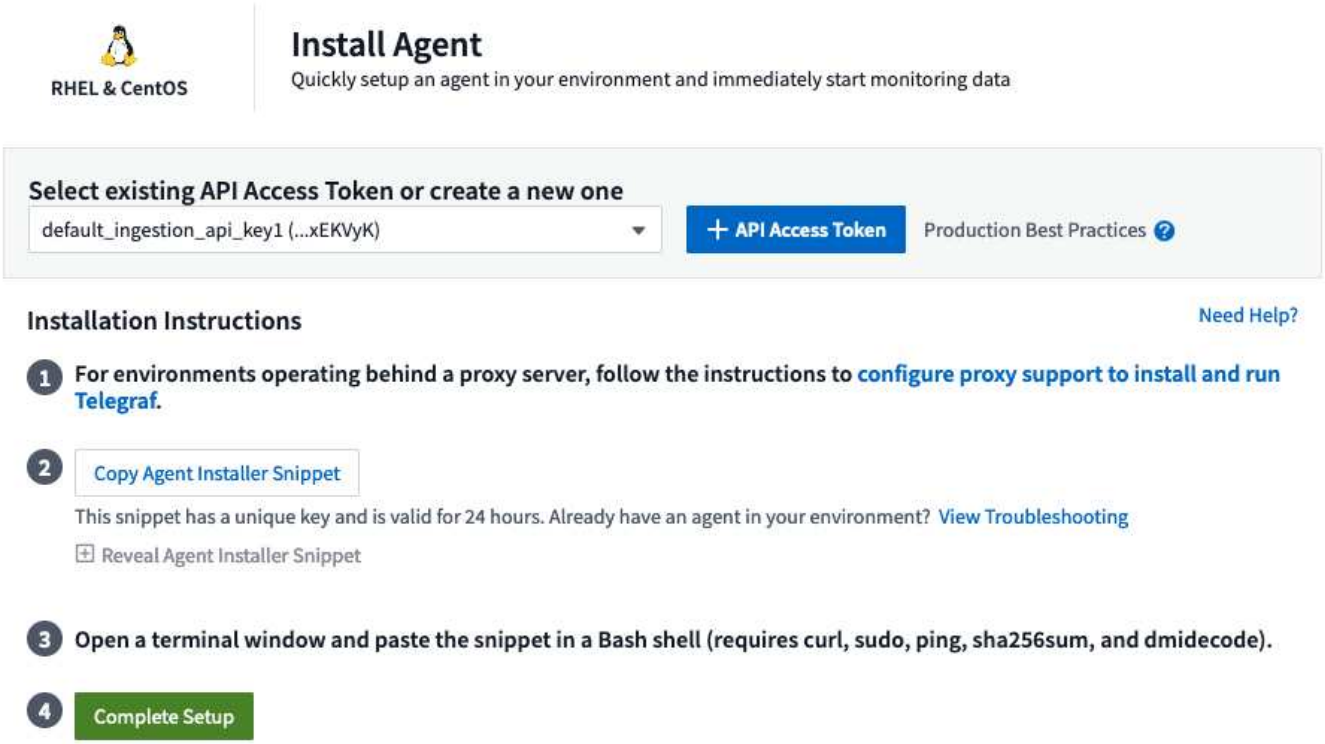
Führen Sie bei Systemen hinter einem Proxy die folgenden Schritte **VOR** der Installation des Telegraf-Agenten aus:

1. Legen Sie die Umgebungsvariable(n) *https_proxy* und/oder *http_proxy* für den aktuellen Benutzer fest:

```
 export https_proxy=<proxy_server>:<proxy_port>
. Erstellen Sie _/etc/default/telegraf_ und fügen Sie Definitionen für
die Variable(n) _https_proxy_ und/oder _http_proxy_ ein:
```

```
https_proxy=<proxy_server>:<proxy_port>
```

Installieren des Agenten



Schritte zum Installieren des Agenten auf RHEL/CentOS:

1. Wählen Sie einen Agent-Zugriffsschlüssel.
2. Kopieren Sie den Befehlsblock aus dem Agent-Installationsdialog. Sie können auf das Zwischenablagesymbol klicken, um den Befehl schnell in die Zwischenablage zu kopieren.
3. Öffnen Sie ein Bash-Fenster
4. Fügen Sie den Befehl in das Bash-Fenster ein und drücken Sie die Eingabetaste.

5. Der Befehl lädt das entsprechende Agent-Installationsprogramm herunter, installiert es und legt eine Standardkonfiguration fest. Wenn der Vorgang abgeschlossen ist, wird der Agentendienst neu gestartet. Der Befehl hat einen eindeutigen Schlüssel und ist 24 Stunden gültig.
6. Klicken Sie auf **Fertig** oder **Weiter**

Nachdem der Agent installiert wurde, können Sie den Dienst mit den folgenden Befehlen starten/stoppen:

Wenn Ihr Betriebssystem systemd verwendet (CentOS 7+ und RHEL 7+):

```
sudo systemctl start telegraf
sudo systemctl stop telegraf
```

Wenn Ihr Betriebssystem nicht systemd verwendet (CentOS 7+ und RHEL 7+):

```
sudo service telegraf start
sudo service telegraf stop
```

Deinstallation des Agenten

Um den Agenten unter RHEL/CentOS zu deinstallieren, gehen Sie in einem Bash-Terminal wie folgt vor:

1. Beenden Sie den Telegraf-Dienst:

   ```
   systemctl stop telegraf (If your operating system is using systemd
   (CentOS 7+ and RHEL 7+)
   /etc/init.d/telegraf stop (for systems without systemd support)
   ```

2. Entfernen Sie den Telegraf-Agenten:

   ```
    yum remove telegraf
   . Entfernen Sie alle Konfigurations- oder Protokolldateien, die
   möglicherweise zurückgeblieben sind:
   ```

   ```
   rm -rf /etc/telegraf*
   rm -rf /var/log/telegraf*
   ```

Aktualisieren des Agenten

Um den Telegraf-Agenten zu aktualisieren, gehen Sie wie folgt vor:

1. Stoppen Sie den Telegraf-Dienst:

```
systemctl stop telegraf (If your operating system is using systemd
(CentOS 7+ and RHEL 7+)
/etc/init.d/telegraf stop (for systems without systemd support)
```

2. Entfernen Sie den vorherigen Telegraf-Agenten:

```
 yum remove telegraf
. xref:{relative_path}#rhel-and-centos["Installieren des neuen Agenten"]
.
```

Ubuntu und Debian

Voraussetzungen:

- Die folgenden Befehle müssen verfügbar sein: curl, sudo, ping, sha256sum, openssl und dmidecode
- Wenn Sie sich hinter einem Proxy befinden, müssen Sie die Anweisungen im Abschnitt **Proxy-Unterstützung für Ubuntu/Debian konfigurieren** befolgen.

Konfigurieren der Proxy-Unterstützung für Ubuntu/Debian

Wenn Ihre Umgebung einen Proxy verwendet, lesen Sie diesen Abschnitt vor der Installation.

Die folgenden Schritte beschreiben die Aktionen, die zum Festlegen der Umgebungsvariablen *http_proxy/https_proxy* erforderlich sind. Für einige Proxy-Umgebungen müssen Benutzer möglicherweise auch die Umgebungsvariable *no_proxy* festlegen.

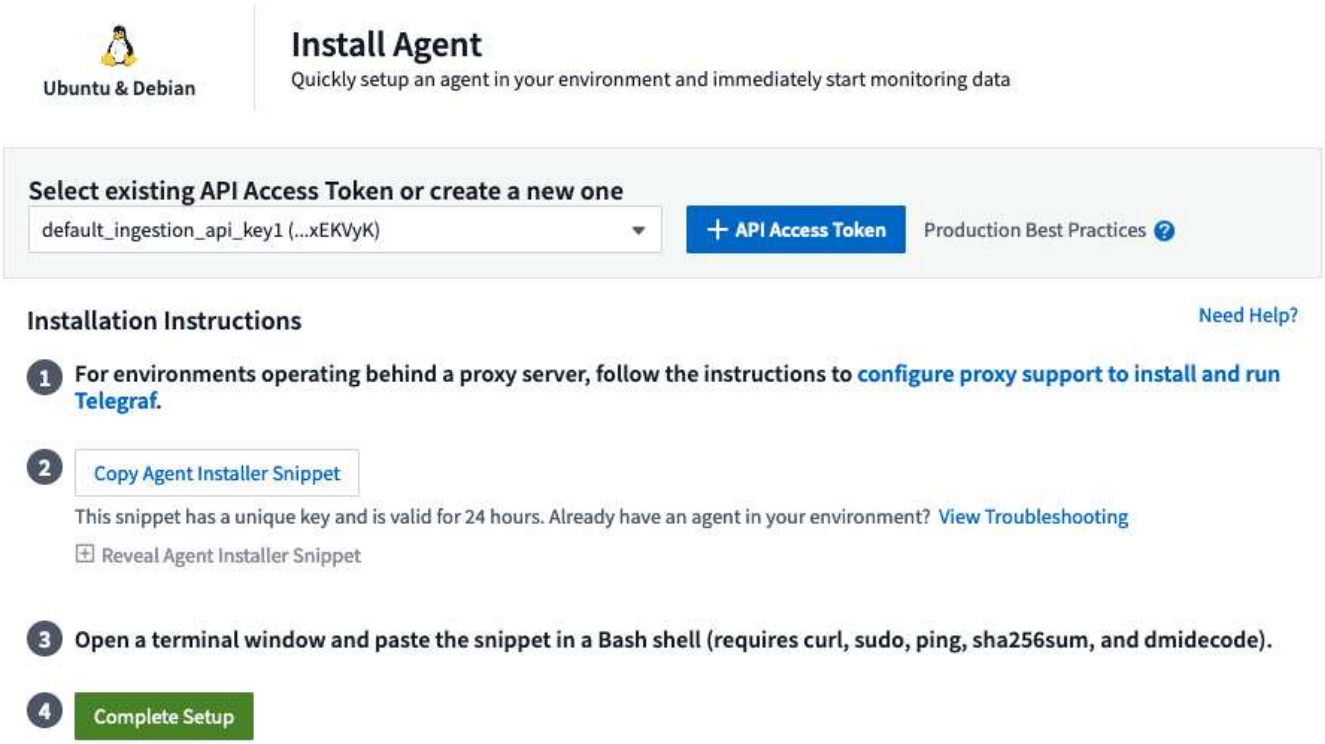
Führen Sie bei Systemen hinter einem Proxy die folgenden Schritte **VOR** der Installation des Telegraf-Agenten aus:

1. Legen Sie die Umgebungsvariable(n) *https_proxy* und/oder *http_proxy* für den aktuellen Benutzer fest:

```
 export https_proxy=<proxy_server>:<proxy_port>
. Erstellen Sie /etc/default/telegraf und fügen Sie Definitionen für die
Variable(n) _https_proxy_ und/oder _http_proxy_ ein:
```

```
https_proxy=<proxy_server>:<proxy_port>
```

Installieren des Agenten



Schritte zum Installieren des Agenten unter Debian oder Ubuntu:

1. Wählen Sie einen Agent-Zugriffsschlüssel.
2. Kopieren Sie den Befehlsblock aus dem Agent-Installationsdialog. Sie können auf das Zwischenablagesymbol klicken, um den Befehl schnell in die Zwischenablage zu kopieren.
3. Öffnen Sie ein Bash-Fenster
4. Fügen Sie den Befehl in das Bash-Fenster ein und drücken Sie die Eingabetaste.
5. Der Befehl lädt das entsprechende Agent-Installationsprogramm herunter, installiert es und legt eine Standardkonfiguration fest. Wenn der Vorgang abgeschlossen ist, wird der Agentendienst neu gestartet. Der Befehl hat einen eindeutigen Schlüssel und ist 24 Stunden gültig.
6. Klicken Sie auf **Fertig** oder **Weiter**

Nachdem der Agent installiert wurde, können Sie den Dienst mit den folgenden Befehlen starten/stoppen:

Wenn Ihr Betriebssystem systemd verwendet:

```
sudo systemctl start telegraf
sudo systemctl stop telegraf
```

Wenn Ihr Betriebssystem systemd nicht verwendet:

```
sudo service telegraf start
sudo service telegraf stop
```

Deinstallation des Agenten

Um den Agenten unter Ubuntu/Debian zu deinstallieren, führen Sie in einem Bash-Terminal Folgendes aus:

1. Beenden Sie den Telegraf-Dienst:

```
systemctl stop telegraf (If your operating system is using systemd)
/etc/init.d/telegraf stop (for systems without systemd support)
```

2. Entfernen Sie den Telegraf-Agenten:

```
 dpkg -r telegraf
. Entfernen Sie alle Konfigurations- oder Protokolldateien, die
möglicherweise zurückgeblieben sind:
```

```
rm -rf /etc/telegraf*
rm -rf /var/log/telegraf*
```

Aktualisieren des Agenten

Um den Telegraf-Agenten zu aktualisieren, gehen Sie wie folgt vor:

1. Stoppen Sie den Telegraf-Dienst:

```
systemctl stop telegraf (If your operating system is using systemd)
/etc/init.d/telegraf stop (for systems without systemd support)
```

2. Entfernen Sie den vorherigen Telegraf-Agenten:

```
 dpkg -r telegraf
. xref:{relative_path}#ubuntu-and-debian["Installieren des neuen
Agenten"] .
```

Überprüfen der Prüfsummen von Telegraf-Paketen

Das Installationsprogramm des Data Infrastructure Insights -Agenten führt Integritätsprüfungen durch, einige Benutzer möchten jedoch möglicherweise eigene Überprüfungen durchführen, bevor sie die heruntergeladene Telegraf-Binärdatei installieren. Dies kann durch Herunterladen des Installationsprogramms und Generieren einer Prüfsumme für das heruntergeladene Paket erfolgen. Anschließendes Vergleichen der Prüfsumme mit dem in den Installationsanweisungen angezeigten Wert.

Laden Sie das Installationspaket herunter, ohne es zu installieren

Um einen reinen Downloadvorgang durchzuführen (im Gegensatz zum standardmäßigen Herunterladen und Installieren), können Benutzer den von der Benutzeroberfläche erhaltenen Agenteninstallationsbefehl bearbeiten und die Option „Installieren“ entfernen.

Gehen Sie folgendermaßen vor:

1. Kopieren Sie den Agent Installer-Ausschnitt wie angegeben.
2. Fügen Sie den Codeausschnitt nicht in ein Befehlsfenster ein, sondern in einen Texteditor.
3. Entfernen Sie das abschließende „--install“ (Linux) oder „-install“ (Windows) aus dem Befehl.
4. Kopieren Sie den gesamten Befehl aus dem Texteditor.
5. Fügen Sie es nun in Ihr Befehlsfenster (in einem Arbeitsverzeichnis) ein und führen Sie es aus.

Nicht-Windows (diese Beispiele gelten für Kubernetes; die tatsächlichen Skriptnamen können abweichen):

- Herunterladen und installieren (Standard):

```
 installerName=cloudinsights-ubuntu_debian.sh … && ./$installerName
--download --verify && sudo -E -H ./$installerName --install
* Nur zum Herunterladen:
```

```
installerName=cloudinsights-ubuntu_debian.sh … && ./$installerName
--download --verify
```

Windows:

- Herunterladen und installieren (Standard):

```
 !$($installerName=".\cloudinsights-windows.ps1") … -and $(if(((Get-
FileHash $installerName).Hash).ToLower() -eq "INSTALLER_CHECKSUM ") {
&$installerName -download -verify -install } else { Write-Host "Install
script checksum does not match"})"
* Nur zum Herunterladen:
```

```
!$($installerName=".\cloudinsights-windows.ps1") … -and $(if(((Get-
FileHash $installerName).Hash).ToLower() -eq "INSTALLER_CHECKSUM ") {
&$installerName -download -verify } else { Write-Host "Install script
checksum does not match"})"
```

Der Nur-Download-Befehl lädt alle erforderlichen Artefakte von Data Infrastructure Insights in das Arbeitsverzeichnis herunter. Zu den Artefakten zählen unter anderem:

- ein Installationsskript
- eine Umgebungsdatei
- eine Telegraf-Binärdatei
- eine Signatur für die Telegraf-Binärdatei
- ein öffentliches Zertifikat zur Überprüfung der Binärsignatur

Das von DII heruntergeladene und kopierte Installations-Snippet führt automatisch eine Prüfsumme des Installationsskripts aus und die Signatur der Telegraf-Binärdatei wird durch das Installationsskript überprüft.

Prüfsummenwert überprüfen

Um den Prüfsummenwert zu generieren, führen Sie den folgenden Befehl für Ihre entsprechende Plattform aus:

- RHEL/Ubuntu:

```
 sha256sum <package_name>
* Windows:
```

```
Get-FileHash telegraf.zip -Algorithm SHA256 | Format-List
```

Installieren Sie das heruntergeladene Paket

Sobald alle Artefakte zufriedenstellend überprüft wurden, kann die Agenteninstallation durch Ausführen des folgenden Befehls gestartet werden:

Nicht-Windows:

```
 sudo -E -H ./<installation_script_name> --install
Windows:
```

```
.\cloudinsights-windows.ps1 -install
```

Erstellen und Verwenden von API-Zugriffstoken

Um ein API-Zugriffstoken für die Telegraf-Datenaufnahme zu erstellen, führen Sie bitte einen der folgenden Schritte aus:

Erstellen über die Data Collector-Installationsseite

1. Navigieren Sie zur Data Collector-Installationsseite für die Plattform, die Sie verwenden möchten (Windows, Linux).
2. Erstellen Sie ein Token mit der Schaltfläche + API-Zugriffstoken.
3. Geben Sie einen Namen ein und klicken Sie auf „Speichern“.

4. Der Tokenname sollte jetzt im Dropdown-Menü ausgewählt werden und wird bei der Installation des Collectors verwendet.

Manuelles Erstellen eines API-Zugriffstokens

1. Navigieren Sie zu Admin > API-Zugriff.
2. Klicken Sie auf + API-Zugriffstoken.
3. Geben Sie einen Namen und optional eine Beschreibung ein.
4. Wählen Sie unter „Für Aufrufe welcher API-Typen wird dieses Token verwendet?“ nur „Datenaufnahme“ aus und deaktivieren Sie dann „Erfassungseinheit“.
5. Wählen Sie unter „Berechtigungen“ Lesen/Schreiben aus.
6. Deaktivieren Sie „Token für Kubernetes automatisch rotieren“.

Um Ihr neu erstelltes API-Zugriffstoken zu verwenden, wählen Sie es aus der Dropdown-Liste „Vorhandenes API-Zugriffstoken auswählen oder neues erstellen“ auf der Installationsseite aus. Bitte beachten Sie, dass nur Token mit den folgenden Eigenschaften verwendet werden können:

- API-Typ: Nur „Datenaufnahme“
- Berechtigungen: Lesen/Schreiben
- Automatische Kubernetes-Rotation: Aus

Fehlerbehebung

Wenn beim Einrichten eines Agenten Probleme auftreten, können Sie Folgendes versuchen:

Problem:	Versuchen Sie Folgendes:
Nach der Konfiguration eines neuen Plug-Ins und dem Neustart von Telegraf kann Telegraf nicht gestartet werden. Die Protokolle zeigen einen Fehler ähnlich dem folgenden an: „[telegraf] Fehler beim Ausführen des Agenten: Fehler beim Laden der Konfigurationsdatei /etc/telegraf/telegraf.d/cloudinsights-default.conf: Plugin-Ausgaben.http: Zeile <Zeilennummer>: In der Konfiguration wurden die Felder ["use_system_proxy"] angegeben, aber sie wurden nicht verwendet.“	Die installierte Telegraf-Version ist veraltet. Befolgen Sie die Schritte auf dieser Seite, um den **Agenten** für Ihre entsprechende Plattform zu aktualisieren.
Ich habe das Installationsskript auf einer alten Installation ausgeführt und jetzt sendet der Agent keine Daten	Deinstallieren Sie den Telegraf-Agenten und führen Sie das Installationsskript erneut aus. Befolgen Sie die Schritte zum **Aktualisieren des Agenten** auf dieser Seite für Ihre entsprechende Plattform.
Ich habe bereits einen Agenten mit Data Infrastructure Insights installiert	Wenn Sie bereits einen Agenten auf Ihrem Host/Ihrer VM installiert haben, müssen Sie den Agenten nicht erneut installieren. Wählen Sie in diesem Fall einfach die entsprechende Plattform und den entsprechenden Schlüssel im Bildschirm „Agent-Installation“ aus und klicken Sie auf „Weiter“ oder „Fertig stellen“.

Problem:	Versuchen Sie Folgendes:
Ich habe bereits einen Agenten installiert, aber nicht mithilfe des Data Infrastructure Insights -Installationsprogramms	Entfernen Sie den vorherigen Agenten und führen Sie die Installation des Data Infrastructure Insights Agenten aus, um die richtigen Standardeinstellungen der Konfigurationsdatei sicherzustellen. Wenn Sie fertig sind, klicken Sie auf **Weiter** oder **Fertig**.

Weitere Informationen finden Sie in der"Support" Seite oder in der"Datensammler-Supportmatrix" .

Konfigurieren von Datenkollektoren

Sie konfigurieren Datenkollektoren in Ihrer Data Infrastructure Insights Umgebung, um Daten von Geräten im Rechenzentrum zu erfassen.

Bevor Sie beginnen

- Sie müssen eine Erfassungseinheit konfiguriert haben, bevor Sie mit der Datenerfassung beginnen können.
- Sie benötigen Anmeldeinformationen für die Geräte, von denen Sie Daten erfassen.
- Für alle Geräte, von denen Sie Daten erfassen, sind Gerätenetzwerkadressen, Kontoinformationen und Passwörter erforderlich.

Schritte

1. Klicken Sie im Menü „Data Infrastructure Insights“ auf **Observability > Collectors**

   Das System zeigt die verfügbaren Datensammler nach Anbieter sortiert an.

2. Klicken Sie auf **+ Collector** und wählen Sie den zu konfigurierenden Datensammler aus.

   Im Dialogfeld können Sie den Datensammler konfigurieren und eine Erfassungseinheit hinzufügen.

3. Geben Sie einen Namen für den Datensammler ein.
4. Klicken Sie auf **Erweiterte Konfiguration**, um zusätzliche Konfigurationsfelder hinzuzufügen. (Nicht alle Datensammler erfordern eine erweiterte Konfiguration.)
5. Klicken Sie auf **Konfiguration testen**, um zu überprüfen, ob der Datensammler richtig konfiguriert ist.
6. Klicken Sie auf **Collector hinzufügen**, um die Konfiguration zu speichern und den Datensammler zu Ihrem Data Infrastructure Insights Mandanten hinzuzufügen.

Es kann bis zu zwei Abfrageperioden dauern, bis Daten des Dienstes in Dashboards angezeigt werden oder für Abfragen verfügbar sind.

- 1. Bestandsaufnahme: sofort
- 1. Leistungsdatenabfrage zur Ermittlung einer Baseline: unmittelbar nach der Bestandsabfrage
- 2. Leistungsumfrage: innerhalb von 15 Sekunden nach Abschluss der 1. Leistungsumfrage

Die Abfrage erfolgt dann gemäß den konfigurierten Bestands- und Leistungsabfrageintervallen.

Ermitteln des Erfassungsstatus des Datensammlers

Da Datensammler die primäre Informationsquelle für Data Infrastructure Insights sind,

müssen Sie unbedingt sicherstellen, dass sie in einem laufenden Zustand bleiben.

Der Status des Datensammlers wird in der oberen rechten Ecke jeder Asset-Seite als Meldung „Vor N Minuten erfasst“ angezeigt, wobei N den aktuellsten Erfassungszeitpunkt des/der Datensammlers/Datensammler des Assets angibt. Außerdem werden Uhrzeit und Datum der Erfassung angezeigt.

Wenn Sie auf die Nachricht klicken, wird eine Tabelle mit dem Namen, dem Status und der letzten erfolgreichen Erfassungszeit des Datensammlers angezeigt. Wenn Sie als Administrator angemeldet sind, gelangen Sie durch Klicken auf den Link mit dem Namen des Datensammlers in der Tabelle zur Detailseite dieses Datensammlers.

Verwalten konfigurierter Datenkollektoren

Die Seite „Installierte Datensammler“ bietet Zugriff auf die Datensammler, die für Data Infrastructure Insights konfiguriert wurden. Auf dieser Seite können Sie vorhandene Datensammler ändern.

Schritte

1. Klicken Sie im Menü „Data Infrastructure Insights“ auf **Observability > Collectors**

   Der Bildschirm „Verfügbare Datensammler“ wird angezeigt.

2. Klicken Sie auf **Installierte Datensammler**

   Es wird eine Liste aller installierten Datensammler angezeigt. Die Liste enthält den Namen und Status des Collectors, die IP-Adresse, auf die der Collector zugreift, und das Datum, an dem zuletzt Daten von einem Gerät abgerufen wurden. Auf diesem Bildschirm können unter anderem folgende Aktionen ausgeführt werden:

   - Kontrollabfragen
   - Ändern der Anmeldeinformationen des Datensammlers
   - Klonen von Datensammlern

Steuern der Datensammlerabfrage

Nachdem Sie eine Änderung an einem Datensammler vorgenommen haben, möchten Sie möglicherweise, dass dieser sofort eine Abfrage durchführt, um Ihre Änderungen zu überprüfen. Oder Sie möchten die Datenerfassung auf einem Datensammler um einen, drei oder fünf Tage verschieben, während Sie an einem Problem arbeiten.

Schritte

1. Klicken Sie im Menü „Data Infrastructure Insights“ auf **Observability > Collectors**
2. Klicken Sie auf **Installierte Datensammler**
3. Aktivieren Sie das Kontrollkästchen links neben dem Datensammler, den Sie ändern möchten
4. Klicken Sie auf **Massenaktionen** und wählen Sie die gewünschte Umfrageaktion aus.

   Massenaktionen können gleichzeitig auf mehreren Datensammlern ausgeführt werden. Wählen Sie die Datensammler aus und wählen Sie die auszuführende Aktion aus dem Menü **Massenaktion**.

Bearbeiten von Datenkollektorinformationen

Sie können vorhandene Einrichtungsinformationen des Datensammlers bearbeiten.

So bearbeiten Sie einen einzelnen Datensammler:

1. Klicken Sie im Menü „Data Infrastructure Insights“ auf **Observability > Collectors**, um die Liste der installierten Datensammler zu öffnen.
2. Klicken Sie im Optionsmenü rechts neben dem Datensammler, den Sie ändern möchten, auf **Bearbeiten**.

   Der Dialog „Collector bearbeiten“ wird geöffnet.

3. Geben Sie die Änderungen ein und klicken Sie auf **Konfiguration testen**, um die neue Konfiguration zu testen, oder klicken Sie auf **Speichern**, um die Konfiguration zu speichern.

Sie können auch mehrere Datensammler bearbeiten:

1. Aktivieren Sie das Kontrollkästchen links neben jedem Datensammler, den Sie ändern möchten.
2. Klicken Sie auf die Schaltfläche **Massenaktionen** und wählen Sie **Bearbeiten**, um das Dialogfeld „Datensammler bearbeiten“ zu öffnen.
3. Ändern Sie die Felder wie oben.

   Die ausgewählten Datensammler müssen vom selben Anbieter und Modell sein und sich auf derselben Erfassungseinheit befinden.

   Beim Bearbeiten mehrerer Datensammler wird im Feld „Name des Datensammlers“ „Gemischt“ angezeigt und kann nicht bearbeitet werden. Andere Felder wie Benutzername und Passwort zeigen „Gemischt“ an und können bearbeitet werden. Felder, die in allen ausgewählten Datensammlern denselben Wert aufweisen, zeigen die aktuellen Werte an und können bearbeitet werden.

   Beim Bearbeiten mehrerer Datensammler ist die Schaltfläche **Konfiguration testen** nicht verfügbar.

Klonen von Datenkollektoren

Mithilfe der Klonfunktion können Sie schnell eine Datenquelle hinzufügen, die über dieselben Anmeldeinformationen und Attribute wie eine andere Datenquelle verfügt. Durch Klonen können Sie problemlos mehrere Instanzen desselben Gerätetyps konfigurieren.

Schritte

1. Klicken Sie im Menü „Data Infrastructure Insights“ auf **Observability > Collectors**.
2. Klicken Sie auf **Installierte Datensammler**.
3. Klicken Sie auf das Kontrollkästchen links neben dem Datensammler, den Sie kopieren möchten.
4. Klicken Sie im Optionsmenü rechts neben dem ausgewählten Datensammler auf **Klonen**.

   Das Dialogfeld „Datensammler klonen“ wird angezeigt.

5. Geben Sie in den erforderlichen Feldern neue Informationen ein.
6. Klicken Sie auf **Speichern**.

Nach Abschluss

Der Klonvorgang kopiert alle anderen Attribute und Einstellungen, um den neuen Datensammler zu erstellen.

Durchführen von Massenaktionen auf Datensammlern

Sie können einige Informationen für mehrere Datensammler gleichzeitig bearbeiten. Mit dieser Funktion können Sie eine Umfrage starten, die Umfrage verschieben und die Umfrage auf mehreren Datensammlern fortsetzen. Darüber hinaus können Sie mehrere Datensammler löschen.

Schritte

1. Klicken Sie im Menü „Data Infrastructure Insights“ auf **Observability > Collectors**
2. Klicken Sie auf **Installierte Datensammler**
3. Klicken Sie auf das Kontrollkästchen links neben den Datensammlern, die Sie ändern möchten.
4. Klicken Sie im Optionsmenü rechts auf die Option, die Sie ausführen möchten.

Nach Abschluss

Der von Ihnen ausgewählte Vorgang wird auf den Datensammlern ausgeführt. Wenn Sie sich für das Löschen von Datensammlern entscheiden, wird ein Dialogfeld angezeigt, in dem Sie aufgefordert werden, die Aktion zu bestätigen.

Untersuchung eines gescheiterten Datensammlers

Wenn ein Datensammler eine Fehlermeldung und eine hohe oder mittlere Auswirkung aufweist, müssen Sie dieses Problem mithilfe der Übersichtsseite des Datensammlers und der darin verknüpften Informationen untersuchen.

Führen Sie die folgenden Schritte aus, um die Ursache für fehlgeschlagene Datensammler zu ermitteln. Fehlermeldungen zum Datensammler werden im Menü **Admin** und auf der Seite **Installierte Datensammler** angezeigt.

Schritte

1. Klicken Sie auf **Admin** > **Datensammler** > **Installierte Datensammler**.
2. Klicken Sie auf den verknüpften Namen des fehlerhaften Datensammlers, um die Seite „Zusammenfassung“ zu öffnen.
3. Überprüfen Sie auf der Seite „Zusammenfassung“ den Bereich „Kommentare“, um alle Notizen zu lesen, die möglicherweise von einem anderen Techniker hinterlassen wurden, der diesen Fehler möglicherweise ebenfalls untersucht.
4. Beachten Sie alle Leistungsmeldungen.
5. Bewegen Sie den Mauszeiger über die Segmente des Ereigniszeitleistendiagramms, um zusätzliche Informationen anzuzeigen.
6. Wählen Sie eine Fehlermeldung für ein Gerät aus, die unterhalb der Ereigniszeitleiste angezeigt wird, und klicken Sie auf das Symbol „Fehlerdetails“, das rechts neben der Meldung angezeigt wird.

   Die Fehlerdetails umfassen den Text der Fehlermeldung, die wahrscheinlichsten Ursachen, verwendete Informationen und Vorschläge, was zur Behebung des Problems versucht werden kann.

7. Im Bereich „Von diesem Datensammler gemeldete Geräte“ können Sie die Liste filtern, um nur die Geräte anzuzeigen, die Sie interessieren, und Sie können auf den verknüpften **Namen** eines Geräts klicken, um die Asset-Seite für dieses Gerät anzuzeigen.
8. Wenn Sie zur Übersichtsseite des Datensammlers zurückkehren, überprüfen Sie den Bereich **Letzte Änderungen anzeigen** unten auf der Seite, um festzustellen, ob das Problem durch kürzliche Änderungen verursacht worden sein könnte.

Dashboards importieren

Data Infrastructure Insights bietet eine Reihe empfohlener Dashboards, um geschäftliche Einblicke in Ihre Daten zu gewähren. Jedes Dashboard enthält Widgets, die Ihnen dabei helfen sollen, eine bestimmte Frage zu beantworten oder ein bestimmtes Problem zu lösen, das für die Daten relevant ist, die derzeit über Ihren Mandanten erfasst werden. Mit DII können Sie auch ein nützliches Dashboard exportieren und in einen anderen Mandanten importieren.

Importieren aus der Dashboard-Galerie

Um ein Dashboard aus der Galerie zu importieren, gehen Sie wie folgt vor:

1. Wählen Sie **Observability > Explore > All Dashboards**
2. Klicken Sie auf **+Dashboard importieren** und wählen Sie *Aus Galerie importieren*.

   Basierend auf den Datensammlern in Ihrer Umgebung wird eine Liste mit **empfohlenen Dashboards** angezeigt. Zur Beantwortung von Fragen zu verschiedenen Objekttypen, darunter AWS, NetApp, Storage, VMware und andere, stehen Dashboards zur Verfügung.

3. Wählen Sie ein oder mehrere Dashboards aus der Liste aus und klicken Sie auf **Dashboards hinzufügen**. Diese Dashboards werden in Ihrer Dashboard-Liste angezeigt.

Zusätzlich zu den empfohlenen Dashboards können Sie auch **zusätzliche Dashboards** importieren, die für Ihre aktuellen Daten nicht relevant sind. Wenn Sie beispielsweise derzeit keine Speicherdatensammler installiert haben, aber planen, in Zukunft welche zu konfigurieren, können Sie dennoch die speicherrelevanten Dashboards importieren. Diese Dashboards stehen zur Anzeige zur Verfügung, zeigen jedoch möglicherweise keine relevanten Daten an, bis mindestens ein Speicherdatensammler konfiguriert ist.

Der Import aus der Dashboard-Galerie ist für Benutzer mit der Rolle „Administrator“ oder „Kontoinhaber“ verfügbar.

Importieren eines exportierten Dashboards

Um ein Dashboard zu **exportieren**, klicken Sie auf der Seite **Observability > Explore > All Dashboards** auf das Menü rechts neben dem Dashboard und wählen Sie *Export*. Sie können auch mehrere Dashboards auswählen und im Dropdown-Menü „Massenaktionen“ die Option „Exportieren“ wählen. Die Dashboards werden in einer ZIP-Datei auf Ihrem lokalen System gespeichert.

Um das Dashboard zu **importieren**, navigieren Sie zum gewünschten Mandanten und gehen Sie wie folgt vor:

1. Wählen Sie **Observability > Explore > All Dashboards**
2. Klicken Sie auf **+Dashboard importieren** und wählen Sie *Aus Datei importieren*. Wählen Sie die ZIP-Datei der zuvor exportierten Datei aus. Die Dashboards werden importiert und in Ihrer Dashboard-Liste angezeigt. Beachten Sie, dass beim Importieren eines Dashboards mit demselben Namen wie ein vorhandenes Dashboard eine „(2)“ an den Dashboard-Namen angehängt wird.

Benutzerkonten und Rollen

Data Infrastructure Insights bietet bis zu vier Benutzerkontorollen: Kontoinhaber, Administrator, Benutzer und Gast. Jedem Konto sind bestimmte Berechtigungsstufen

zugewiesen, wie in der folgenden Tabelle aufgeführt. Benutzer sind entweder"eingeladen" zu Data Infrastructure Insights und einer bestimmten Rolle zugewiesen, oder können sich anmelden über"Single Sign-On (SSO)-Autorisierung" mit einer Standardrolle. Die SSO-Autorisierung ist als Funktion in der Data Infrastructure Insights Premium Edition verfügbar.

Berechtigungsstufen

Sie verwenden ein Konto mit Administratorrechten, um Benutzerkonten zu erstellen oder zu ändern. Jedem Benutzerkonto wird für jede Data Infrastructure Insights -Funktion eine Rolle aus den folgenden Berechtigungsstufen zugewiesen.

Rolle	Beobachtbarkeit	Workload-Sicherheit	Berichterstattung	Administrator
Kontoinhaber	Dasselbe wie Administrator	Dasselbe wie Administrator	Dasselbe wie Administrator	Dasselbe wie Administrator und außerdem Verwaltung der SSO-Authentifizierung und der Identity Federation-Konfiguration. Kann auch zusätzliche Eigentümer zuweisen.
Administrator	Kann alle Observability-Funktionen sowie die Verwaltung von Datensammlern ausführen.	Kann alle Sicherheitsfunktionen ausführen, einschließlich Warnungen, Forensik, Datensammler, Richtlinien für automatisierte Antworten und API-Token für die Sicherheit. Ein Administrator kann auch andere Benutzer einladen, aber nur Sicherheitsrollen zuweisen.	Kann alle Benutzer-/Autorenfunktionen ausführen, einschließlich der Verwaltung von Reporting-API-Token, sowie alle Verwaltungsaufgaben wie die Konfiguration von Berichten und das Herunterfahren und Neustarten von Berichtsaufgaben. Ein Administrator kann auch andere Benutzer einladen, aber nur Berichtsrollen zuweisen.	Kann andere Benutzer einladen, aber nur Observability-Rollen zuweisen. Kann die SSO-Konfiguration anzeigen, aber nicht ändern. Kann API-Zugriffstoken erstellen und verwalten. Kann Auditinformationen anzeigen. Kann Abonnementinformationen, Nutzung und Verlauf anzeigen. Kann globale Empfängerlisten für Warnbenachrichtigungen und Abonnementbenachrichtigungen verwalten.

Rolle	Beobachtbarkeit	Workload-Sicherheit	Berichterstattung	Administrator
Benutzer	Kann Dashboards, Abfragen, Warnungen, Anmerkungen, Anmerkungsregeln und Anwendungen anzeigen und ändern sowie die Geräteauflösung verwalten.	Kann Warnungen anzeigen und verwalten sowie forensische Daten anzeigen. Die Benutzerrolle kann den Alarmstatus ändern, eine Notiz hinzufügen, manuell Schnappschüsse erstellen und den eingeschränkten Benutzerzugriff verwalten.	Kann alle Gast-/Verbraucherfunktionen ausführen sowie Berichte und Dashboards erstellen und verwalten.	Nicht verfügbar
Gast	Hat schreibgeschützten Zugriff auf Asset-Seiten, Dashboards und Warnungen und kann Abfragen anzeigen und ausführen.	Kann Warnungen und Forensik anzeigen. Mit der Gastrolle können Sie den Alarmstatus nicht ändern, keine Notiz hinzufügen, manuell Schnappschüsse erstellen oder den Benutzerzugriff einschränken.	Kann Berichte anzeigen, planen und ausführen und persönliche Einstellungen wie Sprachen und Zeitzonen festlegen. Gäste/Verbraucher können keine Berichte erstellen oder Verwaltungsaufgaben ausführen.	Nicht verfügbar

Es empfiehlt sich, die Anzahl der Benutzer mit Administratorberechtigungen zu begrenzen. Die meisten Konten sollten Benutzer- oder Gastkonten sein.

Data Infrastructure Insights Berechtigungen nach Benutzerrolle

Die folgende Tabelle zeigt die den einzelnen Benutzerrollen erteilten Data Infrastructure Insights Berechtigungen.

Funktion	Administrator/Kontoinhaber	Benutzer	Gast
Erfassungseinheiten: Hinzufügen/Ändern/Löschen	Y	N	N
Warnungen*: Erstellen/Ändern/Löschen	Y	Y	N
Benachrichtigungen*: Anzeigen	Y	Y	Y
Anmerkungsregeln: Erstellen/Ausführen/Ändern/Löschen	Y	Y	N

Anmerkungen: Erstellen/Ändern/Zuweisen/Anzeigen/Entfernen/Löschen	Y	Y	N
API-Zugriff*: Erstellen/Umbenennen/Deaktivieren/Widerrufen	Y	N	N
Anwendungen: Erstellen/Anzeigen/Ändern/Löschen	Y	Y	N
Asset-Seiten: Ändern	Y	Y	N
Asset-Seiten: Ansicht	Y	Y	Y
Audit: Anzeigen	Y	N	N
Cloud-Kosten	Y	N	N
Sicherheit	Y	N	N
Dashboards: Erstellen/Ändern/Löschen	Y	Y	N
Dashboards: Ansicht	Y	Y	Y
Datensammler: Hinzufügen/Ändern/Abfragen/Löschen	Y	N	N
Benachrichtigungen: Anzeigen	Y	Y	Y
Benachrichtigungen: Ändern	Y	N	N
Abfragen: Erstellen/Ändern/Löschen	Y	Y	N
Abfragen: Anzeigen/Ausführen	Y	Y	Y
Geräteauflösung	Y	Y	N
Berichte*: Anzeigen/Ausführen	Y	Y	Y
Berichte*: Erstellen/Ändern/Löschen/Planen	Y	Y	N
Abonnement: Anzeigen/Ändern	Y	N	N
Benutzerverwaltung: Einladen/Hinzufügen/Ändern/Deaktivieren	Y	N	N

*Erfordert Premium Edition

Erstellen von Konten durch Einladen von Benutzern

Das Erstellen eines neuen Benutzerkontos erfolgt über die NetApp Console. Ein Benutzer kann auf die per E-Mail gesendete Einladung antworten. Wenn der Benutzer jedoch kein Konto bei Console hat, muss er sich anmelden, damit er die Einladung annehmen kann.

Bevor Sie beginnen

- Der Benutzername ist die E-Mail-Adresse der Einladung.
- Machen Sie sich mit den Benutzerrollen vertraut, die Sie zuweisen werden.
- Passwörter werden vom Benutzer während des Anmeldevorgangs festgelegt.

Schritte

1. Melden Sie sich bei Data Infrastructure Insights an
2. Klicken Sie im Menü auf **Admin > Benutzerverwaltung**

   Der Bildschirm „Benutzerverwaltung“ wird angezeigt. Der Bildschirm enthält eine Liste aller Konten im System.

3. Klicken Sie auf **+ Benutzer**

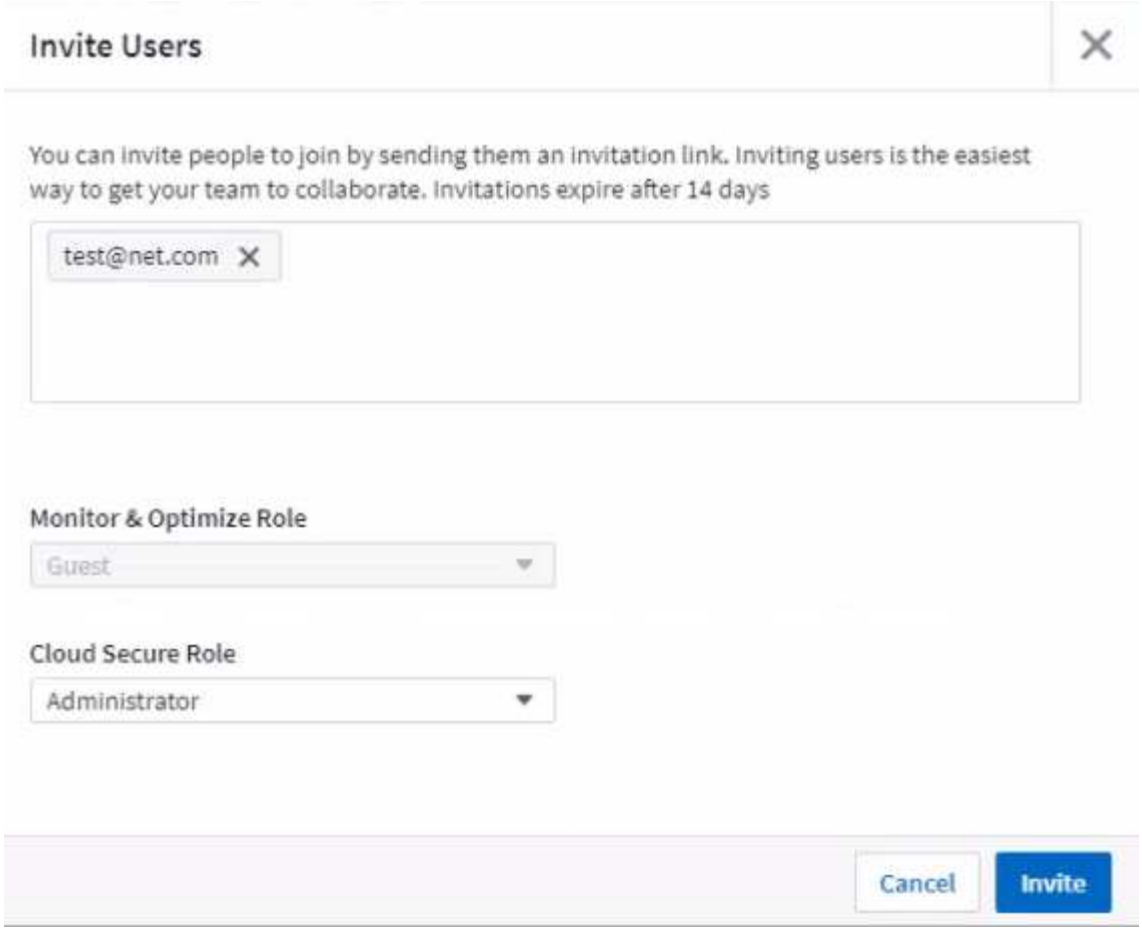
   Der Bildschirm **Benutzer einladen** wird angezeigt.

4. Geben Sie für Einladungen eine oder mehrere E-Mail-Adressen ein.

   Hinweis: Wenn Sie mehrere Adressen eingeben, werden sie alle mit derselben Rolle erstellt. Sie können mehreren Benutzern nur dieselbe Rolle zuweisen.

5. Wählen Sie die Rolle des Benutzers für jede Funktion von Data Infrastructure Insights aus.

   Die Funktionen und Rollen, aus denen Sie auswählen können, hängen davon ab, auf welche Funktionen Sie in Ihrer jeweiligen Administratorrolle Zugriff haben. Wenn Sie beispielsweise nur für die Berichterstellung über die Administratorrolle verfügen, können Sie Benutzern in der Berichterstellung jede beliebige Rolle zuweisen, jedoch keine Rollen für die Beobachtbarkeit oder Sicherheit.



6. Klicken Sie auf **Einladen**

   Die Einladung wird an den Benutzer gesendet. Benutzer haben 14 Tage Zeit, die Einladung anzunehmen. Sobald ein Benutzer die Einladung annimmt, wird er zum NetApp Cloud Portal weitergeleitet, wo er sich mit der E-Mail-Adresse in der Einladung anmeldet. Wenn sie bereits über ein Konto für diese E-Mail-Adresse verfügen, können sie sich einfach anmelden und haben dann Zugriff auf ihre Data Infrastructure Insights -Umgebung.

Ändern der Rolle eines vorhandenen Benutzers

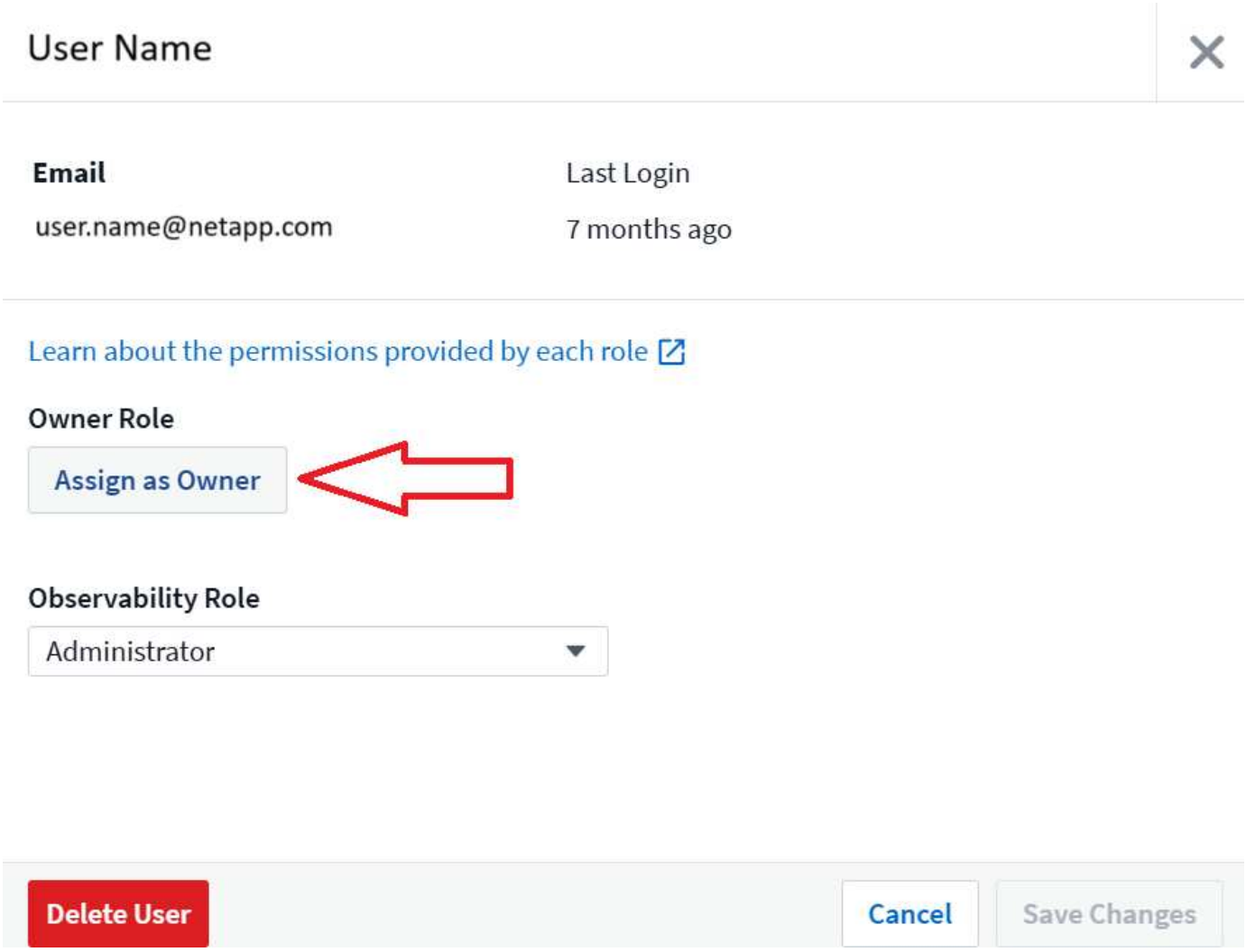
Um die Rolle eines vorhandenen Benutzers zu ändern, einschließlich der Hinzufügung als **sekundärer Kontoinhaber**, führen Sie die folgenden Schritte aus.

1. Klicken Sie auf **Admin > Benutzerverwaltung**. Auf dem Bildschirm wird eine Liste aller Konten im System angezeigt.
2. Klicken Sie auf den Benutzernamen des Kontos, das Sie ändern möchten.
3. Ändern Sie die Rolle des Benutzers in jedem Data Infrastructure Insights -Funktionssatz nach Bedarf.
4. Klicken Sie auf *Änderungen speichern*.

So weisen Sie einen sekundären Kontoinhaber zu

Sie müssen als Kontoinhaber für Observability angemeldet sein, um die Rolle des Kontoinhabers einem anderen Benutzer zuweisen zu können.

1. Klicken Sie auf **Admin > Benutzerverwaltung**.
2. Klicken Sie auf den Benutzernamen des Kontos, das Sie ändern möchten.
3. Klicken Sie im Benutzerdialog auf **Als Eigentümer zuweisen**.
4. Speichern Sie die Änderungen.



Sie können so viele Kontoinhaber haben, wie Sie möchten. Es empfiehlt sich jedoch, die Inhaberrolle auf ausgewählte Personen zu beschränken.

Löschen von Benutzern

Ein Benutzer mit der Administratorrolle kann einen Benutzer löschen (z. B. jemanden, der nicht mehr im Unternehmen ist), indem er auf den Namen des Benutzers klickt und im Dialogfeld auf *Benutzer löschen* klickt. Der Benutzer wird aus der Data Infrastructure Insights -Umgebung entfernt.

Beachten Sie, dass alle vom Benutzer erstellten Dashboards, Abfragen usw. auch nach der Entfernung des Benutzers in der Data Infrastructure Insights -Umgebung verfügbar bleiben.

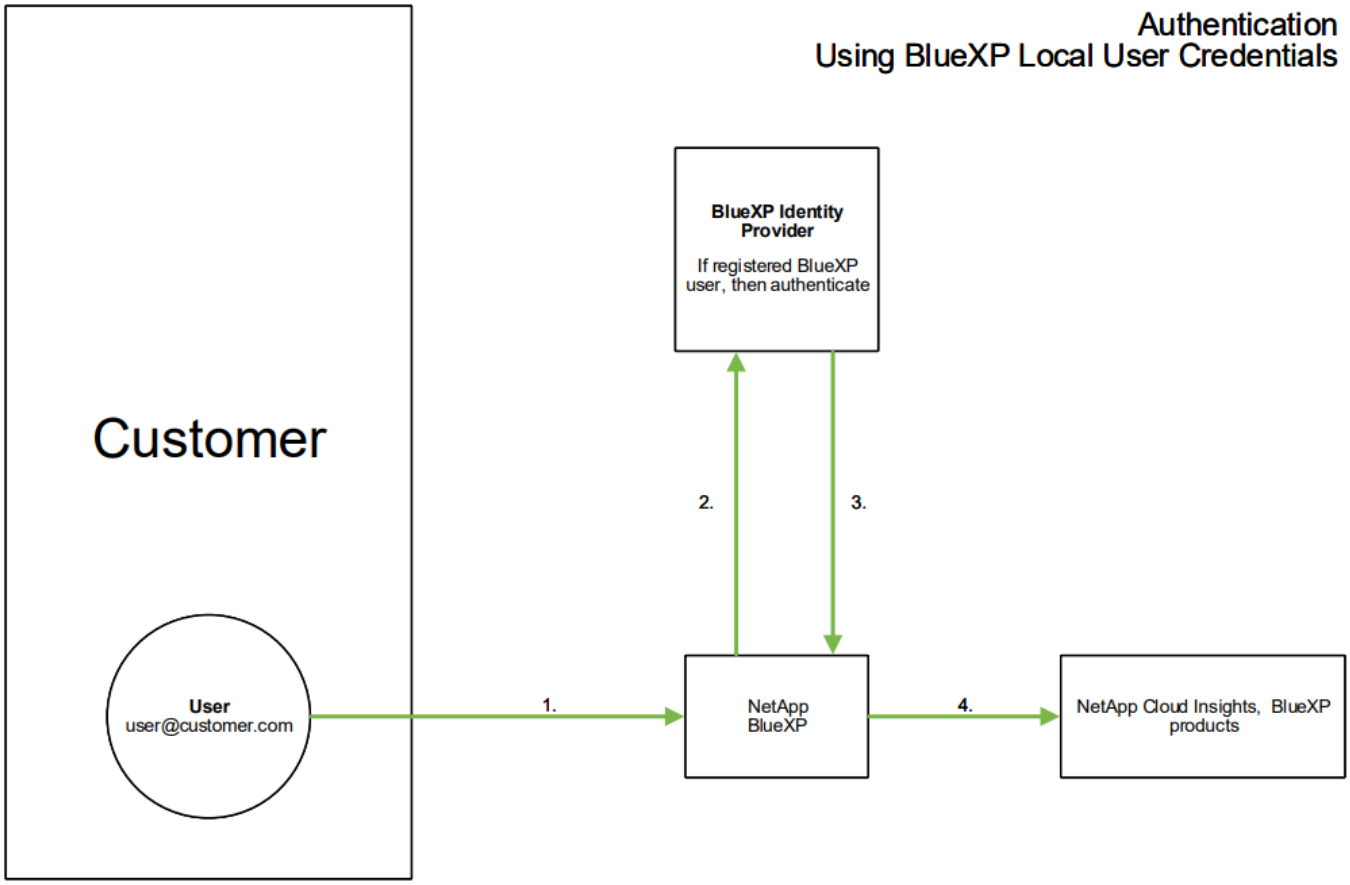
Single Sign-On (SSO) und Identitätsföderation

Was ist Identitätsföderation?

Mit Identity Federation:

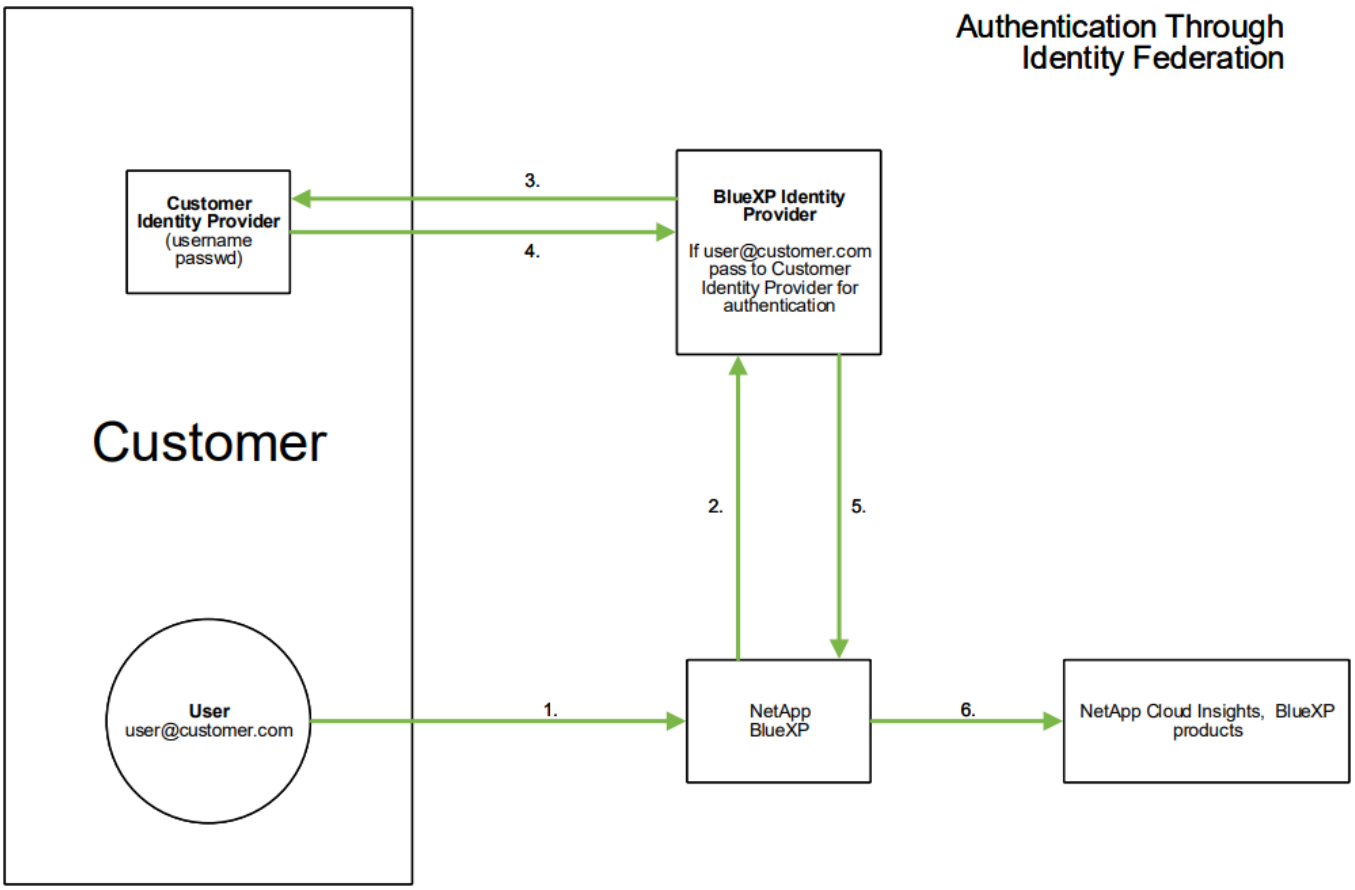
- Die Authentifizierung wird an das Identitätsmanagementsystem des Kunden delegiert, wobei die Anmeldeinformationen des Kunden aus Ihrem Unternehmensverzeichnis und Automatisierungsrichtlinien wie die Multi-Faktor-Authentifizierung (MFA) verwendet werden.
- Benutzer melden sich einmalig bei allen NetApp Console Services an (Single Sign On).

Benutzerkonten werden für alle Cloud-Dienste in der NetApp Console verwaltet. Standardmäßig erfolgt die Authentifizierung mithilfe eines lokalen Konsolenbenutzerprofils. Nachfolgend finden Sie eine vereinfachte Übersicht über diesen Prozess:



Einige Kunden möchten jedoch ihren eigenen Identitätsanbieter verwenden, um ihre Benutzer für Data Infrastructure Insights und ihre anderen NetApp Console Services zu authentifizieren. Mit Identity Federation werden NetApp Console mithilfe von Anmeldeinformationen aus Ihrem Unternehmensverzeichnis authentifiziert.

Das Folgende ist ein vereinfachtes Beispiel für diesen Prozess:



Wenn ein Benutzer im obigen Diagramm auf Data Infrastructure Insights zugreift, wird er zur Authentifizierung an das Identitätsverwaltungssystem des Kunden weitergeleitet. Sobald das Konto authentifiziert ist, wird der Benutzer zur URL des Data Infrastructure Insights Mandanten weitergeleitet.

Aktivieren der Identitätsföderation

Die Konsole verwendet Auth0, um die Identitätsföderation zu implementieren und in Dienste wie Active Directory Federation Services (ADFS) und Microsoft Azure Active Directory (AD) zu integrieren. Informationen zum Konfigurieren der Identitätsföderation finden Sie im"Anweisungen zur Föderation" .

Sie müssen Identity Federation konfigurieren, bevor Sie SSO mit Data Infrastructure Insights verwenden können.

Es ist wichtig zu verstehen, dass die Änderung der Identitätsföderation nicht nur für Data Infrastructure Insights, sondern für alle NetApp Console Services gilt. Der Kunde sollte diese Änderung mit dem NetApp Team jedes seiner Produkte besprechen, um sicherzustellen, dass die von ihm verwendete Konfiguration mit Identity Federation funktioniert oder ob an Konten Anpassungen vorgenommen werden müssen. Der Kunde muss auch sein internes SSO-Team in die Umstellung auf die Identitätsföderation einbeziehen.

Es ist auch wichtig zu wissen, dass nach der Aktivierung der Identitätsföderation alle Änderungen am Identitätsanbieter des Unternehmens (z. B. die Umstellung von SAML auf Microsoft AD) wahrscheinlich eine Fehlerbehebung/Änderungen/Aufmerksamkeit erfordern, um die Profile der Benutzer zu aktualisieren.

Für dieses oder andere Föderationsprobleme können Sie ein Support-Ticket eröffnen unter https://mysupport.netapp.com/site/help .

Automatische Benutzerbereitstellung per Single Sign-On (SSO)

Zusätzlich zum Einladen von Benutzern können Administratoren allen Benutzern in ihrer Unternehmensdomäne den Zugriff auf Data Infrastructure Insights per **Single Sign-On (SSO) User Auto-Provisioning** ermöglichen, ohne sie einzeln einladen zu müssen. Wenn SSO aktiviert ist, kann sich jeder Benutzer mit derselben Domänen-E-Mail-Adresse mit seinen Unternehmensanmeldeinformationen bei Data Infrastructure Insights anmelden.

> *SSO User Auto-Provisioning* ist in der Data Infrastructure Insights Premium Edition verfügbar und muss konfiguriert werden, bevor es für Data Infrastructure Insights aktiviert werden kann. Die Konfiguration der automatischen SSO-Benutzerbereitstellung umfasst"Identitätsföderation" über die NetApp Console , wie im obigen Abschnitt beschrieben. Durch die Föderation können Single-Sign-On-Benutzer mithilfe von Anmeldeinformationen aus Ihrem Unternehmensverzeichnis auf Ihre NetApp Console Konsolenkonten zugreifen. Dabei kommen offene Standards wie Security Assertion Markup Language 2.0 (SAML) und OpenID Connect (OIDC) zum Einsatz.

Um die automatische SSO-Benutzerbereitstellung auf der Seite **Admin > Benutzerverwaltung** zu konfigurieren, müssen Sie zunächst die Identitätsföderation eingerichtet haben. Wählen Sie im Banner den Link **Föderation einrichten**, um mit der Konsolenföderation fortzufahren. Sobald dies konfiguriert ist, können Data Infrastructure Insights Administratoren die SSO-Benutzeranmeldung aktivieren. Wenn ein Administrator die automatische SSO-Benutzerbereitstellung aktiviert, wählt er eine Standardrolle für alle SSO-Benutzer (z. B. Gast oder Benutzer). Benutzer, die sich über SSO anmelden, haben diese Standardrolle.

Gelegentlich möchte ein Administrator einen einzelnen Benutzer aus der SSO-Standardrolle herausstufen (beispielsweise um ihn zum Administrator zu machen). Dies können Sie auf der Seite **Admin > Benutzerverwaltung** erreichen, indem Sie auf das Menü auf der rechten Seite des Benutzers klicken und *Rolle zuweisen* auswählen. Benutzer, denen auf diese Weise eine explizite Rolle zugewiesen wird, haben weiterhin Zugriff auf Data Infrastructure Insights, auch wenn die automatische SSO-Benutzerbereitstellung anschließend deaktiviert wird.

Wenn der Benutzer die erhöhte Rolle nicht mehr benötigt, können Sie auf das Menü klicken, um *Benutzer zu entfernen*. Der Benutzer wird aus der Liste entfernt. Wenn die automatische SSO-Benutzerbereitstellung aktiviert ist, kann sich der Benutzer weiterhin mit der Standardrolle über SSO bei Data Infrastructure Insights anmelden.

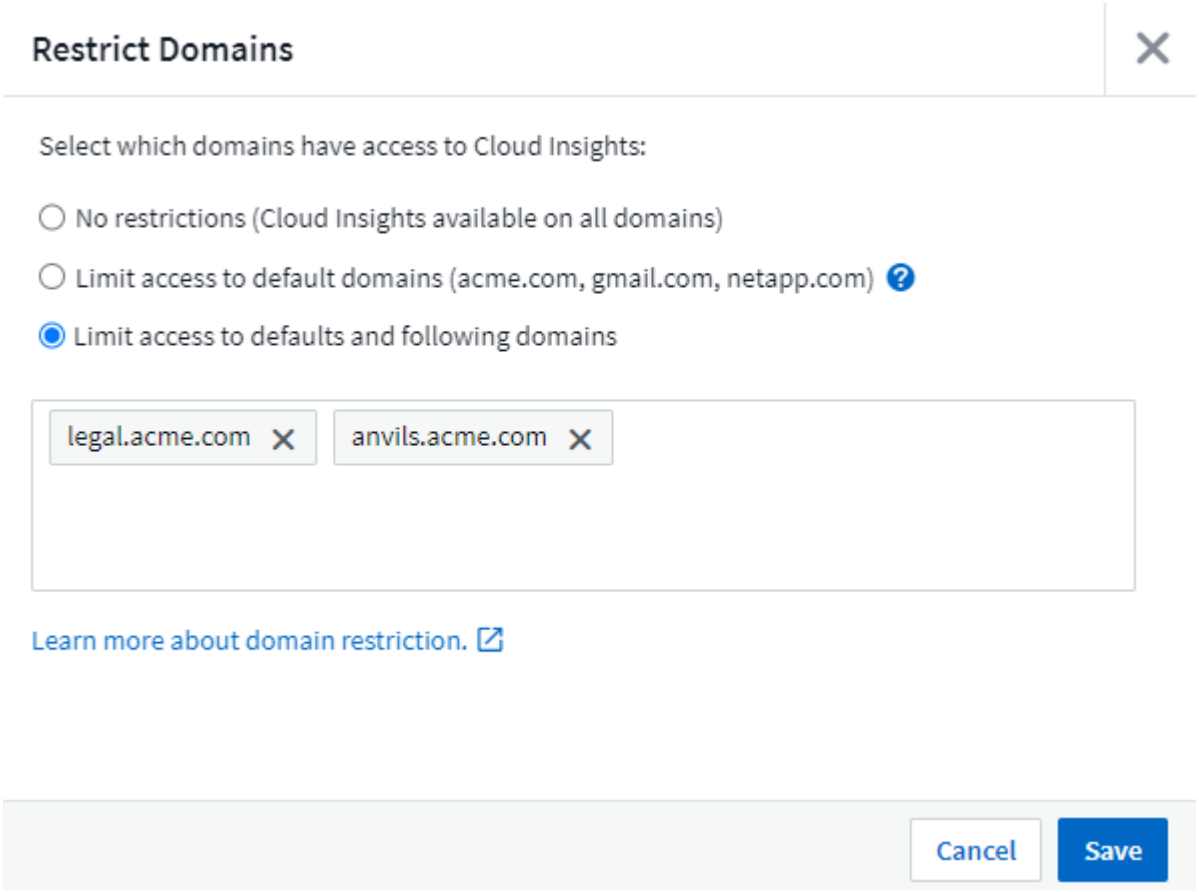
Sie können SSO-Benutzer ausblenden, indem Sie das Kontrollkästchen **SSO-Benutzer anzeigen** deaktivieren.

Aktivieren Sie die automatische SSO-Benutzerbereitstellung jedoch nicht, wenn einer der folgenden Punkte zutrifft:

- Ihre Organisation verfügt über mehr als einen Data Infrastructure Insights Mandanten
- Ihre Organisation möchte nicht, dass jeder Benutzer in der Verbunddomäne einen gewissen Grad an automatischem Zugriff auf den Data Infrastructure Insights Mandanten hat. *Zum jetzigen Zeitpunkt haben wir nicht die Möglichkeit, mit dieser Option Gruppen zur Steuerung des Rollenzugriffs zu verwenden*.

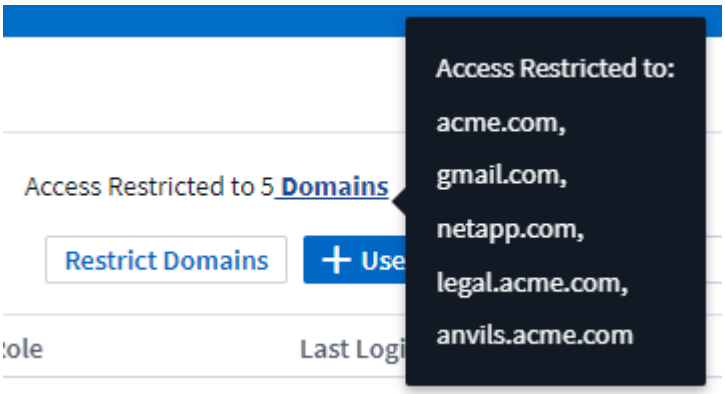
Zugriffsbeschränkung nach Domäne

Data Infrastructure Insights kann den Benutzerzugriff auf die von Ihnen angegebenen Domänen beschränken. Wählen Sie auf der Seite **Admin > Benutzerverwaltung** die Option „Domänen einschränken“ aus.



Ihnen stehen folgende Auswahlmöglichkeiten zur Verfügung:

- Keine Einschränkungen: Data Infrastructure Insights bleibt für Benutzer unabhängig von ihrer Domäne zugänglich.
- Beschränken Sie den Zugriff auf Standarddomänen: Standarddomänen sind diejenigen, die von den Kontobesitzern Ihrer Data Infrastructure Insights -Umgebung verwendet werden. Diese Domänen sind immer zugänglich.
- Beschränken Sie den Zugriff auf die Standardeinstellungen und die von Ihnen angegebenen Domänen. Listen Sie alle Domänen auf, die zusätzlich zu den Standarddomänen Zugriff auf Ihre Data Infrastructure Insights -Umgebung haben sollen.



Data Infrastructure Insights Datensammlerliste

Data Infrastructure Insights unterstützt eine Vielzahl von Datensammlern von vielen Anbietern und Diensten.

Datensammler werden nach diesen Typen kategorisiert:

- Infrastruktur: Von Anbietern erworbene Geräte wie Speicher-Arrays, Switches, Hypervisoren oder Backup-Geräte.
- Dienst: Von Diensten wie Kubernetes oder Docker erworben. Wird auch *Integration* genannt.

Alphabetische Liste der von Data Infrastructure Insights unterstützten Datensammler:

Datensammler	Typ
"Amazon EC2 und EBS"	Infrastruktur
"AWS S3 als Speicher"	Infrastruktur
"Amazon FSx for NetApp ONTAP"	Infrastruktur
"Apache"	Service
"Azure NetApp Files"	Infrastruktur
"Azure-VMs und VHD"	Infrastruktur
"Brocade Network Advisor (BNA)"	Infrastruktur
"Brocade Fibre Channel Switches"	Infrastruktur
"Brocade FOS REST"	Infrastruktur
"Cisco MDS Fabric Switches"	Infrastruktur
"Konsul"	Service
"Couchbase"	Service
"CouchDB"	Service
"Cohesity SmartFiles"	Infrastruktur
"Dell EMC Datendomäne"	Infrastruktur
"Dell EMC ECS"	Infrastruktur
"Dell EMC PowerScale (vormals Isilon)"	Infrastruktur
"Dell EMC Isilon / PowerScale REST"	Infrastruktur
"Dell EMC PowerStore"	Infrastruktur
"Dell EMC Wiederherstellungspunkt"	Infrastruktur
"Dell EMC ScaleIO/PowerFlex"	Infrastruktur
"Dell EMC Unity"	Infrastruktur
"Dell EMC Unisphere REST"	Infrastruktur
"Dell EMC VMAX/PowerMax-Gerätefamilie"	Infrastruktur

Datensammler	Typ
"Dell EMC VNX-Blockspeicher"	Infrastruktur
"Dell EMC VNX-Datei"	Infrastruktur
"Dell EMC VNX Unified"	Infrastruktur
"Dell EMC VPLEX"	Infrastruktur
"Dell EMC XtremIO"	Infrastruktur
"Dell XC-Serie"	Infrastruktur
"Docker"	Service
"Elasticsearch"	Service
"Flink"	Service
"Fujitsu ETERNUS DX"	Infrastruktur
"Google Compute und Storage"	Infrastruktur
"Google Cloud NetApp Volumes"	Infrastruktur
"Hadoop"	Service
"HAProxy"	Service
"Hitachi Content Platform (HCP)"	Infrastruktur
"Hitachi Vantara Command Suite"	Infrastruktur
"Hitachi Vantara NAS-Plattform"	Infrastruktur
"Hitachi Ops Center"	Infrastruktur
"HP Enterprise Alletra 6000 (vormals Nimble) Speicher"	Infrastruktur
"HP Enterprise Alletra 9000 / Primera (vormals 3PAR) Speicher"	Infrastruktur
"HP Enterprise Command View"	Infrastruktur
"Huawei OceanStor- und Dorado-Geräte"	Infrastruktur
"IBM Cleversafe"	Infrastruktur
"IBM CS-Serie"	Infrastruktur
"IBM PowerVM"	Infrastruktur
"IBM SAN Volume Controller (SVC)"	Infrastruktur
"IBM System Storage DS8000-Serie"	Infrastruktur
"IBM XIV- und A9000-Speicher"	Infrastruktur
"Infinidat InfiniBox"	Infrastruktur
"Java"	Service
"Kafka"	Service
"Kondensator"	Service

Datensammler	Typ
"Kibana"	Service
"Kubernetes"	Service
"Lenovo HX-Serie"	Infrastruktur
"Memcached"	Service
"Microsoft Azure NetApp Files"	Infrastruktur
"Microsoft Hyper-V"	Infrastruktur
"MongoDB"	Service
"MySQL"	Service
"NetApp Cloud Volumes ONTAP"	Infrastruktur
"NetApp Cloud Volumes Services für AWS"	Infrastruktur
"NetApp Cloud Connection für ONTAP 9.9+"	Infrastruktur
"NetApp Data ONTAP 7-Mode"	Infrastruktur
"NetApp E-Serie"	Infrastruktur
"NetApp E-Serie REST"	Infrastruktur
"Amazon FSx for NetApp ONTAP"	Infrastruktur
"NetApp HCI Virtual Center"	Infrastruktur
"NetApp ONTAP Datenmanagement-Software"	Infrastruktur
"NetApp ONTAP REST-Kollektor"	Infrastruktur
"NetApp ONTAP ASA r2 (All-SAN Array)-Kollektor"	Infrastruktur
"NetApp ONTAP Select"	Infrastruktur
"NetApp SolidFire All-Flash-Array"	Infrastruktur
"NetApp StorageGRID"	Infrastruktur
"Netstat"	Service
"Nginx"	Service
"Node"	Service
"Nutanix NX-Serie"	Infrastruktur
"OpenZFS"	Service
"Oracle ZFS-Speichergerät"	Infrastruktur
"PostgreSQL"	Service
"Puppenagent"	Service
"Pure Storage FlashArray"	Infrastruktur
"Red Hat Virtualisierung"	Infrastruktur
"Redis"	Service

Datensammler	Typ
"RethinkDB"	Service
"RHEL und CentOS"	Service
"Rubrik CDM-Speicher"	Infrastruktur
"Ubuntu und Debian"	Service
"VAST DataStore"	Infrastruktur
"VMware vSphere"	Infrastruktur
"Windows"	Service
"ZooKeeper"	Service

Abonnieren von Data Infrastructure Insights

Der Einstieg in Data Infrastructure Insights ist in drei einfachen Schritten möglich:

1. Registrieren Sie sich für ein Konto auf"* NetApp Console*" um Zugriff auf alle Cloud-Angebote von NetApp zu erhalten.
2. Registrieren Sie sich für eine kostenlose Testversion von Data Infrastructure Insights, um die verfügbaren Funktionen kennenzulernen. So registrieren Sie sich für eine kostenlose Testversion:
   - Gehe zu https://netapp.com
   - Wählen Sie oben auf der Seite **So kaufen Sie** aus.
   - Wählen Sie **Testversion anfordern**. Wenn Sie noch nicht bei Console registriert sind, geben Sie Ihre Daten ein und melden Sie sich an. Andernfalls melden Sie sich an.
   - Vereinbaren Sie einen Termin oder warten Sie, bis sich ein Vertreter bezüglich Ihres Testzeitraums bei Ihnen meldet.
3. **Abonnieren** Sie Data Infrastructure Insights für einen kontinuierlichen, unterbrechungsfreien Zugriff auf Ihre Daten über eine Vielzahl flexibler Abonnementoptionen:
   - "NetApp Vertrieb direkt"
   - AWS Marketplace:
     - "Abonnement mit fester Laufzeit"
     - "Pay-as-you-go-Abonnement"
     - "Feste Basis + Pay-as-you-go-Abonnement für Überschreitungen"
   - "Azure Marketplace"(alle Abonnementoptionen)

Während des Registrierungsprozesses können Sie die globale Region auswählen, in der Ihre Data Infrastructure Insights -Umgebung gehostet werden soll. Weitere Informationen finden Sie unter Data Infrastructure Insights"Informationen und Region" .

Ausführliche Informationen zu den Funktionen und Preisoptionen von Data Infrastructure Insights finden Sie im"Data Infrastructure Insights Editionen" Seite.

Wenn Sie bei der Verwendung von Data Infrastructure Insights ein Vorhängeschlosssymbol sehen , bedeutet dies, dass die Funktion in Ihrem aktuellen Abonnement nicht oder nur eingeschränkt verfügbar ist. Abonnieren Sie diese Funktion, um vollen Zugriff zu erhalten. Einige Funktionen sind verfügbar alsModulbewertung vor dem Abonnieren.

Testversion

Wenn Sie sich für Data Infrastructure Insights anmelden und Ihre Umgebung aktiv ist, erhalten Sie eine kostenlose 30-tägige Testversion von Data Infrastructure Insights. Während dieser Testphase können Sie die Funktionen von Data Infrastructure Insights in Ihrer eigenen Umgebung erkunden.

Sie können Data Infrastructure Insights jederzeit während Ihres Testzeitraums abonnieren. Das Abonnieren von Data Infrastructure Insights gewährleistet einen unterbrechungsfreien Zugriff auf Ihre Daten sowie erweiterte"**Produktsupport**" Optionen.

Data Infrastructure Insights zeigt ein Banner an, wenn Ihre kostenlose Testversion bald abläuft. In diesem Banner befindet sich ein Link „Abonnement anzeigen“, der die Seite **Admin → Abonnement** öffnet. Benutzer

ohne Administratorrechte sehen das Banner, können jedoch nicht zur Abonnementseite gelangen.

Wenn Sie zusätzliche Zeit zum Auswerten von Data Infrastructure Insights benötigen und Ihre Testversion in 4 Tagen oder weniger abläuft, können Sie Ihre Testversion um weitere 30 Tage verlängern. Sie können die Testversion nur einmal verlängern. Eine Verlängerung ist nicht möglich, wenn Ihre Testversion abgelaufen ist.

Testversion über AWS Marketplace

Sie können sich auch über den AWS Marketplace für eine kostenlose Testversion anmelden. Mit der kostenlosen Testversion von AWS Marketplace erhalten Sie 33 Tage lang Zugriff auf Data Infrastructure Insights .

Die kostenlose Testversion von AWS Marketplace kann nicht verlängert werden.

Was ist, wenn meine Testversion abgelaufen ist?

Wenn Ihre kostenlose Testversion abgelaufen ist und Sie Data Infrastructure Insights noch nicht abonniert haben, steht Ihnen bis zum Abonnement nur eingeschränkte Funktionalität zur Verfügung. Die Datenaufnahme kann eingestellt werden und nach einigen Wochen werden Ihre Daten gemäß unserer Datenaufbewahrungsrichtlinie gelöscht.

Was ist, wenn mein Abonnement abgelaufen ist?

Wenn Sie ein Abonnement für Data Infrastructure Insights haben, dieses Abonnement jedoch abgelaufen ist, haben Sie eine Nachfrist von fünf Tagen, um Ihr Abonnement zu verlängern. Während dieser Übergangsfrist bleiben alle Data Infrastructure Insights -Funktionen aktiv.

Nach Ablauf der Nachfrist wird die Data Infrastructure Insights -Funktionalität bis zur Verlängerung ausgesetzt. Informationen zur Verlängerung finden Sie auf der Seite **Admin > Abonnement** oder wenden Sie sich an den NetApp Vertrieb.

Ihre Data Infrastructure Insights Daten bleiben nach Ablauf der Nachfrist 30 Tage lang intakt. Wenn Sie Ihr Abonnement innerhalb dieser Zeit verlängern, stehen Ihnen alle Ihre Daten bis zum Ablauf der Nachfrist zur Verfügung.

Modulbewertung

Sie können auch die Vorteile der **Modulbewertungen** nutzen. Wenn Sie beispielsweise Infrastructure Observability bereits abonniert haben, aber Kubernetes zu Ihrer Umgebung hinzufügen, beginnen Sie automatisch mit der 30-tägigen Evaluierung von Kubernetes Observability, beginnend mit der Installation des NetApp Kubernetes Monitoring Operator. Die Nutzung Ihrer verwalteten Kubernetes Observability-Einheit wird Ihnen erst am Ende des Evaluierungszeitraums in Rechnung gestellt.

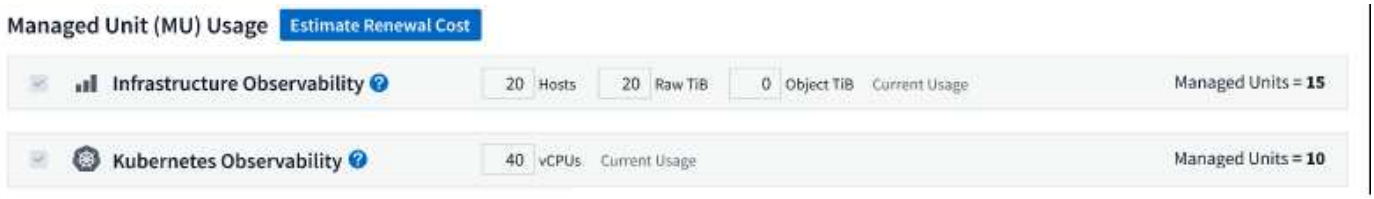
Bedenken Sie, dass Ihnen nach der Evaluierung die Nutzung neuer verwalteter Einheiten (MU) in Rechnung gestellt wird. Planen Sie daher entsprechend. Wenn Ihre Modulbewertung endet, werden Sie benachrichtigt, wenn Sie weitere MUs hinzufügen müssen, um eine Dienstunterbrechung zu vermeiden.

Sie können die Nutzung Ihrer verwalteten Einheit auf der Seite **Admin > Abonnement** auf der Registerkarte **Nutzung** überwachen.

Eine *Modulbewertung* ist keine *Testversion*. Wir verwenden den Begriff „Testversion“, wenn wir Kunden eine kostenlose Testphase für die Nutzung des Data Infrastructure Insights -Dienstes anbieten, um die Eignung zu bestätigen und den Kauf zu ermöglichen. Anders verhält es sich bei einer Modulevaluierung. Dabei ermöglichen wir einem zahlenden Kunden, ein Modul von Data Infrastructure Insights auszuprobieren, das er in den letzten Monaten seines kostenpflichtigen Abonnements nicht verwendet hat. Bei aktiver Evaluierung entfallen die Kosten nur für das neu konfigurierte Modul. Die Arbeitsumgebung des Kunden unterliegt noch einem Abonnement und wurde nicht auf die kostenlose Testversion zurückgesetzt. Das Abonnement hat sich nicht geändert.

Schätzer

Während einer Modulevaluierung wird Ihnen für die für das Modul verbrauchten Ressourcen keine MU-Nutzung in Rechnung gestellt, Sie können jedoch den **Kostenschätzer** (auf der Registerkarte *Zusammenfassung*) öffnen, um zu sehen, wie die MUs nach der Evaluation berechnet werden, und „Was wäre wenn“-Szenarien mit der Anzahl der MUs durchspielen, die Sie möglicherweise in Zukunft benötigen. Setzen Sie die Zahlen zurück, indem Sie den Schätzer beenden.



Aktivieren Sie das Kontrollkästchen neben einem Modul, um die MUs des gesamten Moduls zu den geschätzten Kosten hinzuzufügen oder daraus zu entfernen.

Mit dem Schätzer können Sie auch sehen, wie sich die Zahlen für ein Add-On (bei dem Sie Ihre aktuelle Abonnementlaufzeit beibehalten und die Anzahl der lizenzierten verwalteten Einheiten erhöhen) oder eine Verlängerungsoption für ein Verlängerungsabonnement, das Sie erwerben würden, wenn Ihre aktuelle Abonnementlaufzeit endet, entwickeln.

Beachten Sie, dass Kunden pro Abonnement nur einmal Anspruch auf eine Modulbewertung haben.

Abonnementoptionen

Um sich anzumelden, gehen Sie zu **Admin** → **Abonnement**. Zusätzlich zu den Schaltflächen „Abonnieren“ können Sie Ihre installierten Datensammler sehen und Ihren geschätzten Verbrauch berechnen. Für eine typische Umgebung können Sie auf die Self-Service-Schaltfläche „AWS Marketplace“ klicken. Wenn Ihre Umgebung 1.000 oder mehr verwaltete Einheiten umfasst oder voraussichtlich umfassen wird, haben Sie Anspruch auf Volumenpreise.

Beobachtbarkeitsmessung

Die Beobachtbarkeit von Data Infrastructure Insights wird auf eine von zwei Arten gemessen:

- Kapazitätsmessung
- Verwaltete Einheitenmessung (Legacy)

Ihr Abonnement wird mit einer dieser Methoden gemessen, je nachdem, ob Sie ein bestehendes Abonnement haben oder ein neues Abonnement starten.

Kapazitätsmessung

Data Infrastructure Insights Observability misst die Nutzung entsprechend der Speicherebene Ihres Mandanten. Möglicherweise verfügen Sie über Speicher, die in eine oder mehrere dieser Kategorien fallen:

- Primärroh
- Objekt Rohdaten
- Cloud-Nutzung

Für jede Stufe wird ein anderer Satz berechnet, wobei die Gesamtsumme zusammengerechnet wird, um Ihnen einen gewichteten Anspruch zu geben. Die Formel zur Berechnung der gewichteten Nutzung lautet wie folgt:

```
 Weighted Capacity = Raw TiB + (0.1 x Object Tier Raw TiB) + (0.25 x Cloud
Tier Provisioned TiB)
Um dies zu ermöglichen, berechnet DII eine einzelne *gewichtete
Berechtigungszahl* basierend auf den _abonnierten_ Mengen. Anschließend
berechnet es dieselbe Zahl basierend auf dem _entdeckten_ Speicher und
erklärt nur dann einen Verstoß, wenn die entdeckte Kapazität größer ist
als die gewichtete Berechtigung.  Dadurch haben Sie die Flexibilität,
Mengen zu überwachen, die von den abonnierten Mengen für jede Stufe
abweichen. DII ermöglicht dies, solange der gesamte ermittelte Speicher
innerhalb der abonnierten gewichteten Berechtigung liegt.
```

Verwaltete Einheitenmessung (Legacy)

Data Infrastructure Insights: Nutzung des Infrastruktur-Observability- und Kubernetes-Observability-Messgeräts pro **verwalteter Einheit**. Die Nutzung Ihrer verwalteten Einheiten wird anhand der Anzahl der **Hosts oder virtuellen Maschinen** und der Menge der **unformatierten Kapazität** berechnet, die in Ihrer Infrastrukturumgebung verwaltet wird.

- 1 verwaltete Einheit = 2 Hosts (jede virtuelle oder physische Maschine)

- 1 verwaltete Einheit = 4 TiB unformatierte Kapazität physischer oder virtueller Festplatten
- 1 verwaltete Einheit = 40 TiB unformatierte Kapazität ausgewählten sekundären Speichers: AWS S3, Cohesity SmartFiles, Dell EMC Data Domain, Dell EMC ECS, Hitachi Content Platform, IBM Cleversafe, NetApp StorageGRID, Rubrik.
- 1 verwaltete Einheit = 4 vCPUs von Kubernetes.
  - 1 verwaltete Einheit K8s-Anpassung = 2 Knoten oder Hosts, die ebenfalls von der Infrastruktur überwacht werden.

Workload-Sicherheitsmessung

Die Workload-Sicherheit wird vom Cluster mit demselben Ansatz wie die Observability-Messung gemessen.

Sie können Ihre Workload Security-Nutzung auf der Seite **Admin > Abonnement** auf der Registerkarte **Workload Security** anzeigen.

Bei vorhandenen Workload Security-Abonnements wird die MU-Nutzung angepasst, sodass die Knotennutzung keine verwalteten Einheiten verbraucht. Data Infrastructure Insights misst die Nutzung, um die Einhaltung der lizenzierten Nutzung sicherzustellen.

Wie abonniere ich?

Wenn Ihre Managed Unit-Anzahl weniger als 1.000 beträgt, können Sie über NetApp Sales abonnieren, oderSelbstabonnement über AWS Marketplace.

Abonnieren Sie direkt über den NetApp Vertrieb

Wenn die erwartete Anzahl verwalteter Einheiten 1.000 oder mehr beträgt, klicken Sie auf das**"Vertrieb kontaktieren"** Klicken Sie auf die Schaltfläche, um sich über das NetApp -Vertriebsteam anzumelden.

Sie müssen Ihrem NetApp Vertriebsmitarbeiter Ihre Data Infrastructure Insights **Seriennummer** mitteilen, damit Ihr kostenpflichtiges Abonnement auf Ihre Data Infrastructure Insights Umgebung angewendet werden kann. Die Seriennummer identifiziert Ihre Data Infrastructure Insights -Testumgebung eindeutig und ist auf der Seite **Admin > Abonnement** zu finden.

Selbstabonnement über AWS Marketplace

Sie müssen Kontoinhaber oder Administrator sein, um ein AWS Marketplace-Abonnement auf Ihr bestehendes Data Infrastructure Insights -Testkonto anzuwenden. Darüber hinaus müssen Sie über ein Amazon Web Services (AWS)-Konto verfügen.

Klicken Sie auf den Amazon Marketplace-Link, um den AWS "Data Infrastructure Insights" Abonnementseite, auf der Sie Ihr Abonnement abschließen können. Beachten Sie, dass die von Ihnen in den Rechner eingegebenen Werte nicht auf der AWS-Abonnementseite angezeigt werden. Sie müssen auf dieser Seite die Gesamtzahl der verwalteten Einheiten eingeben.

Nachdem Sie die Gesamtzahl der verwalteten Einheiten eingegeben und eine Abonnementlaufzeit von 12 oder 36 Monaten gewählt haben, klicken Sie auf **Konto einrichten**, um den Abonnementvorgang abzuschließen.

Sobald der AWS-Abonnementvorgang abgeschlossen ist, werden Sie zu Ihrer Data Infrastructure Insights

-Umgebung zurückgeleitet. Oder wenn die Umgebung nicht mehr aktiv ist (z. B. weil Sie sich abgemeldet haben), werden Sie zur Anmeldeseite der NetAPp-Konsole weitergeleitet. Wenn Sie sich erneut bei Data Infrastructure Insights anmelden, ist Ihr Abonnement aktiv.

Nachdem Sie auf der AWS Marketplace-Seite auf **Konto einrichten** geklickt haben, müssen Sie den AWS-Abonnementvorgang innerhalb einer Stunde abschließen. Wenn Sie es nicht innerhalb einer Stunde abschließen, müssen Sie erneut auf **Konto einrichten** klicken, um den Vorgang abzuschließen.

Wenn ein Problem auftritt und der Abonnementvorgang nicht ordnungsgemäß abgeschlossen werden kann, wird beim Anmelden bei Ihrer Umgebung weiterhin das Banner „Testversion“ angezeigt. In diesem Fall können Sie zu **Admin > Abonnement** gehen und den Abonnementvorgang wiederholen.

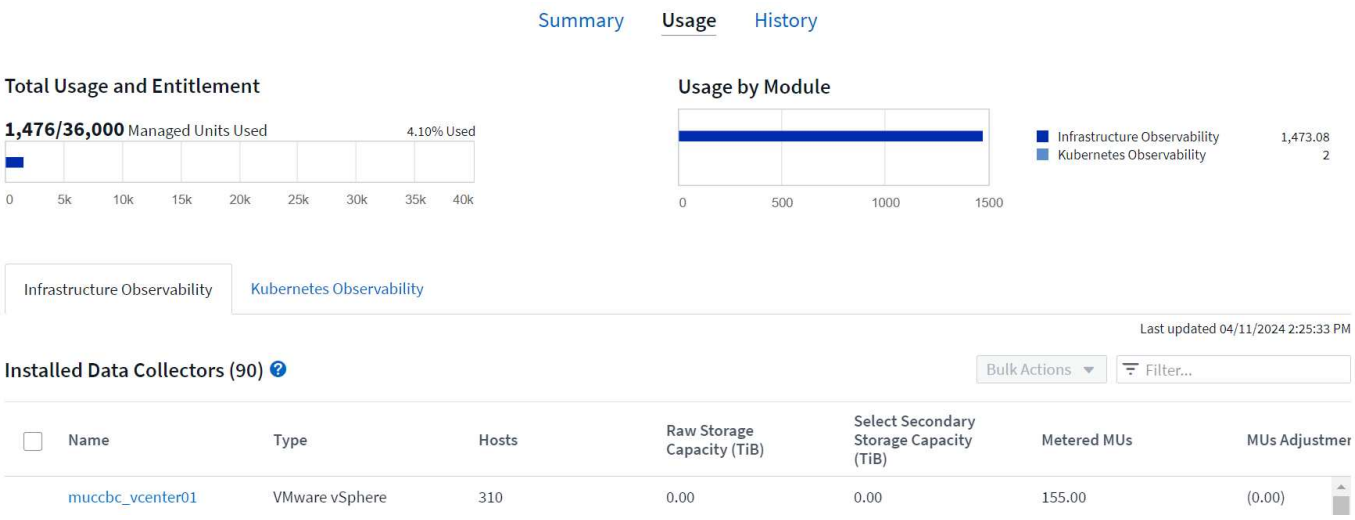
Zeigen Sie Ihren Abonnementstatus an

Sobald Ihr Abonnement aktiv ist, können Sie Ihren Abonnementstatus und die Nutzung der verwalteten Einheit auf der Seite **Admin > Abonnement** anzeigen.

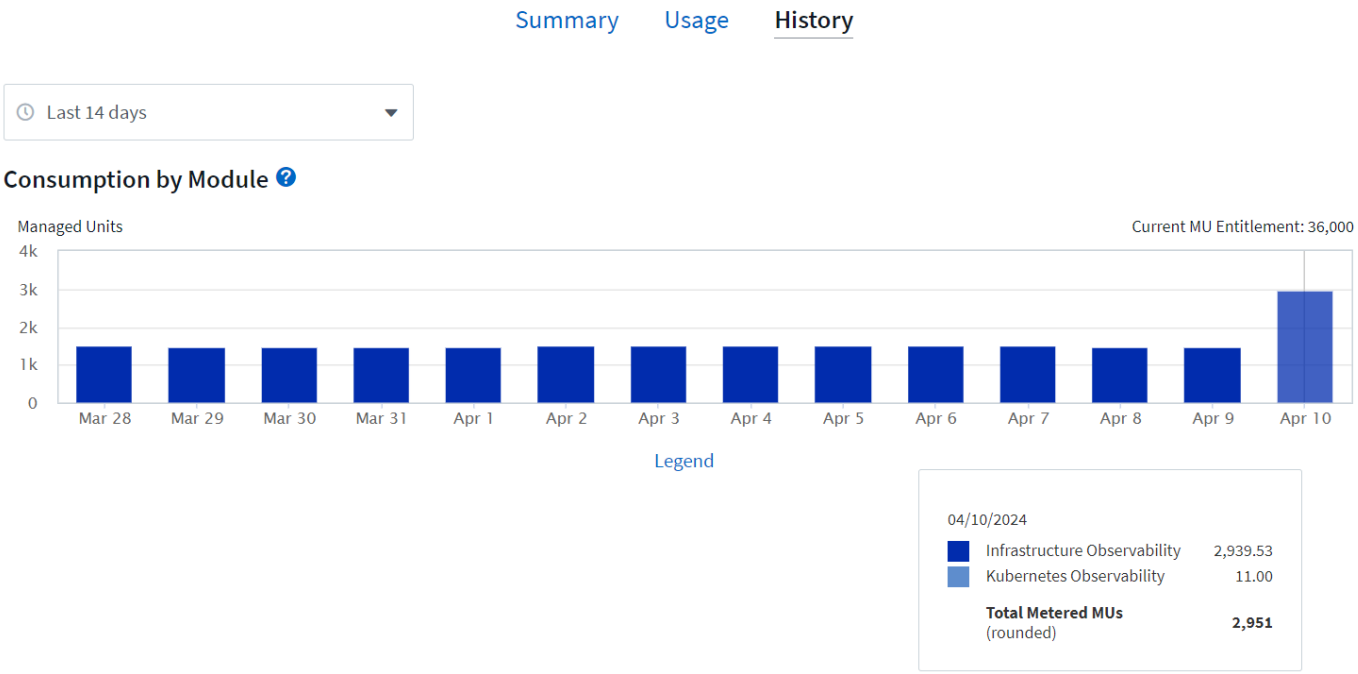
Auf der Registerkarte „Abonnement **Zusammenfassung**“ werden beispielsweise die folgenden Informationen angezeigt:

- Aktuelle Ausgabe
- Abonnement-Seriennummer
- Aktueller MU-Anspruch

Die Registerkarte **Nutzung** zeigt Ihnen Ihre aktuelle MU-Nutzung und wie sich diese Nutzung nach Datensammler aufschlüsselt.



Die Registerkarte **Verlauf** gibt Ihnen Einblick in Ihre MU-Nutzung der letzten 7 bis 90 Tage. Wenn Sie mit der Maus über eine Spalte im Diagramm fahren, erhalten Sie eine Aufschlüsselung nach Modul (z. B. Observability, Kubernetes).



Zeigen Sie Ihr Nutzungsmanagement an

Die Registerkarte „Nutzungsverwaltung“ zeigt eine Übersicht über die Nutzung verwalteter Einheiten sowie Registerkarten, die den Verbrauch verwalteter Einheiten nach Collector oder Kubernetes-Cluster aufschlüsseln.

Die unformatierte Anzahl der verwalteten Einheiten mit Kapazität spiegelt die Summe der gesamten Rohkapazität in der Umgebung wider und wird auf die nächste verwaltete Einheit aufgerundet.

Die Summe der verwalteten Einheiten kann geringfügig von der Anzahl der Datensammler im Abschnitt „Zusammenfassung“ abweichen. Dies liegt daran, dass die Anzahl der verwalteten Einheiten auf die nächste verwaltete Einheit aufgerundet wird. Die Summe dieser Zahlen in der Liste der Datensammler kann etwas höher sein als die Gesamtzahl der verwalteten Einheiten im Statusabschnitt. Der Abschnitt „Zusammenfassung“ gibt die tatsächliche Anzahl Ihrer verwalteten Einheiten für Ihr Abonnement wieder.

Falls Ihre Nutzung sich Ihrem Abonnementbetrag nähert oder diesen überschreitet, können Sie die Nutzung reduzieren, indem Sie Datensammler löschen oder die Überwachung von Kubernetes-Clustern beenden. Löschen Sie ein Element in dieser Liste, indem Sie auf das Menü mit den drei Punkten klicken und *Löschen* auswählen.

Was passiert, wenn ich meinen abonnierten Verbrauch überschreite?

Warnungen werden angezeigt, wenn die Nutzung Ihrer verwalteten Einheit 80 %, 90 % und 100 % Ihres gesamten Abonnementbetrags überschreitet:

Bei einer Nutzung von mehr als:	Dies passiert / Empfohlene Aktion:
80 %	Es wird ein Informationsbanner angezeigt. Es ist keine Aktion erforderlich.
90%	Es wird ein Warnbanner angezeigt. Möglicherweise möchten Sie die Anzahl Ihrer abonnierten verwalteten Einheiten erhöhen.
100 %	Ein Fehlerbanner wird angezeigt, bis Sie eine der folgenden Aktionen ausführen: • Entfernen Sie Datensammler, sodass die Nutzung Ihrer verwalteten Einheiten Ihrem Abonnement entspricht oder darunter liegt. • Ändern Sie Ihr Abonnement, um die Anzahl der abonnierten verwalteten Einheiten zu erhöhen

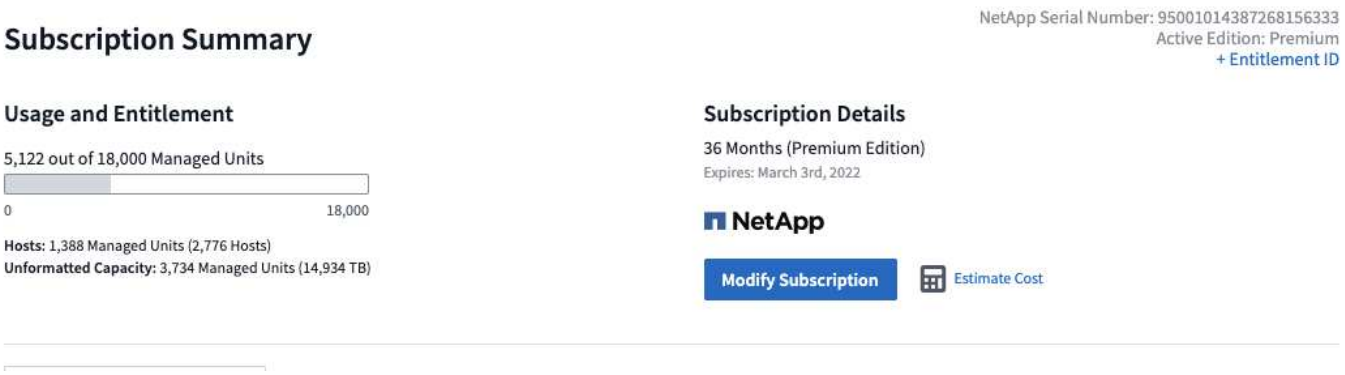
Direkt abonnieren und die Testphase überspringen

Sie können Data Infrastructure Insights auch direkt über die "AWS Marketplace" , ohne vorher eine Testumgebung zu erstellen. Sobald Ihr Abonnement abgeschlossen und Ihre Umgebung eingerichtet ist, werden Sie sofort angemeldet.

Hinzufügen einer Berechtigungs-ID

Wenn Sie ein gültiges NetApp -Produkt besitzen, das mit Data Infrastructure Insights gebündelt ist, können Sie die Seriennummer dieses Produkts zu Ihrem bestehenden Data Infrastructure Insights -Abonnement hinzufügen. Wenn Sie beispielsweise NetApp Astra Control Center erworben haben, kann die Seriennummer der Astra Control Center-Lizenz verwendet werden, um das Abonnement in Data Infrastructure Insights zu identifizieren. Data Infrastructure Insights bezeichnet dies als *Entitlement ID*.

Um Ihrem Data Infrastructure Insights -Abonnement eine Berechtigungs-ID hinzuzufügen, klicken Sie auf der Seite **Admin > Abonnement** auf *+Berechtigungs-ID*.



Beobachtbarkeit

Dashboards erstellen

Dashboards – Übersicht

Data Infrastructure Insights bietet Benutzern die Flexibilität, Betriebsansichten von Infrastrukturdaten zu erstellen, indem Sie benutzerdefinierte Dashboards mit einer Vielzahl von Widgets erstellen können, von denen jedes umfassende Flexibilität bei der Anzeige und Diagrammerstellung Ihrer Daten bietet.

Die Beispiele in diesen Abschnitten dienen nur zu Erklärungszwecken und decken nicht jedes mögliche Szenario ab. Mit den hierin enthaltenen Konzepten und Schritten können Sie Ihre eigenen Dashboards erstellen, um die Daten hervorzuheben, die für Ihre speziellen Anforderungen spezifisch sind.

Erstellen eines Dashboards

Sie erstellen ein neues Dashboard an einem von zwei Orten:

- **Dashboards > [+Neues Dashboard]**
- **Dashboards > Alle Dashboards anzeigen >** Klicken Sie auf die Schaltfläche **[+Dashboard]**

Sehen Sie es in Aktion

Erstellen Sie leistungsstarke Dashboards mit NetApp (Video), Fenster=Später lesen

Dashboard-Steuerelemente

Der Dashboard-Bildschirm verfügt über mehrere Steuerelemente:

- **Zeitauswahl**: Ermöglicht Ihnen die Anzeige von Dashboard-Daten für einen Zeitraum von den letzten 15 Minuten bis zu den letzten 30 Tagen oder einen benutzerdefinierten Zeitraum von bis zu 31 Tagen. Sie können diesen globalen Zeitbereich in einzelnen Widgets überschreiben.
- Schaltfläche **Speichern**: Ermöglicht Ihnen, das Dashboard zu speichern oder zu löschen.

  Sie können das aktuelle Dashboard umbenennen, indem Sie im Menü „Speichern“ auf „Umbenennen“ klicken.

- Schaltfläche **+ Widget hinzufügen**, mit der Sie dem Dashboard eine beliebige Anzahl von Tabellen, Diagrammen oder anderen Widgets hinzufügen können.

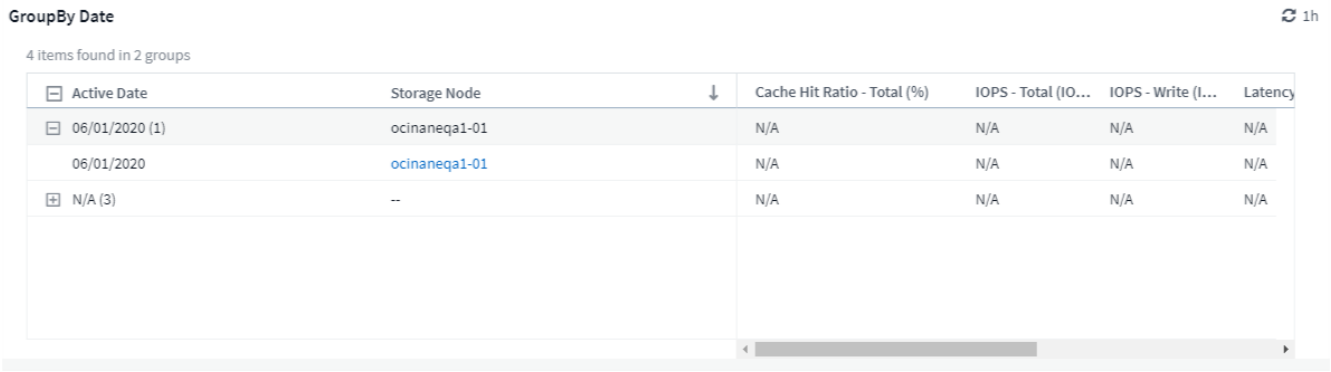
  Die Größe von Widgets kann geändert und sie können an verschiedene Positionen innerhalb des Dashboards verschoben werden, um Ihnen entsprechend Ihren aktuellen Anforderungen die beste Ansicht Ihrer Daten zu bieten.

- Schaltfläche **+ Variable hinzufügen**, mit der Sie Variablen verwenden können, um die Dashboard-Daten aktiv zu filtern.

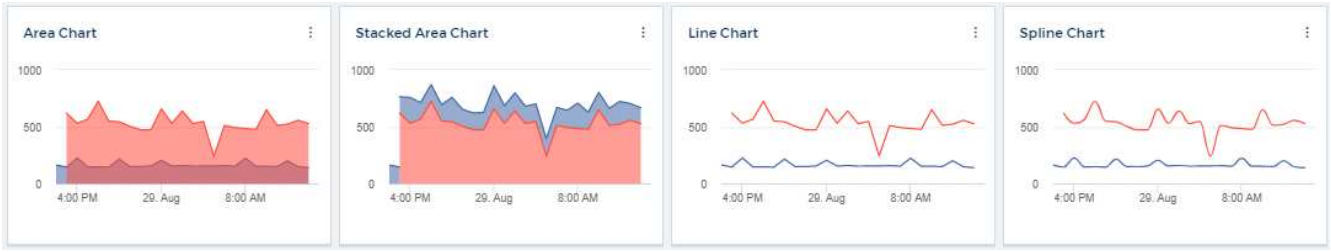
Widget-Typen

Sie können aus den folgenden Widget-Typen wählen:

- **Tabellen-Widget**: Eine Tabelle, die Daten entsprechend den von Ihnen ausgewählten Filtern und Spalten anzeigt. Tabellendaten können in Gruppen zusammengefasst werden, die ein- und ausgeblendet werden können.

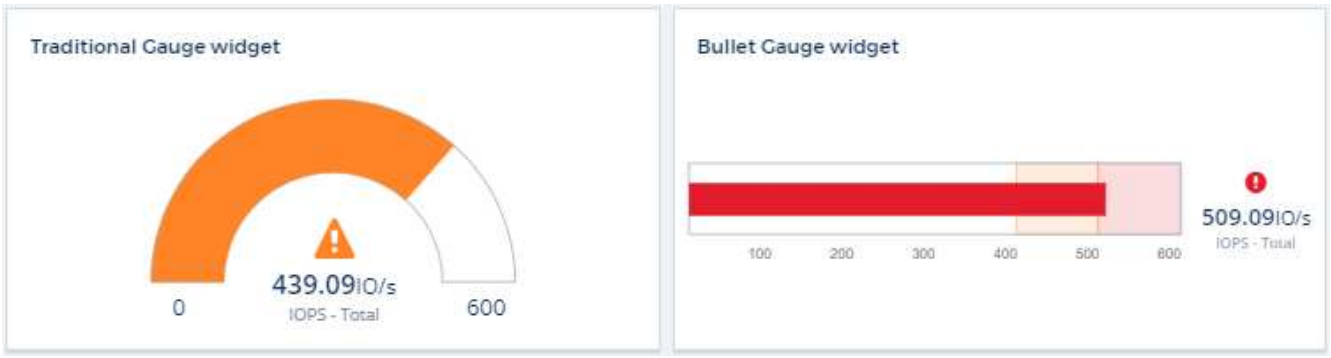


- **Linien-, Spline-, Flächen- und gestapelte Flächendiagramme**: Dies sind Zeitreihendiagramm-Widgets, auf denen Sie die Leistung und andere Daten im Zeitverlauf anzeigen können.

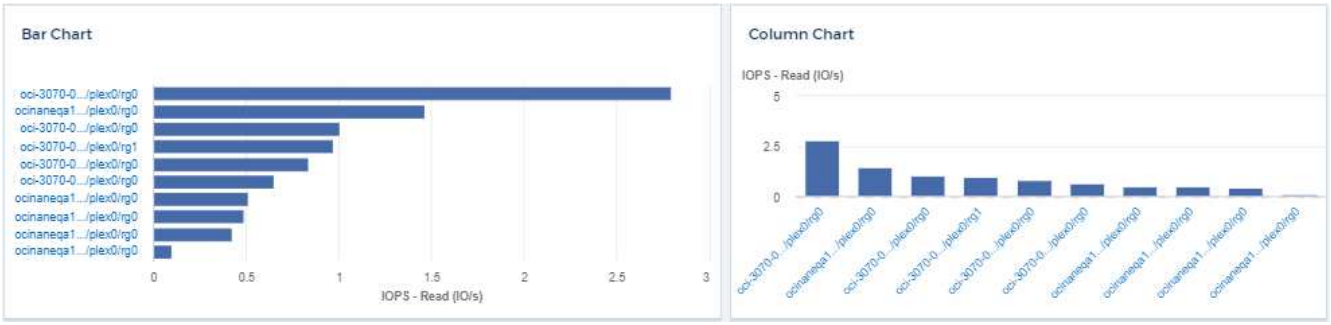


- **Einzelwert-Widget**: Ein Widget, mit dem Sie einen einzelnen Wert anzeigen können, der entweder direkt von einem Zähler abgeleitet oder mithilfe einer Abfrage oder eines Ausdrucks berechnet werden kann. Sie können Schwellenwerte für die Farbformatierung definieren, um anzuzeigen, ob der Wert im erwarteten, Warn- oder kritischen Bereich liegt.

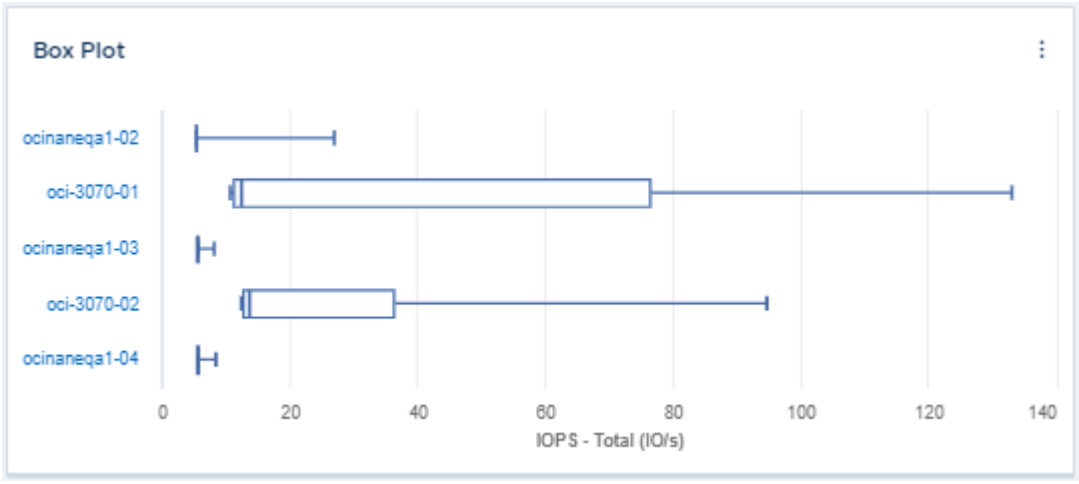
- **Messgerät-Widget**: Zeigt Einzelwertdaten in einem herkömmlichen (durchgezogenen) Messgerät oder Bullet-Messgerät an, mit Farben basierend auf den von Ihnen gewählten "Warn-" oder "Kritischen" Werten"anpassen" .



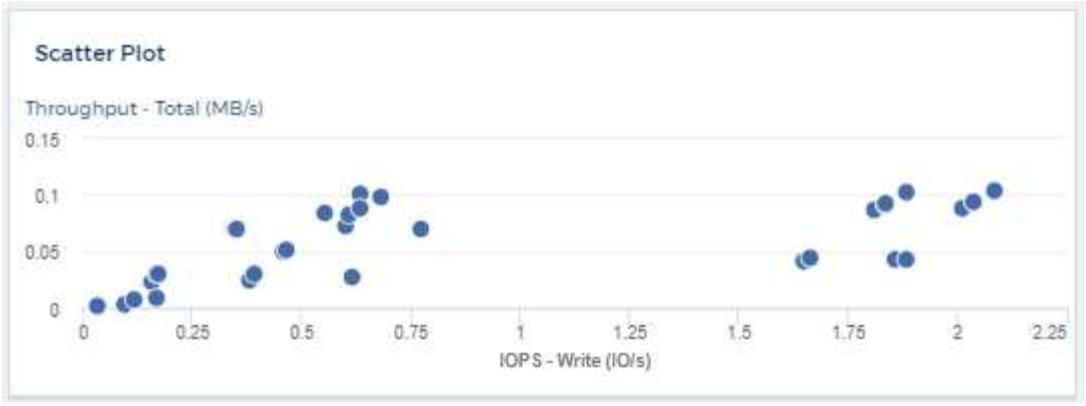
- **Balken-, Säulendiagramme**: Zeigt die höchsten oder niedrigsten N-Werte an, z. B. die zehn größten Speicher nach Kapazität oder die fünf untersten Volumes nach IOPS.



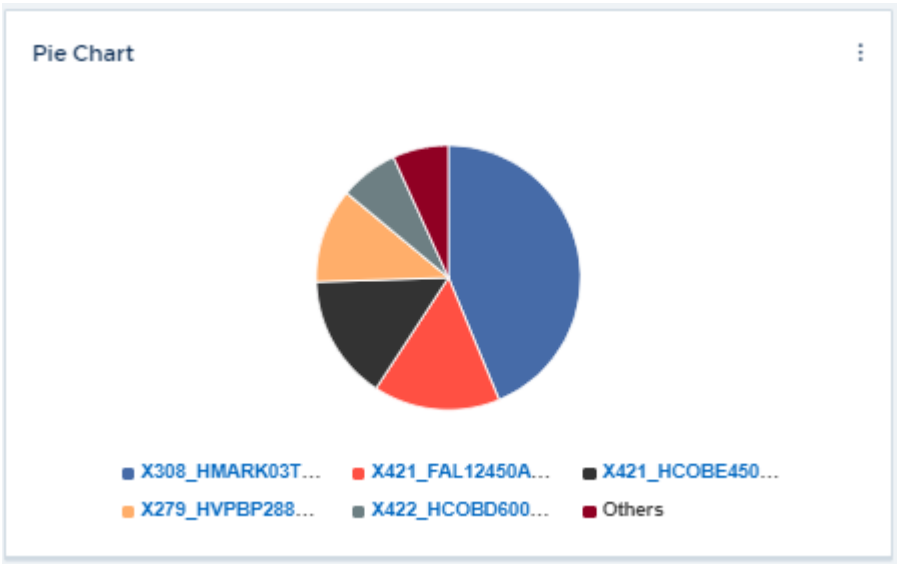
- **Boxplot-Diagramm**: Eine Darstellung des Minimums, Maximums, Medians und des Bereichs zwischen dem unteren und oberen Quartil der Daten in einem einzigen Diagramm.



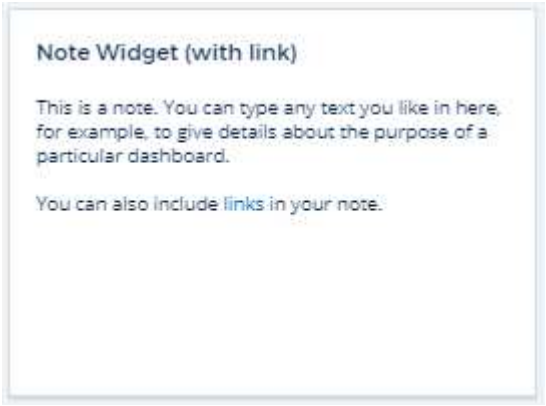
- **Streudiagramm**: Stellt verwandte Daten als Punkte dar, beispielsweise IOPS und Latenz. In diesem Beispiel können Sie schnell Assets mit hohem Durchsatz und niedrigem IOPS finden.



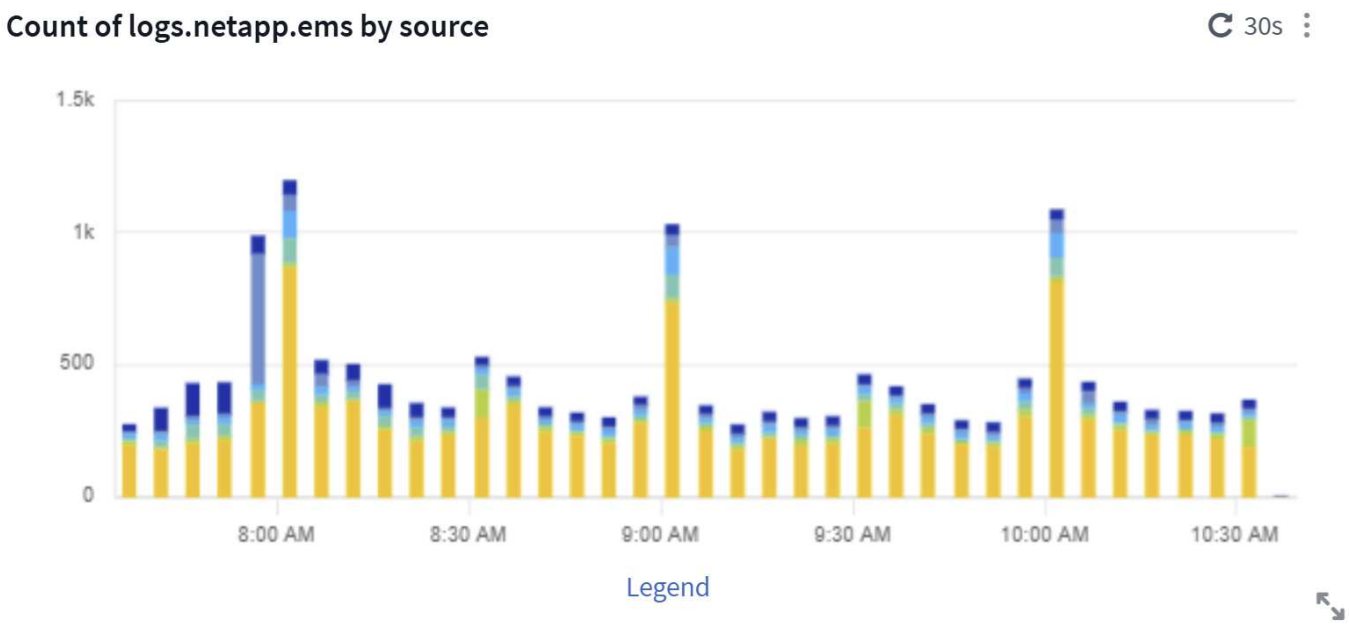
- **Kreisdiagramm**: ein traditionelles Kreisdiagramm zur Anzeige von Daten als Teil des Gesamtwerts.



- **Notiz-Widget**: Bis zu 1000 Zeichen Freitext.



- **Zeitbalkendiagramm**: Zeigt Protokoll- oder Messdaten im Zeitverlauf an.



- **Warnungstabelle**: Zeigt bis zu den letzten 1.000 Warnungen an.

Ausführlichere Erklärungen zu diesen und anderen Dashboard-Funktionen finden Sie unter"klicken Sie hier," .

Ein Dashboard als Startseite festlegen

Sie können mit einer der folgenden Methoden auswählen, welches Dashboard als **Startseite** Ihres Mandanten festgelegt werden soll:

- Gehen Sie zu **Dashboards > Alle Dashboards anzeigen**, um die Liste der Dashboards auf Ihrem Mandanten anzuzeigen. Klicken Sie auf das Optionsmenü rechts neben dem gewünschten Dashboard und wählen Sie **Als Startseite festlegen**.
- Klicken Sie auf ein Dashboard in der Liste, um das Dashboard zu öffnen. Klicken Sie auf das Dropdown-Menü in der oberen Ecke und wählen Sie **Als Startseite festlegen**.

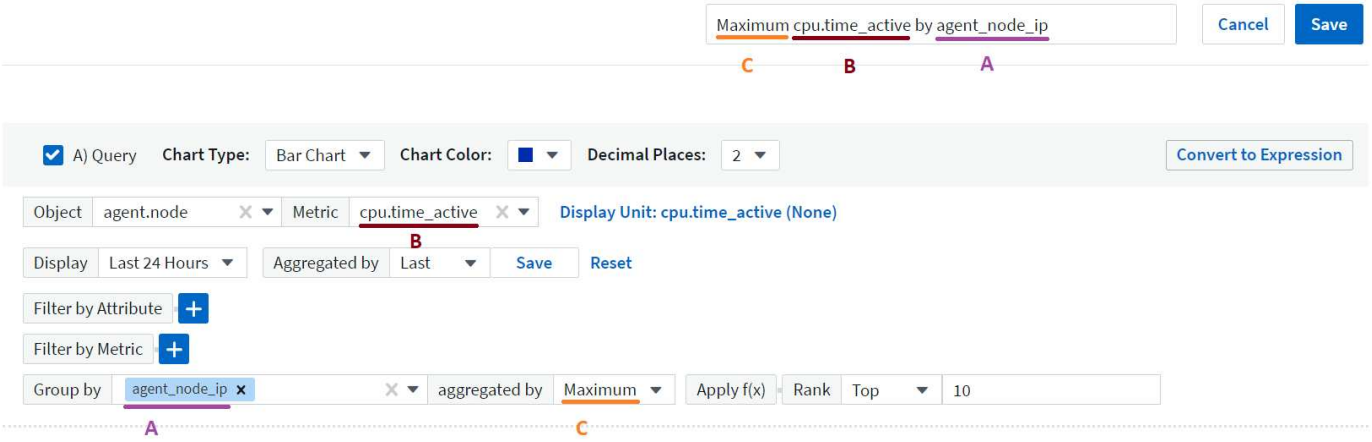
Dashboard-Funktionen

Dashboards und Widgets ermöglichen große Flexibilität bei der Datenanzeige. Hier sind einige Konzepte, die Ihnen dabei helfen, das Beste aus Ihren benutzerdefinierten Dashboards herauszuholen.

Inhaltsverzeichnis:[]

Widget-Benennung

Widgets werden automatisch basierend auf dem Objekt, der Metrik oder dem Attribut benannt, das für die erste Widget-Abfrage ausgewählt wurde. Wenn Sie zusätzlich eine Gruppierung für das Widget wählen, werden die „Gruppieren nach“-Attribute in die automatische Benennung (Aggregationsmethode und Metrik) einbezogen.



Durch Auswahl eines neuen Objekts oder Gruppierungsattributs wird der automatische Name aktualisiert.

Wenn Sie den automatischen Widget-Namen nicht verwenden möchten, können Sie einfach einen neuen Namen eingeben.

Platzierung und Größe des Widgets

Alle Dashboard-Widgets können entsprechend Ihren Anforderungen für das jeweilige Dashboard positioniert und in der Größe angepasst werden.

Duplizieren eines Widgets

Klicken Sie im Dashboard-Bearbeitungsmodus auf das Menü im Widget und wählen Sie **Duplizieren**. Der Widget-Editor wird gestartet und ist bereits mit der Konfiguration des Original-Widgets und dem Suffix „Kopie“ im Widget-Namen ausgefüllt. Sie können problemlos alle erforderlichen Änderungen vornehmen und das neue Widget speichern. Das Widget wird unten in Ihrem Dashboard platziert und Sie können es nach Bedarf positionieren. Denken Sie daran, Ihr Dashboard zu speichern, wenn alle Änderungen abgeschlossen sind.

Anzeigen von Widget-Legenden

Die meisten Widgets auf Dashboards können mit oder ohne Legenden angezeigt werden. Legenden in Widgets können auf einem Dashboard mit einer der folgenden Methoden ein- oder ausgeschaltet werden:

- Klicken Sie beim Anzeigen des Dashboards auf die Schaltfläche **Optionen** im Widget und wählen Sie im Menü **Legenden anzeigen** aus.

Wenn sich die im Widget angezeigten Daten ändern, wird die Legende für dieses Widget dynamisch aktualisiert.

Wenn Legenden angezeigt werden und die Zielseite des durch die Legende angegebenen Assets aufgerufen werden kann, wird die Legende als Link zu dieser Asset-Seite angezeigt. Wenn in der Legende „Alle“ angezeigt wird, wird durch Klicken auf den Link eine Abfrageseite angezeigt, die der ersten Abfrage im Widget entspricht.

Metriken transformieren

Data Infrastructure Insights bietet verschiedene *Transformations*optionen für bestimmte Metriken in Widgets (insbesondere die als „Benutzerdefiniert“ oder „Integrationsmetriken“ bezeichneten Metriken, z. B. von Kubernetes, ONTAP Advanced Data, Telegraf-Plugins usw.), sodass Sie die Daten auf verschiedene Arten anzeigen können. Wenn Sie einem Widget transformierbare Metriken hinzufügen, wird Ihnen ein Dropdown-

Menü mit den folgenden Transformationsoptionen angezeigt:

Keine: Die Daten werden unverändert und ohne Manipulation angezeigt.

Rate: Aktueller Wert geteilt durch den Zeitraum seit der letzten Beobachtung.

Kumulativ: Die Ansammlung der Summe der vorherigen Werte und des aktuellen Werts.

Delta: Die Differenz zwischen dem vorherigen Beobachtungswert und dem aktuellen Wert.

Deltarate: Deltawert geteilt durch den Zeitraum seit der letzten Beobachtung.

Kumulative Rate: Kumulativer Wert geteilt durch den Zeitraum seit der letzten Beobachtung.

Beachten Sie, dass durch die Transformation von Metriken nicht die zugrunde liegenden Daten selbst geändert werden, sondern nur die Art und Weise, wie die Daten angezeigt werden.

Dashboard-Widget-Abfragen und -Filter

Abfragen

Die Abfrage in einem Dashboard-Widget ist ein leistungsstarkes Tool zum Verwalten der Anzeige Ihrer Daten. Hier sind einige Dinge, die Sie bei Widget-Abfragen beachten sollten.

Einige Widgets können bis zu fünf Abfragen haben. Jede Abfrage zeichnet ihren eigenen Satz von Linien oder Diagrammen im Widget. Das Festlegen von Rollup, Gruppierung, Top-/Bottom-Ergebnissen usw. für eine Abfrage hat keine Auswirkungen auf andere Abfragen für das Widget.

Sie können auf das Augensymbol klicken, um eine Abfrage vorübergehend auszublenden. Die Widget-Anzeige wird automatisch aktualisiert, wenn Sie eine Abfrage ausblenden oder anzeigen. Auf diese Weise können Sie beim Erstellen Ihres Widgets Ihre angezeigten Daten für einzelne Abfragen überprüfen.

Die folgenden Widgettypen können mehrere Abfragen haben:

- Flächendiagramm
- Gestapeltes Flächendiagramm
- Liniendiagramm
- Spline-Diagramm
- Einzelwert-Widget

Die übrigen Widgettypen können nur eine einzige Abfrage haben:

- Tabelle
- Balkendiagramm
- Boxplot
- Streudiagramm

Filtern in Dashboard-Widget-Abfragen

Hier sind einige Dinge, die Sie tun können, um das Beste aus Ihren Filtern herauszuholen.

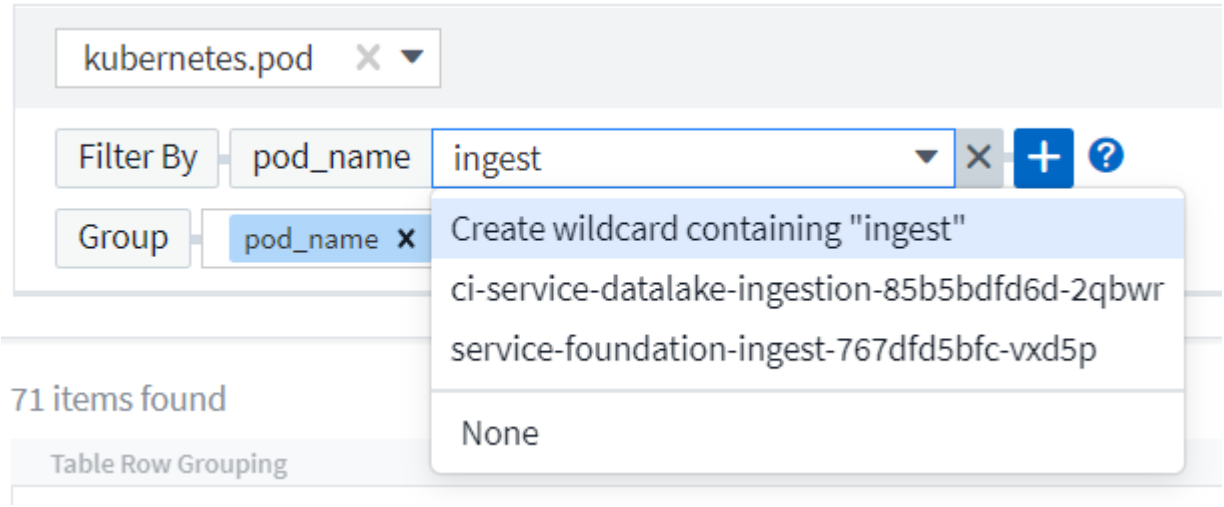
Filtern nach exakter Übereinstimmung

Wenn Sie eine Filterzeichenfolge in doppelte Anführungszeichen setzen, behandelt Insight alles zwischen dem ersten und letzten Anführungszeichen als exakte Übereinstimmung. Alle Sonderzeichen oder Operatoren innerhalb der Anführungszeichen werden als Literale behandelt. Wenn Sie beispielsweise nach „*“ filtern, werden Ergebnisse zurückgegeben, die ein Sternchen sind. Das Sternchen wird in diesem Fall nicht als Platzhalter behandelt. Die Operatoren AND, OR und NOT werden auch als Literalzeichenfolgen behandelt, wenn sie in doppelte Anführungszeichen eingeschlossen sind.

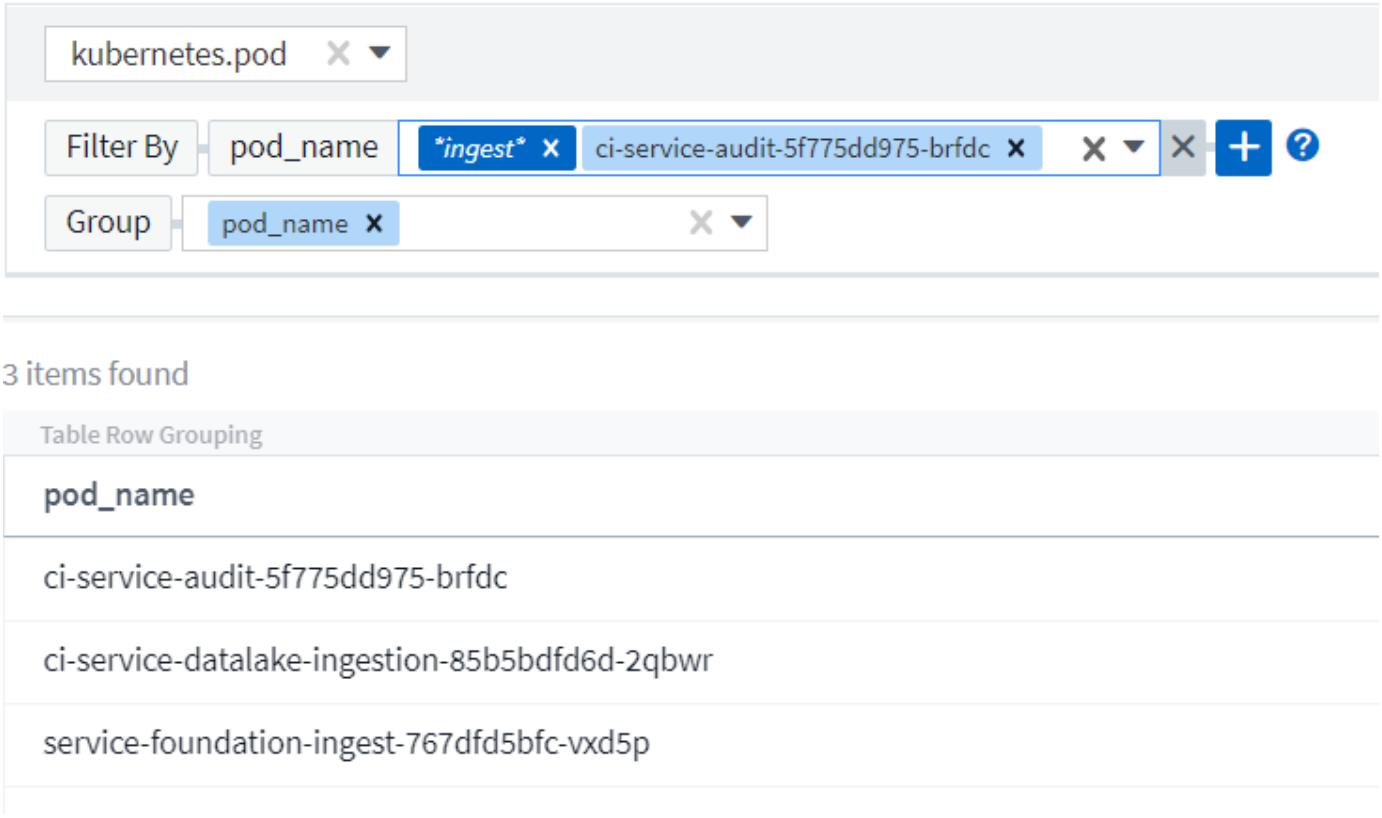
Sie können Filter für exakte Übereinstimmungen verwenden, um bestimmte Ressourcen zu finden, beispielsweise den Hostnamen. Wenn Sie nur den Hostnamen „marketing“ suchen, aber „marketing01“, „marketing-boston“ usw. ausschließen möchten, schließen Sie den Namen „marketing“ einfach in Anführungszeichen ein.

Platzhalter und Ausdrücke

Wenn Sie in Abfragen oder Dashboard-Widgets nach Text oder Listenwerten filtern, wird Ihnen beim Eintippen die Option angezeigt, einen **Platzhalterfilter** basierend auf dem aktuellen Text zu erstellen. Wenn Sie diese Option auswählen, werden alle Ergebnisse zurückgegeben, die mit dem Platzhalterausdruck übereinstimmen. Sie können **Ausdrücke** auch mit NOT oder OR erstellen oder die Option „Keine“ auswählen, um nach Nullwerten im Feld zu filtern.



Filter, die auf Platzhaltern oder Ausdrücken basieren (z. B. NICHT, ODER, „Keine“ usw.), werden im Filterfeld dunkelblau angezeigt. Elemente, die Sie direkt aus der Liste auswählen, werden hellblau angezeigt.



Beachten Sie, dass die Platzhalter- und Ausdrucksfilterung mit Text oder Listen funktioniert, jedoch nicht mit Zahlen, Datumsangaben oder Booleschen Werten.

Erweiterte Textfilterung mit kontextbezogenen Type-Ahead-Vorschlägen

Das Filtern in Widget-Abfragen ist *kontextbezogen*. Wenn Sie einen oder mehrere Filterwerte für ein Feld auswählen, zeigen die anderen Filter für diese Abfrage die für diesen Filter relevanten Werte an. Wenn Sie beispielsweise einen Filter für einen bestimmten Objektnamen festlegen, werden im Feld zum Filtern nach Modell nur Werte angezeigt, die für diesen Objektnamen relevant sind.

Die kontextbezogene Filterung gilt auch für Dashboard-Seitenvariablen (nur Textattribute oder Anmerkungen). Wenn Sie einen Filterwert für eine Variable auswählen, werden für alle anderen Variablen, die verwandte Objekte verwenden, nur mögliche Filterwerte basierend auf dem Kontext dieser verwandten Variablen angezeigt.

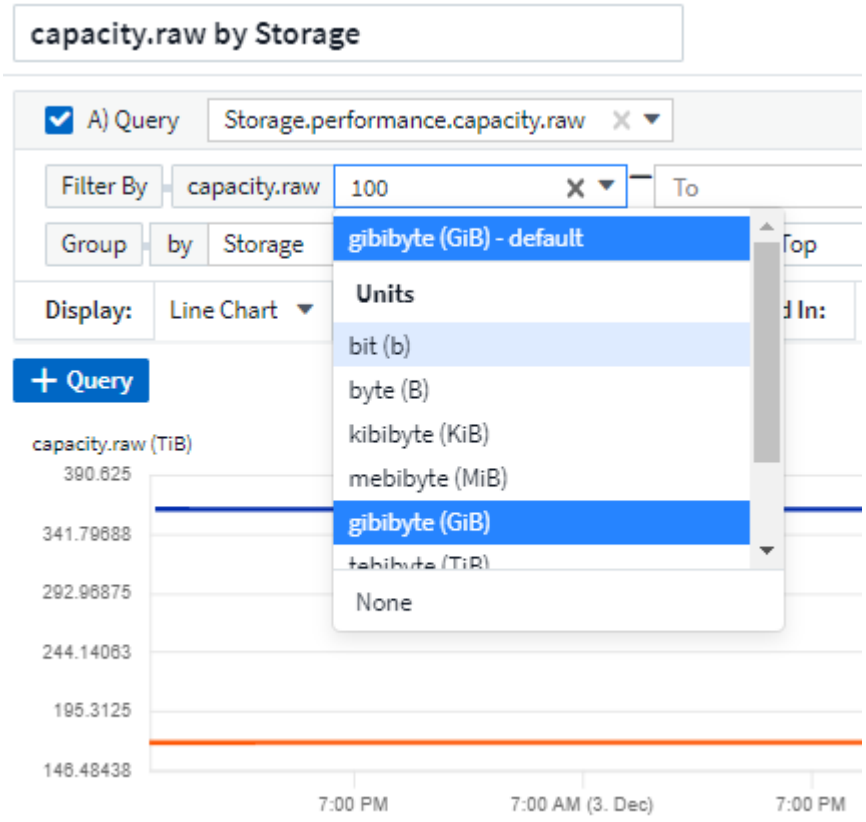
Beachten Sie, dass nur Textfilter kontextbezogene Type-Ahead-Vorschläge anzeigen. Für Datum, Enumeration (Liste) usw. werden keine Vorschläge zur Typvervollständigung angezeigt. Das heißt, Sie *können* einen Filter auf ein Enumerationsfeld (d. h. ein Listenfeld) setzen und andere Textfelder im Kontext filtern lassen. Wenn Sie beispielsweise einen Wert in einem Enumerationsfeld wie „Rechenzentrum“ auswählen, werden in anderen Filtern nur die Modelle/Namen in diesem Rechenzentrum angezeigt, aber nicht umgekehrt.

Der ausgewählte Zeitraum bietet auch Kontext für die in den Filtern angezeigten Daten.

Auswahl der Filtereinheiten

Wenn Sie einen Wert in ein Filterfeld eingeben, können Sie die Einheiten auswählen, in denen die Werte im Diagramm angezeigt werden sollen. Sie können beispielsweise nach Rohkapazität filtern und die Anzeige im Standard-GiB oder ein anderes Format wie TiB auswählen. Dies ist nützlich, wenn Sie auf Ihrem Dashboard mehrere Diagramme haben, die Werte in TiB anzeigen, und Sie möchten, dass alle Ihre Diagramme

konsistente Werte anzeigen.



Zusätzliche Filterverfeinerungen

Mit den folgenden Angaben können Sie Ihre Filter weiter verfeinern.

- Mit einem Sternchen können Sie nach allem suchen. Zum Beispiel,

  ```
  vol*rhel
  ```

  zeigt alle Ressourcen an, die mit „vol“ beginnen und mit „rhel“ enden.

- Mit dem Fragezeichen können Sie nach einer bestimmten Anzahl von Zeichen suchen. Zum Beispiel,

  ```
  BOS-PRD??-S12
  ```

  zeigt *BOS-PRD12-S12*, *BOS-PRD13-S12* usw. an.

- Mit dem ODER-Operator können Sie mehrere Entitäten angeben. Zum Beispiel,

  ```
  FAS2240 OR CX600 OR FAS3270
  ```

  findet mehrere Speichermodelle.

- Mit dem Operator „NOT“ können Sie Text aus den Suchergebnissen ausschließen. Zum Beispiel,

```
NOT EMC*
```

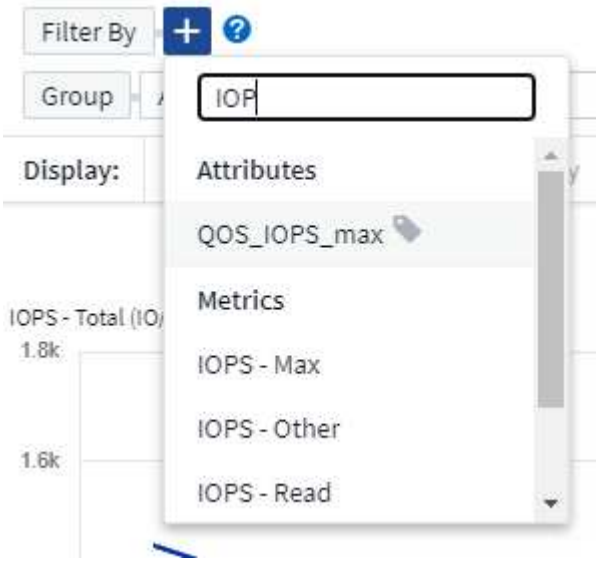
findet alles, was nicht mit „EMC“ beginnt. Sie können

```
NOT *
```

um Felder anzuzeigen, die keinen Wert enthalten.

Identifizieren von Objekten, die von Abfragen und Filtern zurückgegeben werden

Die von Abfragen und Filtern zurückgegebenen Objekte ähneln denen in der folgenden Abbildung. Objekte mit zugewiesenen „Tags“ sind Anmerkungen, während Objekte ohne Tags Leistungsindikatoren oder Objektattribute sind.



Gruppierung und Aggregation

Gruppierung (Aufrollen)

Die in einem Widget angezeigten Daten werden aus den während der Erfassung gesammelten zugrunde liegenden Datenpunkten gruppiert (manchmal auch als zusammengefasst bezeichnet). Wenn Sie beispielsweise über ein Liniendiagramm-Widget verfügen, das die Speicher-IOPS im Zeitverlauf anzeigt, möchten Sie möglicherweise für jedes Ihrer Rechenzentren eine separate Linie anzeigen, um einen schnellen Vergleich zu ermöglichen. Sie können diese Daten auf verschiedene Arten gruppieren:

- **Durchschnitt**: zeigt jede Zeile als *Durchschnitt* der zugrunde liegenden Daten an.
- **Maximum**: zeigt jede Zeile als *Maximum* der zugrunde liegenden Daten an.
- **Minimum**: zeigt jede Zeile als *Minimum* der zugrunde liegenden Daten an.
- **Summe**: zeigt jede Zeile als *Summe* der zugrunde liegenden Daten an.
- **Anzahl**: Zeigt eine *Anzahl* von Objekten an, die innerhalb des angegebenen Zeitraums Daten gemeldet

haben. Sie können das *Gesamte Zeitfenster* entsprechend dem Zeitbereich des Dashboards auswählen.

Schritte

Gehen Sie wie folgt vor, um die Gruppierungsmethode festzulegen.

1. Wählen Sie in der Abfrage Ihres Widgets einen Asset-Typ und eine Metrik (z. B. *Speicher*) und eine Metrik (z. B. *Performance IOPS Total*) aus.
2. Wählen Sie für **Gruppe** eine Rollup-Methode (z. B. *Durchschnitt*) und wählen Sie die Attribute oder Metriken aus, nach denen die Daten zusammengefasst werden sollen (z. B. *Rechenzentrum*).

   Das Widget wird automatisch aktualisiert und zeigt Daten für jedes Ihrer Rechenzentren an.

Sie können auch *alle* zugrunde liegenden Daten im Diagramm oder in der Tabelle gruppieren. In diesem Fall erhalten Sie für jede Abfrage im Widget eine einzelne Zeile, die den Durchschnitt, das Minimum, das Maximum, die Summe oder die Anzahl der ausgewählten Metrik(en) für alle zugrunde liegenden Assets anzeigt.

Wenn Sie auf die Legende eines Widgets klicken, dessen Daten nach „Alle“ gruppiert sind, wird eine Abfrageseite geöffnet, auf der die Ergebnisse der ersten im Widget verwendeten Abfrage angezeigt werden.

Wenn Sie einen Filter für die Abfrage festgelegt haben, werden die Daten basierend auf den gefilterten Daten gruppiert.

Beachten Sie, dass Sie, wenn Sie ein Widget nach einem beliebigen Feld (z. B. *Modell*) gruppieren, dennoch nach diesem Feld filtern müssen, um die Daten für dieses Feld im Diagramm oder in der Tabelle richtig anzuzeigen.

Daten aggregieren

Sie können Ihre Zeitreihendiagramme (Linie, Fläche usw.) weiter ausrichten, indem Sie Datenpunkte in Minuten-, Stunden- oder Tagesintervalle aggregieren, bevor diese Daten anschließend nach Attributen zusammengefasst werden (falls ausgewählt). Sie können Datenpunkte nach ihrem *Durchschnitt, Maximum, Minimum, ihrer Summe oder ihrer _Anzahl* aggregieren.

Ein kleines Intervall in Kombination mit einem langen Zeitbereich kann zu der Warnung „Aggregationsintervall ergab zu viele Datenpunkte.“ führen. Dies wird möglicherweise angezeigt, wenn Sie ein kleines Intervall haben und den Zeitrahmen des Dashboards auf 7 Tage erhöhen. In diesem Fall erhöht Insight vorübergehend das Aggregationsintervall, bis Sie einen kleineren Zeitrahmen auswählen.

Sie können Daten auch im Balkendiagramm-Widget und im Einzelwert-Widget aggregieren.

Die meisten Asset-Zähler ergeben standardmäßig den *Durchschnitt*. Einige Zähler werden standardmäßig zu *Max, Min* oder *Sum* aggregiert. Beispielsweise werden Portfehler standardmäßig zu *Summe* aggregiert, während Speicher-IOPS zu *Durchschnitt* aggregiert werden.

Anzeigen der Top-/Bottom-Ergebnisse

In einem Diagramm-Widget können Sie entweder die **obersten** oder **untersten** Ergebnisse für zusammengefasste Daten anzeigen und die Anzahl der angezeigten Ergebnisse aus der bereitgestellten Dropdown-Liste auswählen. In einem Tabellen-Widget können Sie nach jeder Spalte sortieren.

Diagramm-Widget oben/unten

Wenn Sie in einem Diagramm-Widget die Daten nach einem bestimmten Attribut zusammenfassen, haben Sie

die Möglichkeit, entweder die obersten N oder die untersten N Ergebnisse anzuzeigen. Beachten Sie, dass Sie nicht die obersten oder untersten Ergebnisse auswählen können, wenn Sie die Zusammenfassung nach *allen* Attributen auswählen.

Sie können auswählen, welche Ergebnisse angezeigt werden sollen, indem Sie im Feld **Anzeigen** der Abfrage entweder **Oben** oder **Unten** auswählen und einen Wert aus der bereitgestellten Liste auswählen.

Tabellen-Widget zeigt Einträge an

In einem Tabellen-Widget können Sie die Anzahl der in den Tabellenergebnissen angezeigten Ergebnisse auswählen. Sie haben nicht die Möglichkeit, die obersten oder untersten Ergebnisse auszuwählen, da Sie in der Tabelle bei Bedarf nach jeder Spalte aufsteigend oder absteigend sortieren können.

Sie können die Anzahl der in der Tabelle auf dem Dashboard anzuzeigenden Ergebnisse auswählen, indem Sie einen Wert aus dem Feld **Einträge anzeigen** der Abfrage auswählen.

Gruppierung im Tabellen-Widget

Daten in einem Tabellen-Widget können nach jedem verfügbaren Attribut gruppiert werden, sodass Sie eine Übersicht über Ihre Daten erhalten und für weitere Details tiefer in die Daten einsteigen können. Die Messwerte in der Tabelle werden zur einfacheren Anzeige in jeder reduzierten Zeile zusammengefasst.

Mit Tabellen-Widgets können Sie Ihre Daten basierend auf den von Ihnen festgelegten Attributen gruppieren. Beispielsweise möchten Sie möglicherweise, dass Ihre Tabelle die gesamten Speicher-IOPS gruppiert nach den Rechenzentren anzeigt, in denen sich diese Speicher befinden. Oder Sie möchten eine Tabelle mit virtuellen Maschinen anzeigen, die nach dem Hypervisor gruppiert sind, auf dem sie gehostet werden. In der Liste können Sie jede Gruppe erweitern, um die Assets in dieser Gruppe anzuzeigen.

Gruppierung ist nur im Widgettyp „Tabelle“ verfügbar.

Gruppierungsbeispiel (mit Erläuterung der Zusammenfassung)

Mit Tabellen-Widgets können Sie Daten zur einfacheren Anzeige gruppieren.

In diesem Beispiel erstellen wir ein Tabellen-Widget, das alle VMs gruppiert nach Rechenzentrum anzeigt.

Schritte

1. Erstellen oder öffnen Sie ein Dashboard und fügen Sie ein **Tabellen**-Widget hinzu.
2. Wählen Sie *Virtuelle Maschine* als Asset-Typ für dieses Widget.
3. Klicken Sie auf den Spaltenselektor und wählen Sie *Hypervisorname* und *IOPS – Gesamt*.

   Diese Spalten werden jetzt in der Tabelle angezeigt.

4. Lassen Sie uns alle VMs ohne IOPS außer Acht lassen und nur VMs einbeziehen, deren Gesamt-IOPS größer als 1 ist. Klicken Sie auf die Schaltfläche **Filtern nach [+]** und wählen Sie *IOPS – Gesamt* aus. Klicken Sie auf *Beliebig* und geben Sie im Feld **Von 1** ein. Lassen Sie das Feld **An** leer. Drücken Sie die Eingabetaste oder klicken Sie außerhalb des Filterfelds, um den Filter anzuwenden.

   Die Tabelle zeigt jetzt alle VMs mit einem Gesamt-IOPS größer oder gleich 1. Beachten Sie, dass in der Tabelle keine Gruppierung vorhanden ist. Alle VMs werden angezeigt.

5. Klicken Sie auf die Schaltfläche **Gruppieren nach [+]**.

   Sie können nach jedem angezeigten Attribut oder jeder angezeigten Anmerkung gruppieren. Wählen Sie

Alle, um alle VMs in einer einzigen Gruppe anzuzeigen.

Jede Spaltenüberschrift für eine Leistungsmetrik zeigt ein Drei-Punkte-Menü mit einer **Rollup**-Option an. Die Standard-Rollup-Methode ist *Durchschnitt*. Dies bedeutet, dass die für die Gruppe angezeigte Zahl der Durchschnitt aller für jede VM innerhalb der Gruppe gemeldeten Gesamt-IOPS ist. Sie können diese Spalte nach *Durchschnitt, Summe, Minimum* oder *Maximum* aufrollen. Jede von Ihnen angezeigte Spalte mit Leistungsmetriken kann einzeln zusammengefasst werden.

6. Klicken Sie auf *Alle* und wählen Sie *Hypervisorname* aus.

   Die VM-Liste ist jetzt nach Hypervisor gruppiert. Sie können jeden Hypervisor erweitern, um die von ihm gehosteten VMs anzuzeigen.

7. Klicken Sie auf **Speichern**, um die Tabelle im Dashboard zu speichern. Sie können die Größe des Widgets nach Wunsch ändern oder es verschieben.
8. Klicken Sie auf **Speichern**, um das Dashboard zu speichern.

Leistungsdaten-Rollup

Wenn Sie in ein Tabellen-Widget eine Spalte für Leistungsdaten (z. B. *IOPS – Gesamt*) aufnehmen und die Daten gruppieren möchten, können Sie anschließend eine Rollup-Methode für diese Spalte auswählen. Die Standard-Rollup-Methode besteht darin, den Durchschnitt (*avg*) der zugrunde liegenden Daten in der Gruppenzeile anzuzeigen. Sie können auch wählen, ob die Summe, das Minimum oder das Maximum der Daten angezeigt werden soll.

Dashboard-Zeitbereichsauswahl

Sie können den Zeitraum für Ihre Dashboard-Daten auswählen. In Widgets auf dem Dashboard werden nur Daten angezeigt, die für den ausgewählten Zeitraum relevant sind. Sie können aus folgenden Zeiträumen auswählen:

- Letzte 15 Minuten
- Letzte 30 Minuten
- Letzte 60 Minuten

- Letzte 2 Stunden
- Letzte 3 Stunden (dies ist die Standardeinstellung)
- Letzte 6 Stunden
- Letzte 12 Stunden
- Letzte 24 Stunden
- Letzte 2 Tage
- Letzte 3 Tage
- Letzte 7 Tage
- Letzte 30 Tage
- Benutzerdefinierter Zeitbereich

  Mit dem benutzerdefinierten Zeitbereich können Sie bis zu 31 aufeinanderfolgende Tage auswählen. Sie können auch die Start- und Endzeit des Tages für diesen Bereich festlegen. Die Standardstartzeit ist 0:00 Uhr am ersten ausgewählten Tag und die Standardendzeit ist 23:59 Uhr am letzten ausgewählten Tag. Durch Klicken auf **Übernehmen** wird der benutzerdefinierte Zeitraum auf das Dashboard angewendet.

In einen Zeitbereich hineinzoomen

Beim Anzeigen eines Zeitreihen-Widgets (Linie, Spline, Fläche, gestapelte Fläche) – oder eines Diagramms auf einer Zielseite – können Sie die Maus über das Diagramm ziehen, um es zu vergrößern. Oben rechts auf dem Bildschirm können Sie dann diesen Zeitraum sperren, sodass Diagramme auf anderen Seiten Daten für diesen gesperrten Zeitraum widerspiegeln. Wählen Sie zum Entsperren einen anderen Zeitraum aus der Liste aus.

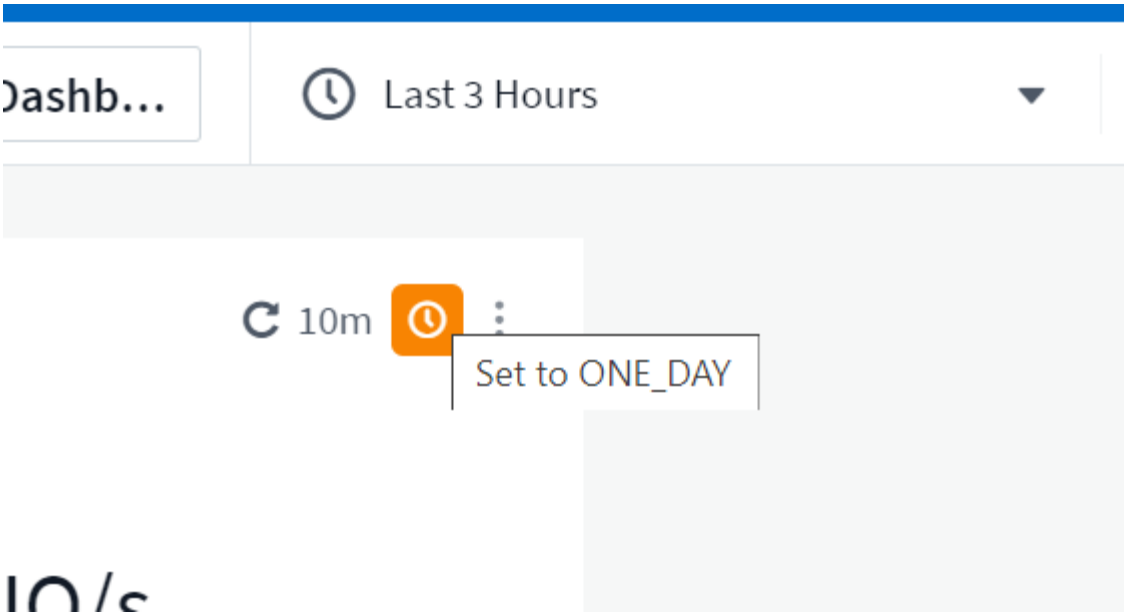
Überschreiben der Dashboard-Zeit in einzelnen Widgets

Sie können die Zeitbereichseinstellung des Haupt-Dashboards in einzelnen Widgets überschreiben. Diese Widgets zeigen Daten basierend auf ihrem festgelegten Zeitrahmen an, nicht auf dem Zeitrahmen des Dashboards.

Um die Dashboard-Zeit zu überschreiben und ein Widget zu zwingen, seinen eigenen Zeitrahmen zu verwenden, wählen Sie im Bearbeitungsmodus des Widgets den gewünschten Zeitraum aus und speichern Sie das Widget im Dashboard.

Das Widget zeigt seine Daten entsprechend dem dafür festgelegten Zeitrahmen an, unabhängig von dem Zeitrahmen, den Sie auf dem Dashboard selbst auswählen.

Der Zeitrahmen, den Sie für ein Widget festlegen, wirkt sich nicht auf andere Widgets auf dem Dashboard aus.



Primäre und sekundäre Achse

Verschiedene Metriken verwenden unterschiedliche Maßeinheiten für die Daten, die sie in einem Diagramm darstellen. Bei IOPS beispielsweise ist die Maßeinheit die Anzahl der E/A-Vorgänge pro Sekunde (IO/s), während die Latenz ein reines Zeitmaß ist (Millisekunden, Mikrosekunden, Sekunden usw.). Wenn Sie beide Metriken in einem einzelnen Liniendiagramm mit einem einzigen Satz von Werten für die Y-Achse darstellen, werden die Latenzzahlen (normalerweise einige Millisekunden) auf derselben Skala wie die IOPS (normalerweise im Tausenderbereich) dargestellt, und die Latenzlinie geht in dieser Skala verloren.

Es ist jedoch möglich, beide Datensätze in einem einzigen aussagekräftigen Diagramm darzustellen, indem man eine Maßeinheit auf der primären (linken) Y-Achse und die andere Maßeinheit auf der sekundären (rechten) Y-Achse festlegt. Jede Metrik wird in einem eigenen Maßstab dargestellt.

Schritte

Dieses Beispiel veranschaulicht das Konzept der primären und sekundären Achsen in einem Diagramm-Widget.

1. Erstellen oder öffnen Sie ein Dashboard. Fügen Sie dem Dashboard ein Liniendiagramm-, Spline-Diagramm-, Flächendiagramm- oder gestapeltes Flächendiagramm-Widget hinzu.
2. Wählen Sie einen Asset-Typ (z. B. *Speicher*) und wählen Sie *IOPS – Gesamt* für Ihre erste Metrik. Legen Sie beliebige Filter fest und wählen Sie bei Bedarf eine Rollup-Methode.

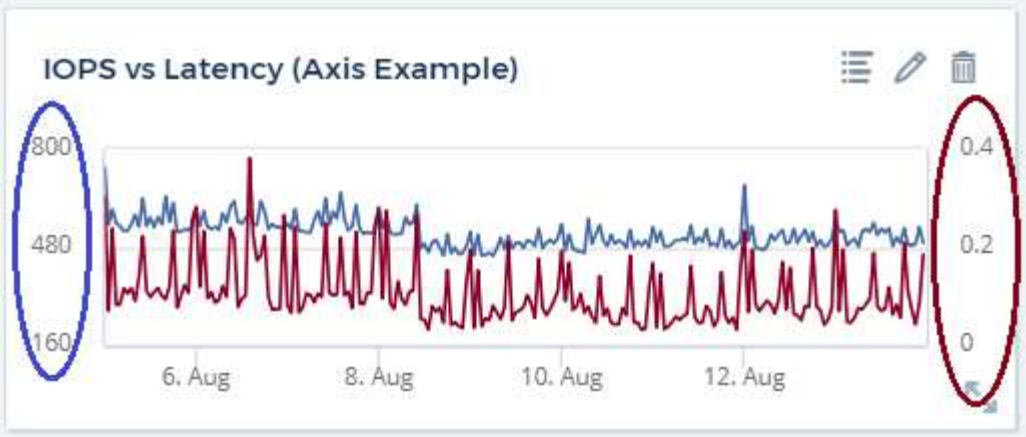
   Die IOPS-Linie wird im Diagramm angezeigt, ihre Skala ist links dargestellt.

3. Klicken Sie auf **[+Abfrage]**, um dem Diagramm eine zweite Linie hinzuzufügen. Wählen Sie für diese Zeile als Metrik *Latenz – Gesamt*.

   Beachten Sie, dass die Linie unten im Diagramm flach angezeigt wird. Dies liegt daran, dass sie *im gleichen Maßstab* wie die IOPS-Linie gezeichnet wird.

4. Wählen Sie in der Latenzabfrage **Y-Achse: Sekundär** aus.

   Die Latenzlinie wird jetzt in einer eigenen Skala gezeichnet, die auf der rechten Seite des Diagramms angezeigt wird.



Ausdrücke in Widgets

In einem Dashboard können Sie mit jedem Zeitreihen-Widget (Linie, Spline, Fläche, gestapelte Fläche), Balkendiagramm, Säulendiagramm, Kreisdiagramm oder Tabellen-Widget Ausdrücke aus den von Ihnen gewählten Metriken erstellen und das Ergebnis dieser Ausdrücke in einem einzelnen Diagramm (oder einer Spalte im Fall desTabellen-Widget). In den folgenden Beispielen werden Ausdrücke verwendet, um bestimmte Probleme zu lösen. Im ersten Beispiel möchten wir die Lese-IOPS als Prozentsatz der Gesamt-IOPS für alle Speicherressourcen Ihres Mandanten anzeigen. Das zweite Beispiel bietet Einblick in die „System“- oder „Overhead“-IOPS, die auf Ihrem Mandanten auftreten – jene IOPS, die nicht direkt durch das Lesen oder Schreiben von Daten entstehen.

Sie können Variablen in Ausdrücken verwenden (z. B. *$Var1 * 100*).

Ausdrucksbeispiel: IOPS-Prozentsatz lesen

In diesem Beispiel möchten wir die Lese-IOPS als Prozentsatz der Gesamt-IOPS anzeigen. Sie können sich dies als folgende Formel vorstellen:

```
 Read Percentage = (Read IOPS / Total IOPS) x 100
Diese Daten können in einem Liniendiagramm auf Ihrem Dashboard angezeigt
werden.  Gehen Sie hierzu folgendermaßen vor:
```

Schritte

1. Erstellen Sie ein neues Dashboard oder öffnen Sie ein vorhandenes Dashboard im Bearbeitungsmodus.
2. Fügen Sie dem Dashboard ein Widget hinzu. Wählen Sie **Flächendiagramm**.

   Das Widget wird im Bearbeitungsmodus geöffnet. Standardmäßig wird eine Abfrage angezeigt, die *IOPS – Gesamt* für *Speicher*-Assets anzeigt. Wählen Sie bei Bedarf einen anderen Asset-Typ aus.

3. Klicken Sie rechts auf den Link **In Ausdruck konvertieren**.

   Die aktuelle Abfrage wird in den Ausdrucksmodus konvertiert. Beachten Sie, dass Sie den Asset-Typ im Ausdrucksmodus nicht ändern können. Während Sie sich im Ausdrucksmodus befinden, ändert sich der Link in **Zurück zur Abfrage**. Klicken Sie hierauf, wenn Sie jederzeit wieder in den Abfragemodus wechseln möchten. Beachten Sie, dass beim Wechseln zwischen den Modi die Felder auf ihre Standardwerte zurückgesetzt werden.

   Bleiben Sie vorerst im Ausdrucksmodus.

4. Die Metrik **IOPS – Gesamt** befindet sich jetzt im alphabetischen Variablenfeld „**a**“. Klicken Sie im Variablenfeld „**b**“ auf **Auswählen** und wählen Sie **IOPS – Lesen**.

   Sie können Ihrem Ausdruck bis zu fünf alphabetische Variablen hinzufügen, indem Sie auf die Schaltfläche + hinter den Variablenfeldern klicken. Für unser Beispiel mit dem Leseprozentsatz benötigen wir nur die Gesamt-IOPS („**a**“) und die Lese-IOPS („**b**“).

5. Im Feld **Ausdruck** verwenden Sie die Buchstaben, die den einzelnen Variablen entsprechen, um Ihren Ausdruck zu erstellen. Wir wissen, dass der Leseprozentsatz = (Lese-IOPS / Gesamt-IOPS) x 100 ist, daher würden wir diesen Ausdruck wie folgt schreiben:

   ```
    (b / a) * 100
   . Das Feld *Label* identifiziert den Ausdruck.  Ändern Sie die
   Beschriftung in „Leseprozentsatz“ oder etwas für Sie ähnlich Sinnvolles.
   . Ändern Sie das Feld *Einheiten* in „%“ oder „Prozent“.
   ```

   Das Diagramm zeigt den IOPS-Leseprozentsatz im Zeitverlauf für die ausgewählten Speichergeräte an. Bei Bedarf können Sie einen Filter setzen oder eine andere Rollup-Methode wählen. Beachten Sie, dass bei Auswahl von „Summe“ als Rollup-Methode alle Prozentwerte addiert werden, was möglicherweise über 100 % liegen kann.

6. Klicken Sie auf **Speichern**, um das Diagramm in Ihrem Dashboard zu speichern.

Ausdrucksbeispiel: „System“-E/A

Beispiel 2: Zu den aus Datenquellen gesammelten Metriken gehören Lese-, Schreib- und Gesamt-IOPS. Allerdings umfasst die Gesamtzahl der von einer Datenquelle gemeldeten IOPS manchmal auch „System“-IOPS, also E/A-Vorgänge, die nicht direkt zum Lesen oder Schreiben von Daten gehören. Diese System-E/A kann auch als „Overhead“-E/A betrachtet werden, die für den ordnungsgemäßen Systembetrieb erforderlich ist, aber nicht direkt mit Datenoperationen zusammenhängt.

Um diese System-E/As anzuzeigen, können Sie die Lese- und Schreib-IOPS von den gesamten IOPS abziehen, die bei der Erfassung gemeldet wurden. Die Formel könnte folgendermaßen aussehen:

```
 System IOPS = Total IOPS - (Read IOPS + Write IOPS)
Diese Daten können dann in einem Liniendiagramm auf Ihrem Dashboard
angezeigt werden.  Gehen Sie hierzu folgendermaßen vor:
```

Schritte

1. Erstellen Sie ein neues Dashboard oder öffnen Sie ein vorhandenes Dashboard im Bearbeitungsmodus.
2. Fügen Sie dem Dashboard ein Widget hinzu. Wählen Sie **Liniendiagramm**.

   Das Widget wird im Bearbeitungsmodus geöffnet. Standardmäßig wird eine Abfrage angezeigt, die *IOPS – Gesamt* für *Speicher*-Assets anzeigt. Wählen Sie bei Bedarf einen anderen Asset-Typ aus.

3. Wählen Sie im Feld **Roll Up** die Option *Sum* by *All*.

   Das Diagramm zeigt eine Linie mit der Summe aller IOPS.

4. Klicken Sie auf das Symbol „Diese Abfrage duplizieren“, um eine Kopie der Abfrage zu erstellen.

Unter dem Original wird ein Duplikat der Abfrage hinzugefügt.

5. Klicken Sie in der zweiten Abfrage auf die Schaltfläche **In Ausdruck konvertieren**.

   Die aktuelle Abfrage wird in den Ausdrucksmodus konvertiert. Klicken Sie auf **Zurück zur Abfrage**, wenn Sie jederzeit wieder in den Abfragemodus wechseln möchten. Beachten Sie, dass beim Wechseln zwischen den Modi die Felder auf ihre Standardwerte zurückgesetzt werden.

   Bleiben Sie vorerst im Ausdrucksmodus.

6. Die Metrik *IOPS – Gesamt* befindet sich jetzt im alphabetischen Variablenfeld „**a**“. Klicken Sie auf *IOPS – Gesamt* und ändern Sie es in *IOPS – Lesen*.
7. Klicken Sie im Variablenfeld „**b**“ auf **Auswählen** und wählen Sie *IOPS – Schreiben*.
8. Im Feld **Ausdruck** verwenden Sie die Buchstaben, die den einzelnen Variablen entsprechen, um Ihren Ausdruck zu erstellen. Wir würden unseren Ausdruck einfach so schreiben:

   ```
   a + b
   ```

   Wählen Sie im Abschnitt „Anzeige“ für diesen Ausdruck **Flächendiagramm** aus.

9. Das Feld **Label** identifiziert den Ausdruck. Ändern Sie die Bezeichnung in „System-IOPS“ oder etwas für Sie ebenso Sinnvolles.

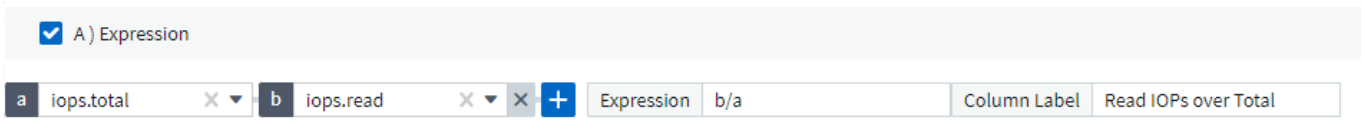
   Das Diagramm zeigt die gesamten IOPS als Liniendiagramm an, darunter ein Flächendiagramm, das die Kombination aus Lese- und Schreib-IOPS zeigt. Die Lücke zwischen den beiden zeigt die IOPS, die nicht direkt mit Datenlese- oder -schreibvorgängen zusammenhängen. Dies sind Ihre „System“-IOPS.

10. Klicken Sie auf **Speichern**, um das Diagramm in Ihrem Dashboard zu speichern.

Um eine Variable in einem Ausdruck zu verwenden, geben Sie einfach den Variablennamen ein, zum Beispiel *$var1 * 100*. In Ausdrücken können nur numerische Variablen verwendet werden.

Ausdrücke in einem Tabellen-Widget

Tabellen-Widgets behandeln Ausdrücke etwas anders. Sie können bis zu fünf Ausdrücke in einem einzelnen Tabellen-Widget haben, von denen jeder als neue Spalte zur Tabelle hinzugefügt wird. Jeder Ausdruck kann bis zu fünf Werte enthalten, auf deren Grundlage die Berechnung durchgeführt wird. Sie können der Spalte ganz einfach einen aussagekräftigen Namen geben.



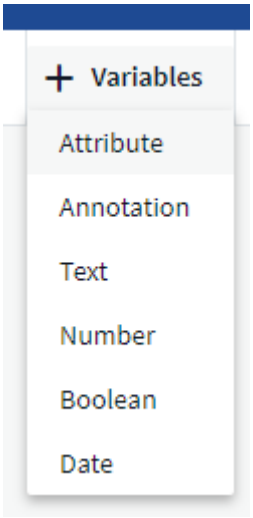
Variablen

Mithilfe von Variablen können Sie die in einigen oder allen Widgets auf einem Dashboard angezeigten Daten gleichzeitig ändern. Indem Sie ein oder mehrere Widgets so einstellen, dass sie eine gemeinsame Variable verwenden, führen an einer Stelle vorgenommene Änderungen dazu, dass die in jedem Widget angezeigten Daten automatisch aktualisiert werden.

Variablentypen

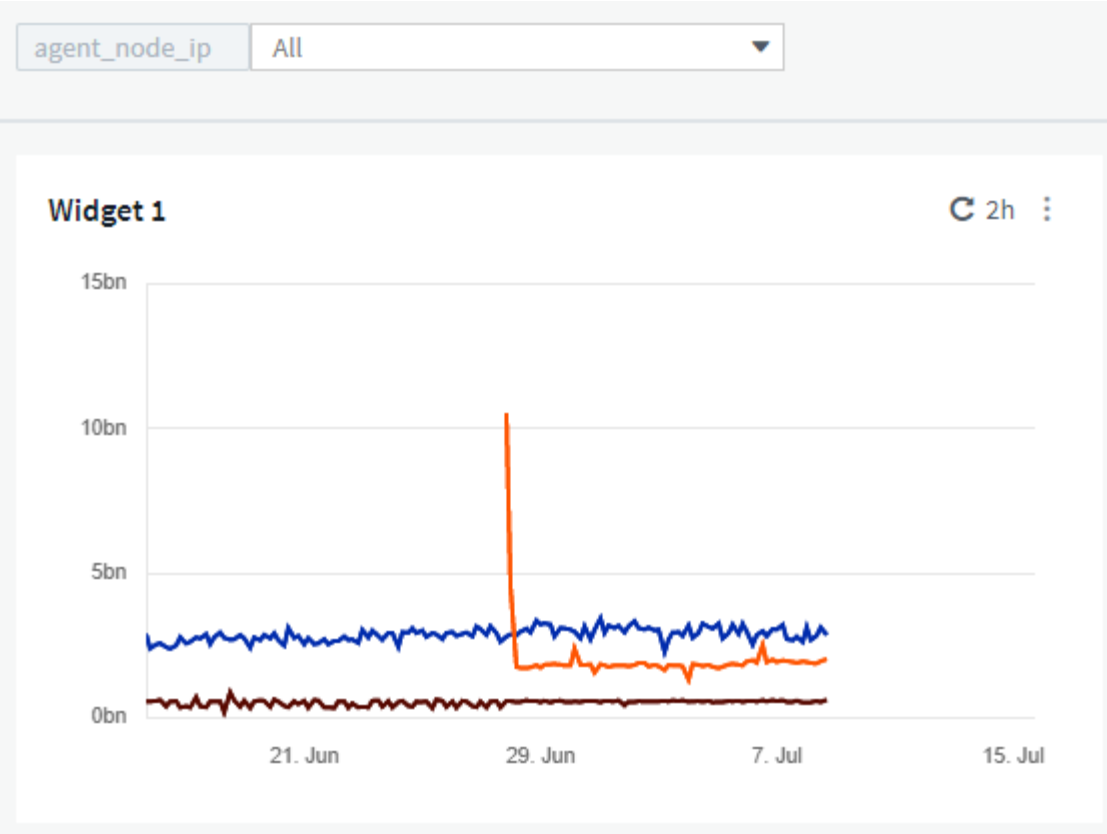
Eine Variable kann einen der folgenden Typen haben:

- **Attribut**: Verwenden Sie die Attribute oder Metriken eines Objekts zum Filtern
- **Anmerkung**: Verwenden Sie eine vordefinierte"Anmerkung" um Widget-Daten zu filtern.
- **Text**: Eine alphanumerische Zeichenfolge.
- **Numerisch**: Ein Zahlenwert. Verwenden Sie es allein oder als „Von“- oder „Bis“-Wert, abhängig von Ihrem Widget-Feld.
- **Boolesch**: Für Felder mit den Werten „Wahr/Falsch“, „Ja/Nein“ usw. verwenden. Für die boolesche Variable stehen die Auswahlmöglichkeiten „Ja“, „Nein“, „Keine“ und „Beliebig“ zur Verfügung.
- **Datum**: Ein Datumswert. Verwenden Sie es als „Von“- oder „Bis“-Wert, abhängig von der Konfiguration Ihres Widgets.

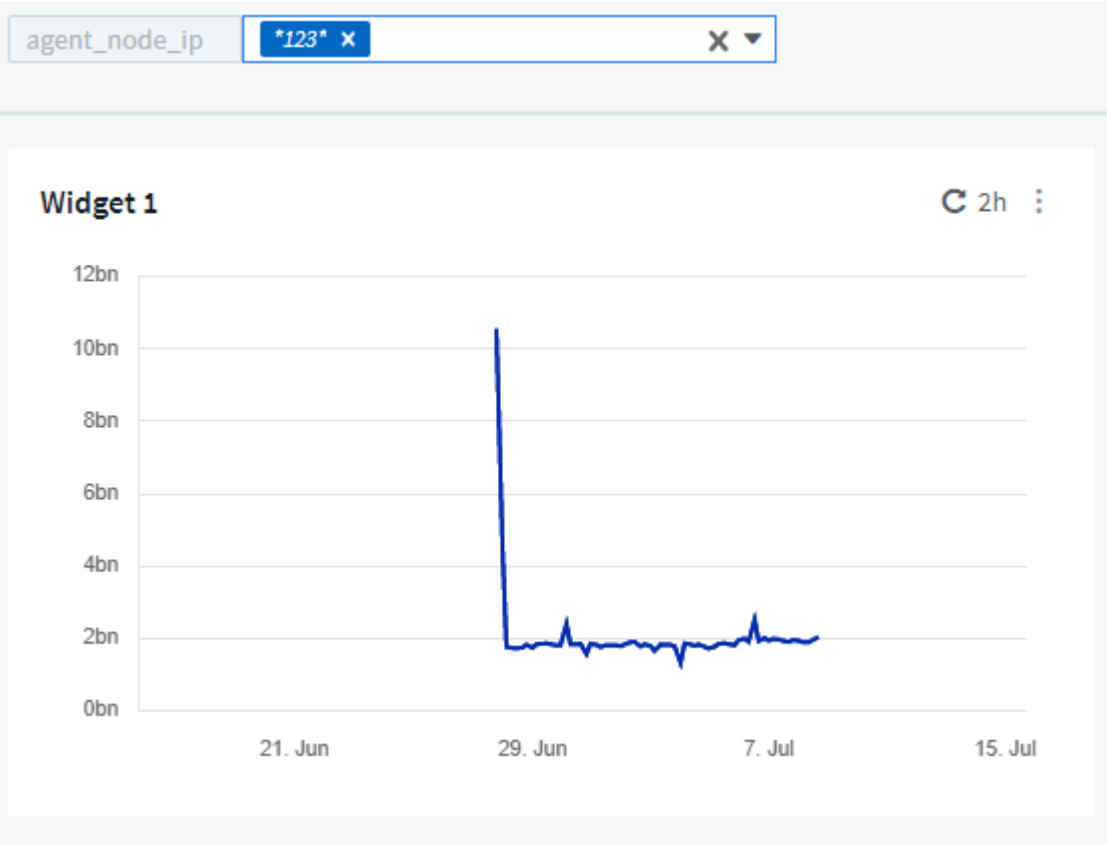


Attributvariablen

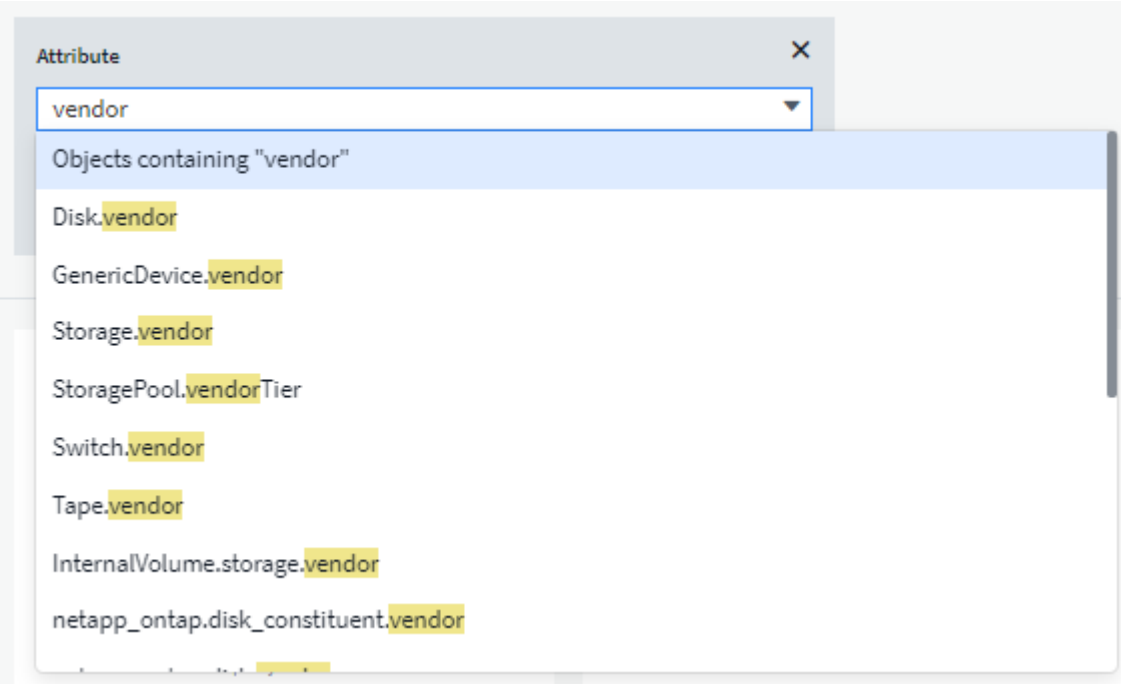
Durch Auswahl einer Attributtypvariable können Sie nach Widgetdaten filtern, die den oder die angegebenen Attributwerte enthalten. Das folgende Beispiel zeigt ein Linien-Widget, das Trends zum freien Speicher für Agent-Knoten anzeigt. Wir haben eine Variable für Agent-Knoten-IPs erstellt, die derzeit so eingestellt ist, dass alle IPs angezeigt werden:



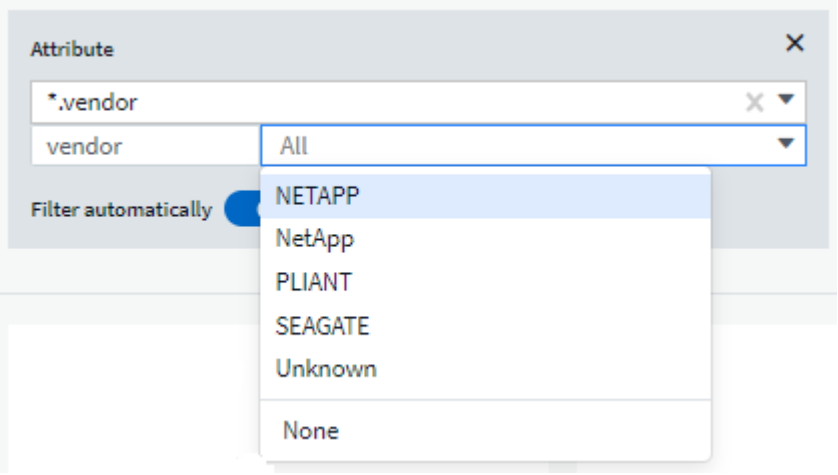
Wenn Sie jedoch vorübergehend nur Knoten in einzelnen Subnetzen Ihres Mandanten sehen möchten, können Sie die Variable auf eine oder mehrere bestimmte Agent-Knoten-IPs festlegen oder ändern. Hier sehen wir nur die Knoten im Subnetz „123“:



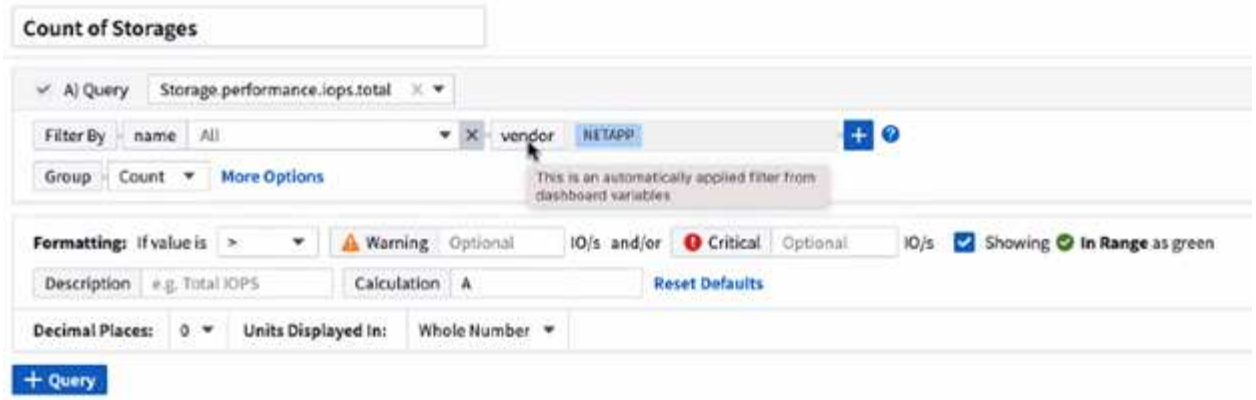
Sie können auch eine Variable festlegen, um nach *allen* Objekten mit einem bestimmten Attribut zu filtern, unabhängig vom Objekttyp, beispielsweise nach Objekten mit dem Attribut „Anbieter“, indem Sie **.Anbieter* im Variablenfeld angeben. Sie müssen das „*.“ nicht eingeben. Data Infrastructure Insights liefert dies, wenn Sie die Platzhalteroption auswählen.



Wenn Sie die Auswahlliste für den Variablenwert herunterklappen, werden die Ergebnisse gefiltert, sodass nur die verfügbaren Anbieter basierend auf den Objekten auf Ihrem Dashboard angezeigt werden.



Wenn Sie ein Widget auf Ihrem Dashboard bearbeiten, bei dem der Attributfilter relevant ist (d. h. die Objekte des Widgets enthalten ein **.vendor-Attribut*), wird Ihnen angezeigt, dass der Attributfilter automatisch angewendet wird.

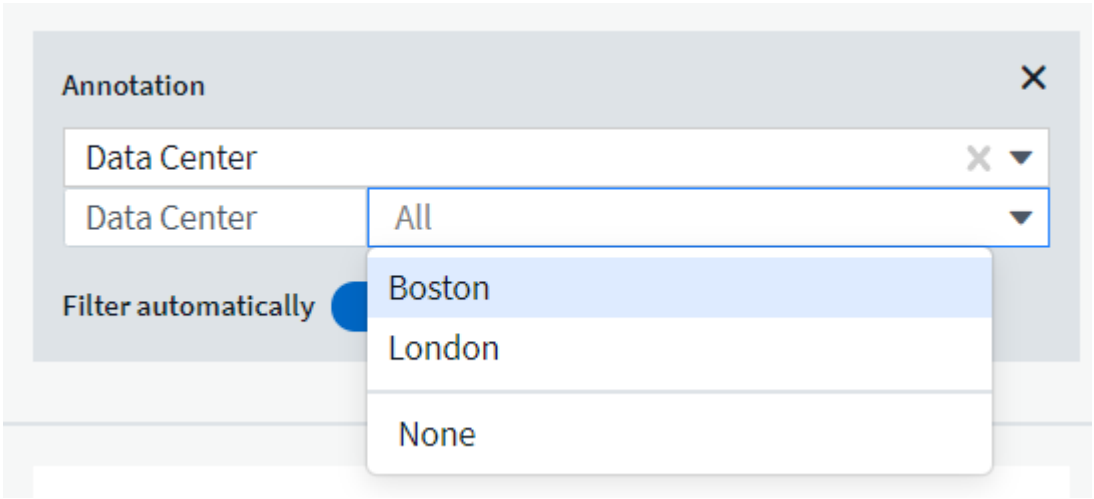


14

Das Anwenden von Variablen ist so einfach wie das Ändern der Attributdaten Ihrer Wahl.

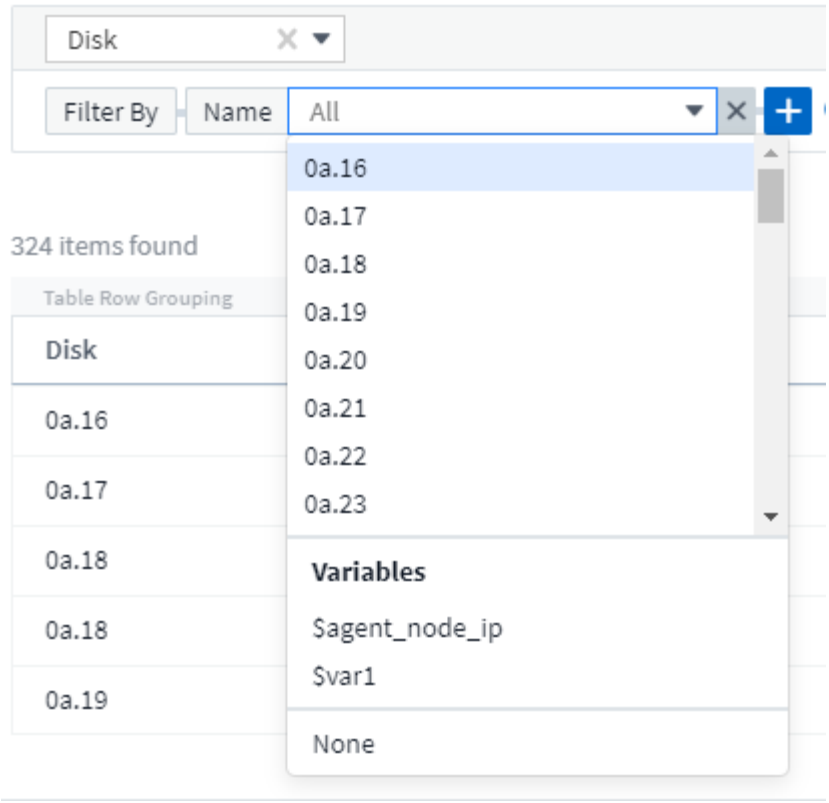
Annotationsvariablen

Durch Auswahl einer Annotation-Variable können Sie nach Objekten filtern, die mit dieser Annotation verknüpft sind, beispielsweise nach Objekten, die zum selben Rechenzentrum gehören.



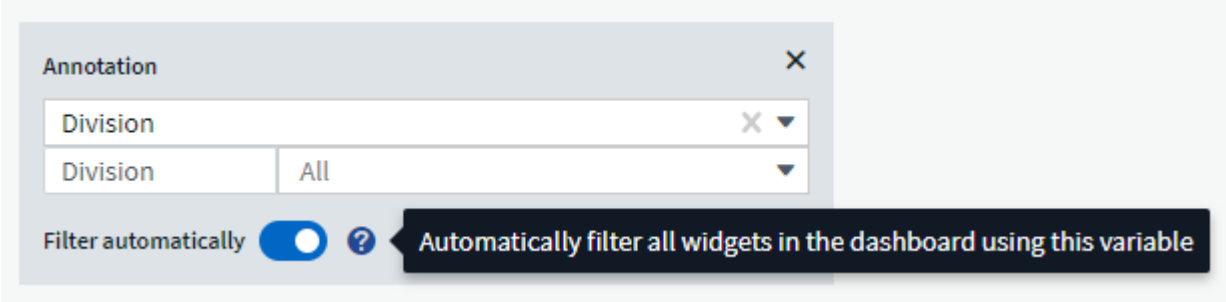
Text, Zahl, Datum oder Boolesche Variable

Sie können generische Variablen erstellen, die keinem bestimmten Attribut zugeordnet sind, indem Sie einen Variablentyp aus *Text*, *Zahl*, *Boolean* oder *Datum* auswählen. Sobald die Variable erstellt wurde, können Sie sie in einem Widget-Filterfeld auswählen. Wenn Sie in einem Widget einen Filter festlegen, werden neben bestimmten Werten, die Sie für den Filter auswählen können, alle für das Dashboard erstellten Variablen in der Liste angezeigt. Diese sind im Dropdown-Menü unter dem Abschnitt „Variablen“ gruppiert und haben Namen, die mit „$“ beginnen. Wenn Sie in diesem Filter eine Variable auswählen, können Sie nach Werten suchen, die Sie in das Variablenfeld auf dem Dashboard selbst eingeben. Alle Widgets, die diese Variable in einem Filter verwenden, werden dynamisch aktualisiert.



Variabler Filterbereich

Wenn Sie Ihrem Dashboard eine Anmerkungs- oder Attributvariable hinzufügen, kann die Variable auf *alle* Widgets im Dashboard angewendet werden. Dies bedeutet, dass alle Widgets auf Ihrem Dashboard Ergebnisse anzeigen, die nach dem von Ihnen in der Variable festgelegten Wert gefiltert sind.



Beachten Sie, dass nur Attribut- und Anmerkungsvariablen auf diese Weise automatisch gefiltert werden können. Nicht-Annotation- oder -Attributvariablen können nicht automatisch gefiltert werden. Einzelne Widgets müssen jeweils für die Verwendung von Variablen dieser Typen konfiguriert werden.

Um die automatische Filterung zu deaktivieren, sodass die Variable nur für die Widgets gilt, für die Sie sie ausdrücklich festgelegt haben, klicken Sie auf den Schieberegler „Automatisch filtern“, um sie zu deaktivieren.

Um eine Variable in einem einzelnen Widget festzulegen, öffnen Sie das Widget im Bearbeitungsmodus und wählen Sie die spezifische Anmerkung oder das Attribut im Feld *Filtern nach* aus. Mit einer Annotation-Variable können Sie einen oder mehrere bestimmte Werte auswählen oder den Variablennamen (gekennzeichnet durch das vorangestellte „$“) auswählen, um die Eingabe der Variable auf Dashboard-Ebene zu ermöglichen. Dasselbe gilt für Attributvariablen. Nur die Widgets, für die Sie die Variable festlegen, zeigen die gefilterten Ergebnisse an.

Das Filtern in Variablen ist *kontextbezogen*. Wenn Sie einen oder mehrere Filterwerte für eine Variable auswählen, werden in den anderen Variablen auf Ihrer Seite nur die für diesen Filter relevanten Werte angezeigt. Wenn Sie beispielsweise einen Variablenfilter auf ein bestimmtes Speichermodell einstellen, werden für alle Variablen, die auf den Filter für den Speichernamen eingestellt sind, nur die für dieses Modell relevanten Werte angezeigt.

Um eine Variable in einem Ausdruck zu verwenden, geben Sie einfach den Variablennamen als Teil des Ausdrucks ein, zum Beispiel *$var1 * 100*. In Ausdrücken können nur numerische Variablen verwendet werden. Sie können in Ausdrücken keine numerischen Anmerkungs- oder Attributvariablen verwenden.

Das Filtern in Variablen ist *kontextbezogen*. Wenn Sie einen oder mehrere Filterwerte für eine Variable auswählen, werden in den anderen Variablen auf Ihrer Seite nur die für diesen Filter relevanten Werte angezeigt. Wenn Sie beispielsweise einen Variablenfilter auf ein bestimmtes Speichermodell einstellen, werden für alle Variablen, die auf den Filter für den Speichernamen eingestellt sind, nur die für dieses Modell relevanten Werte angezeigt.

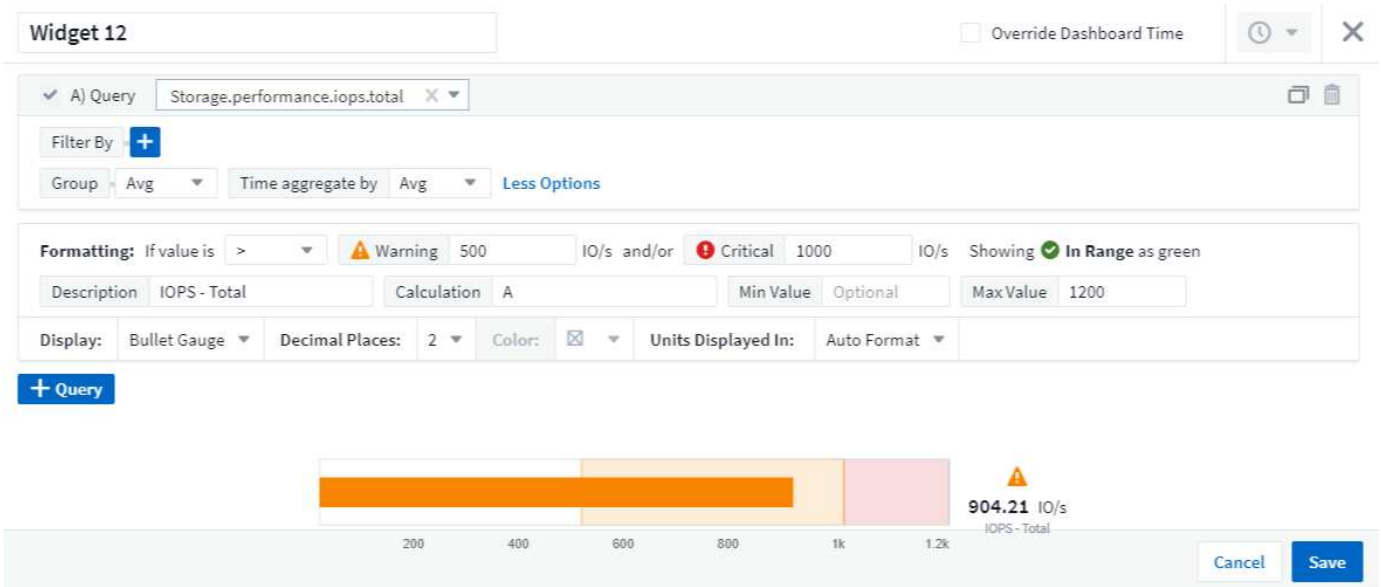
Variablenbenennung

Variablennamen:

- Darf nur die Buchstaben a-z, die Ziffern 0-9, Punkt (.), Unterstrich (_) und Leerzeichen ( ) enthalten.
- Darf nicht länger als 20 Zeichen sein.
- Unterscheiden zwischen Groß- und Kleinschreibung: $CityName und $cityname sind unterschiedliche Variablen.
- Darf nicht mit einem vorhandenen Variablennamen identisch sein.
- Darf nicht leer sein.

Formatieren von Messinstrument-Widgets

Mit den Widgets „Vollständige Anzeige“ und „Aufzählungszeichen“ können Sie Schwellenwerte für die Stufen „Warnung“ und/oder „Kritisch“ festlegen und so eine klare Darstellung der von Ihnen angegebenen Daten bereitstellen.



Um die Formatierung für diese Widgets festzulegen, führen Sie die folgenden Schritte aus:

1. Wählen Sie, ob Sie Werte hervorheben möchten, die größer (>) oder kleiner (<) als Ihre Schwellenwerte sind. In diesem Beispiel markieren wir Werte, die größer (>) als die Schwellenwerte sind.
2. Wählen Sie einen Wert für den Schwellenwert „Warnung“. Wenn das Widget Werte anzeigt, die über diesem Niveau liegen, wird die Anzeige in Orange angezeigt.
3. Wählen Sie einen Wert für den Schwellenwert „Kritisch“. Bei Werten über diesem Wert wird die Anzeige rot angezeigt.

Optional können Sie einen Minimal- und Maximalwert für die Anzeige wählen. Bei Werten unter dem Minimum wird die Anzeige nicht angezeigt. Bei Werten über dem Maximum wird eine volle Anzeige angezeigt. Wenn Sie keine Mindest- oder Höchstwerte auswählen, wählt das Widget basierend auf dem Wert des Widgets die optimalen Mindest- und Höchstwerte aus.

Formatieren des Einzelwert-Widgets

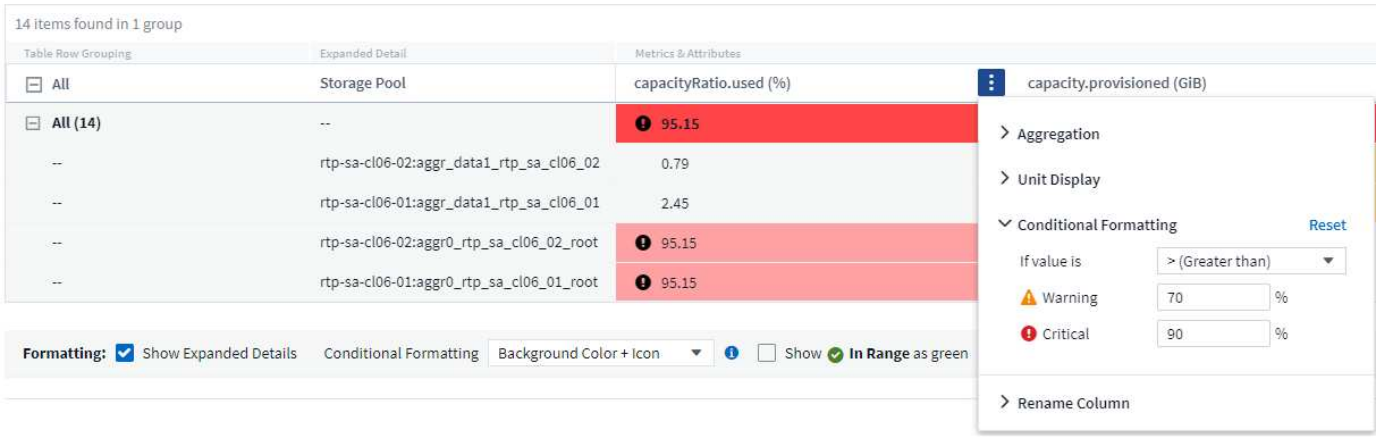
Im Einzelwert-Widget können Sie zusätzlich zur Einstellung der Warnschwellen (orange) und der kritischen Schwelle (rot) wählen, ob Werte „im Bereich“ (unter der Warnstufe) mit grünem oder weißem Hintergrund angezeigt werden sollen.

Wenn Sie in einem Einzelwert-Widget oder einem Messinstrument-Widget auf den Link klicken, wird eine Abfrageseite angezeigt, die der ersten Abfrage im Widget entspricht.

Tabellen-Widgets formatieren

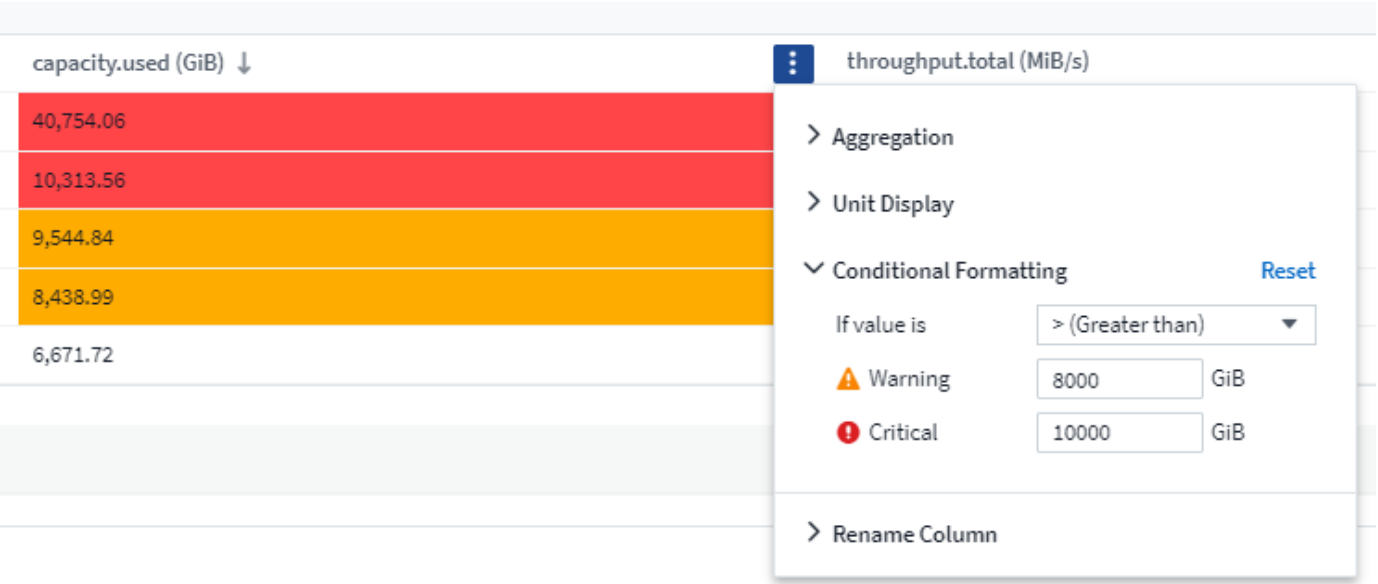
Wie bei Einzelwert- und Mess-Widgets können Sie in Tabellen-Widgets eine bedingte Formatierung festlegen, sodass Sie Daten mit Farben und/oder speziellen Symbolen hervorheben können.

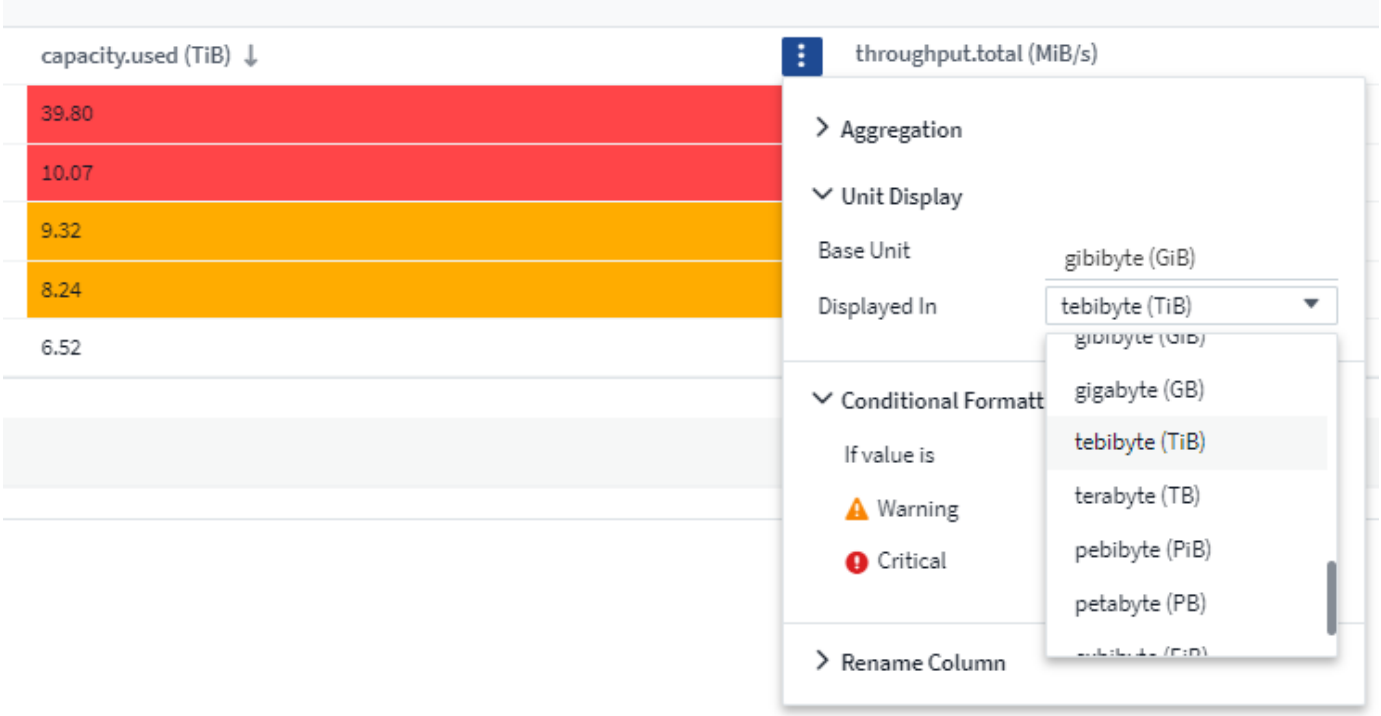
Mit der bedingten Formatierung können Sie Schwellenwerte für Warn- und kritische Werte in Tabellen-Widgets festlegen und hervorheben, sodass Ausreißer und außergewöhnliche Datenpunkte sofort sichtbar werden.



Die bedingte Formatierung wird für jede Spalte einer Tabelle separat festgelegt. Sie können beispielsweise einen Schwellenwertsatz für eine Kapazitätsspalte und einen anderen Satz für eine Durchsatzspalte auswählen.

Wenn Sie die Einheitenanzeige für eine Spalte ändern, bleibt die bedingte Formatierung erhalten und spiegelt die Werteänderung wider. Die folgenden Bilder zeigen dieselbe bedingte Formatierung, obwohl die Anzeigeeinheit unterschiedlich ist.



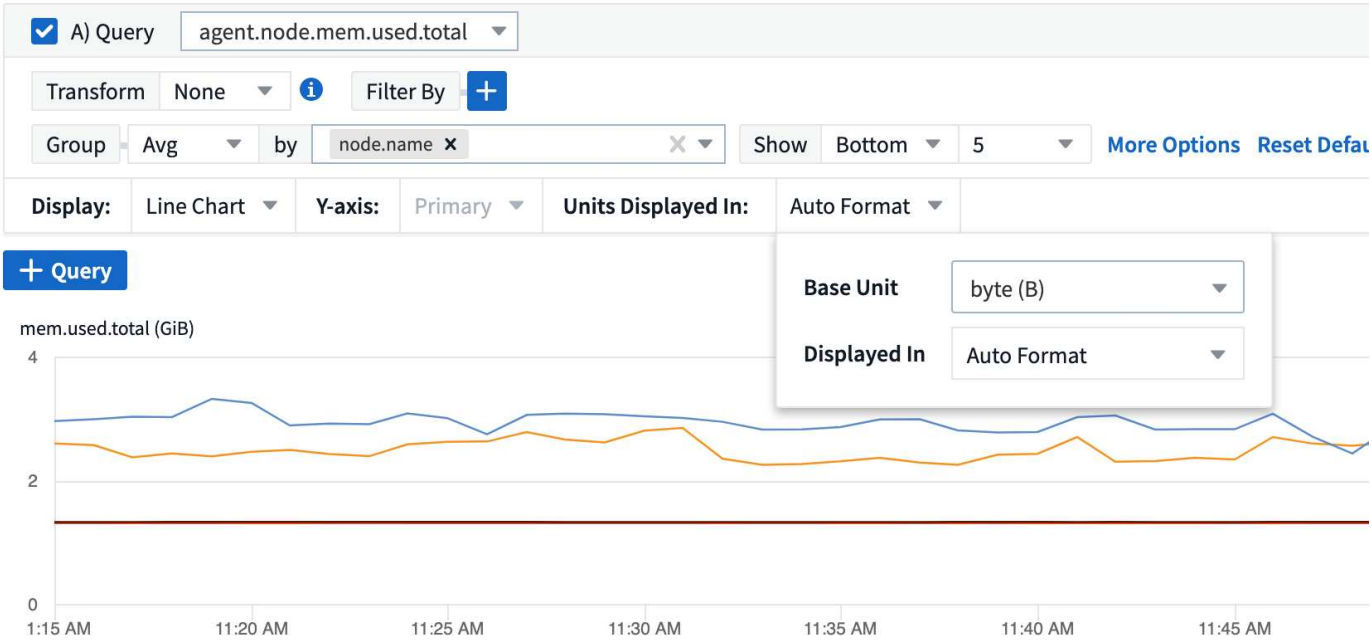


Sie können wählen, ob die Bedingungsformatierung als Farbe, Symbole oder beides angezeigt werden soll.

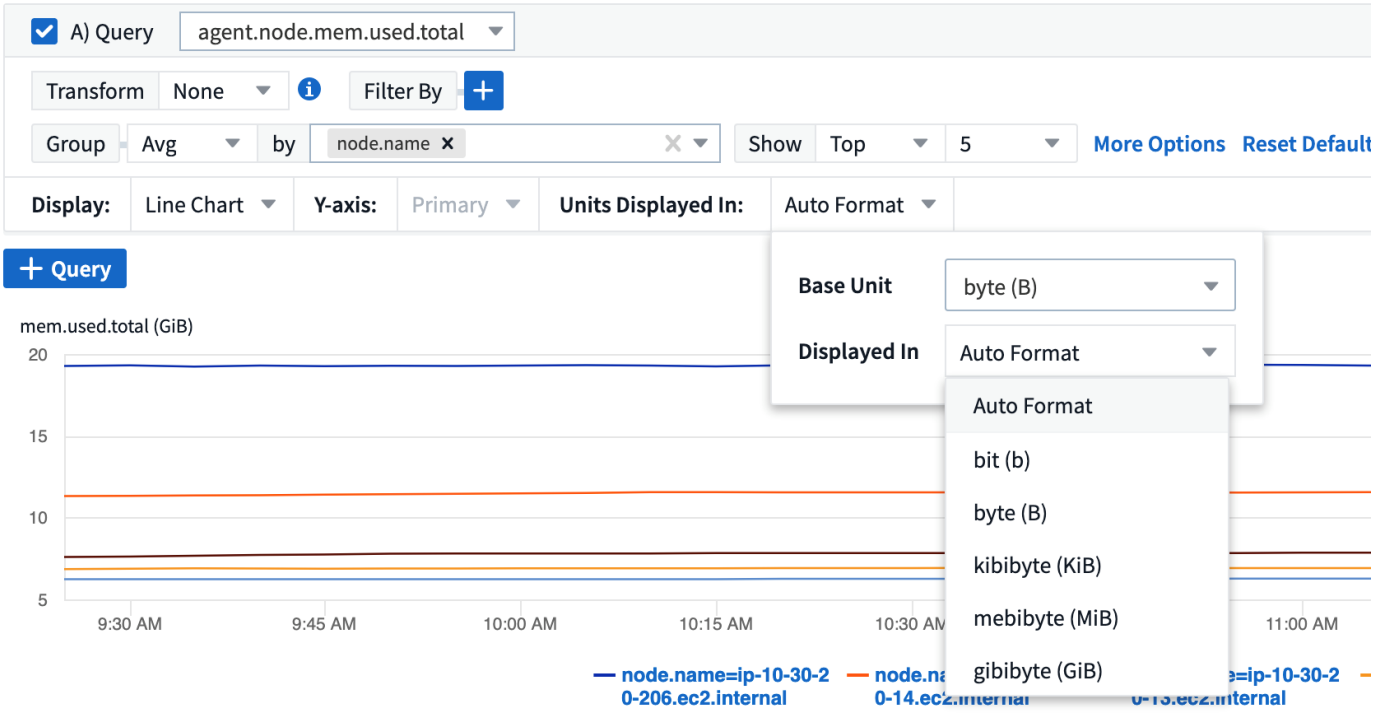
Auswählen der Einheit zur Datenanzeige

Bei den meisten Widgets auf einem Dashboard können Sie die Einheiten angeben, in denen Werte angezeigt werden sollen, beispielsweise *Megabyte*, *Tausende*, *Prozent*, *Millisekunden (ms)* usw. In vielen Fällen kennt Data Infrastructure Insights das beste Format für die erfassten Daten. In Fällen, in denen das beste Format nicht bekannt ist, können Sie das gewünschte Format festlegen.

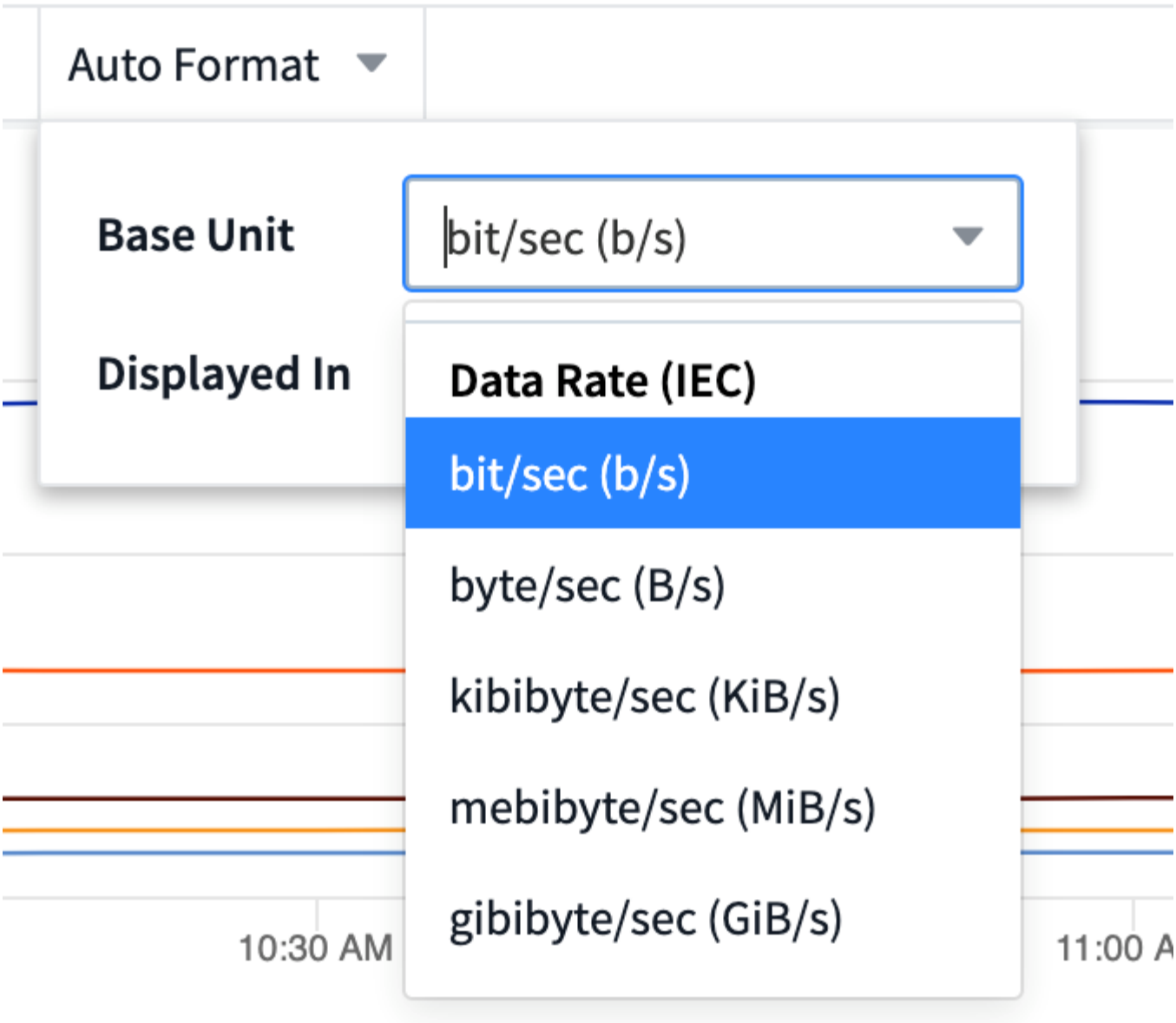
Im folgenden Liniendiagrammbeispiel liegen die für das Widget ausgewählten Daten bekanntermaßen in *Bytes* vor (die grundlegende IEC-Dateneinheit: siehe Tabelle unten), daher wird die Basiseinheit automatisch als „Byte (B)“ ausgewählt. Die Datenwerte sind jedoch groß genug, um als Gibibyte (GiB) dargestellt zu werden, sodass Data Infrastructure Insights die Werte standardmäßig automatisch als GiB formatiert. Die Y-Achse im Diagramm zeigt „GiB“ als Anzeigeeinheit und alle Werte werden in dieser Einheit angezeigt.



Wenn Sie das Diagramm in einer anderen Einheit anzeigen möchten, können Sie ein anderes Format für die Anzeige der Werte auswählen. Da die Basiseinheit in diesem Beispiel *Byte* ist, können Sie aus den unterstützten „bytebasierten“ Formaten wählen: Bit (b), Byte (B), Kibibyte (KiB), Mebibyte (MiB), Gibibyte (GiB). Die Beschriftung und die Werte der Y-Achse ändern sich je nach dem von Ihnen gewählten Format.



In Fällen, in denen die Basiseinheit nicht bekannt ist, können Sie eine Einheit aus den folgenden"verfügbare Einheiten" , oder geben Sie Ihren eigenen ein. Nachdem Sie eine Basiseinheit zugewiesen haben, können Sie die Daten in einem der entsprechenden unterstützten Formate anzeigen.



Um Ihre Einstellungen zu löschen und neu zu beginnen, klicken Sie auf **Auf Standard zurücksetzen**.

Ein Wort zur automatischen Formatierung

Die meisten Messwerte werden von Datensammlern in der kleinsten Einheit gemeldet, beispielsweise als ganze Zahl wie 1.234.567.890 Bytes. Standardmäßig formatiert Data Infrastructure Insights den Wert automatisch für die am besten lesbare Anzeige. Beispielsweise würde ein Datenwert von 1.234.567.890 Bytes automatisch auf 1,23 *Gibibytes* formatiert. Sie können es auch in einem anderen Format anzeigen, beispielsweise *Mebibyte*. Der Wert wird entsprechend angezeigt.

Data Infrastructure Insights verwendet amerikanische englische Nummernbenennungsstandards. Die amerikanische „Milliarde“ entspricht „Tausend Millionen“.

Widgets mit mehreren Abfragen

Wenn Sie ein Zeitreihen-Widget (z. B. Linie, Spline, Fläche, gestapelte Fläche) mit zwei Abfragen haben, die beide auf der primären Y-Achse dargestellt werden, wird die Basiseinheit oben auf der Y-Achse nicht angezeigt. Wenn Ihr Widget jedoch eine Abfrage auf der primären Y-Achse und eine Abfrage auf der

sekundären Y-Achse hat, werden die Basiseinheiten für jede angezeigt.

Wenn Ihr Widget drei oder mehr Abfragen hat, werden auf der Y-Achse keine Basiseinheiten angezeigt.

Verfügbare Einheiten

Die folgende Tabelle zeigt alle verfügbaren Einheiten nach Kategorie.

Kategorie	Einheiten
Währung	Cent-Dollar
Daten (IEC)	Bit Byte Kibibyte Mebibyte Gibibyte Tebibyte Pebibyte Exbibyte
Datenrate (IEC)	Bit/Sek. Byte/Sek. Kibibyte/Sek. Mebibyte/Sek. Gibibyte/Sek. Tebibyte/Sek. Pebibyte/Sek.
Daten (metrisch)	Kilobyte Megabyte Gigabyte Terabyte Petabyte Exabyte
Datenrate (metrisch)	Kilobyte/Sek. Megabyte/Sek. Gigabyte/Sek. Terabyte/Sek. Petabyte/Sek. Exabyte/Sek.
IEC	kibi mebi gibi tebi pebi exbi
Dezimal	ganze Zahl Tausend Millionen Milliarden Billionen
Prozentsatz	Prozentsatz
Zeit	Nanosekunde Mikrosekunde Millisekunde Sekunde Minute Stunde
Temperatur	Celsius Fahrenheit
Frequenz	Hertz Kilohertz Megahertz Gigahertz
CPU	Nanokerne, Mikrokerne, Millikerne, Kerne, Kilokerne, Megakerne, Gigakerne, Terakerne, Petakerne, Exakerne
Durchsatz	E/A-Operationen/Sek. Operationen/Sek. Anfragen/Sek. Lesevorgänge/Sek. Schreibvorgänge/Sek. Operationen/Min. Lesevorgänge/Min. Schreibvorgänge/Min.

TV-Modus und automatische Aktualisierung

Daten in Widgets auf Dashboards und Asset-Landingpages werden automatisch gemäß einem Aktualisierungsintervall aktualisiert, das durch den ausgewählten Dashboard-Zeitbereich bestimmt wird. Das

Aktualisierungsintervall hängt davon ab, ob es sich bei dem Widget um ein Zeitreihen- (Linien-, Spline-, Flächen-, gestapeltes Flächendiagramm) oder Nicht-Zeitreihen- (alle anderen Diagramme) Widget handelt.

Dashboard-Zeitbereich	Aktualisierungsintervall für Zeitreihen	Nicht-Zeitreihen-Aktualisierungsintervall
Letzte 15 Minuten	10 Sekunden	1 Minute
Letzte 30 Minuten	15 Sekunden	1 Minute
Letzte 60 Minuten	15 Sekunden	1 Minute
Letzte 2 Stunden	30 Sekunden	5 Minuten
Letzte 3 Stunden	30 Sekunden	5 Minuten
Letzte 6 Stunden	1 Minute	5 Minuten
Letzte 12 Stunden	5 Minuten	10 Minuten
Letzte 24 Stunden	5 Minuten	10 Minuten
Letzte 2 Tage	10 Minuten	10 Minuten
Letzte 3 Tage	15 Minuten	15 Minuten
Letzte 7 Tage	1 Stunde	1 Stunde
Letzte 30 Tage	2 Stunden	2 Stunden

Jedes Widget zeigt sein automatisches Aktualisierungsintervall in der oberen rechten Ecke des Widgets an.

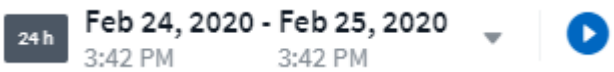
Die automatische Aktualisierung ist für den benutzerdefinierten Dashboard-Zeitbereich nicht verfügbar.

In Kombination mit dem **TV-Modus** ermöglicht die automatische Aktualisierung die Anzeige von Daten auf einem Dashboard oder einer Asset-Seite nahezu in Echtzeit. Der TV-Modus bietet eine übersichtliche Anzeige; das Navigationsmenü ist ausgeblendet, wodurch mehr Platz auf dem Bildschirm für die Anzeige Ihrer Daten zur Verfügung steht, ebenso wie die Schaltfläche „Bearbeiten“. Der TV-Modus ignoriert typische Timeouts von Data Infrastructure Insights und lässt die Anzeige aktiv, bis Sie manuell oder automatisch durch Autorisierungssicherheitsprotokolle abgemeldet werden.

Da die NetApp Console über ein eigenes Zeitlimit für die Benutzeranmeldung von 7 Tagen verfügt, muss sich Data Infrastructure Insights bei diesem Ereignis ebenfalls abmelden. Sie können sich einfach erneut anmelden und Ihr Dashboard wird weiterhin angezeigt.

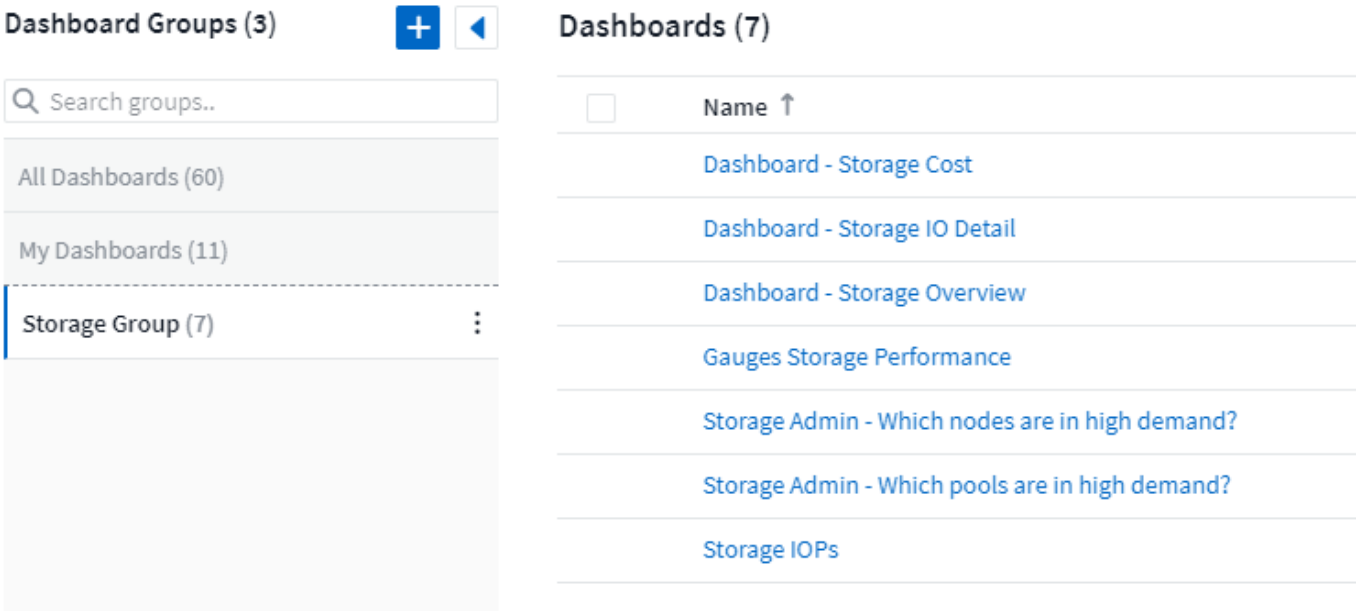
- Um den TV-Modus zu aktivieren, klicken Sie auf die Schaltfläche „TV-Modus“.
- Um den TV-Modus zu deaktivieren, klicken Sie oben links auf dem Bildschirm auf die Schaltfläche **Beenden**.

Sie können die automatische Aktualisierung vorübergehend unterbrechen, indem Sie auf die Schaltfläche „Pause“ in der oberen rechten Ecke klicken. Während der Pause zeigt das Zeitbereichsfeld des Dashboards den aktiven Zeitbereich der angehaltenen Daten an. Ihre Daten werden weiterhin erfasst und aktualisiert, während die automatische Aktualisierung angehalten ist. Klicken Sie auf die Schaltfläche „Fortsetzen“, um die automatische Aktualisierung der Daten fortzusetzen.



Dashboard-Gruppen

Durch Gruppieren können Sie zugehörige Dashboards anzeigen und verwalten. Sie können beispielsweise eine Dashboard-Gruppe einrichten, die ausschließlich dem Speicher Ihres Mandanten gewidmet ist. Dashboard-Gruppen werden auf der Seite **Dashboards > Alle Dashboards anzeigen** verwaltet.



Standardmäßig werden zwei Gruppen angezeigt:

- **Alle Dashboards** listet alle erstellten Dashboards auf, unabhängig vom Besitzer.
- **Meine Dashboards** listet nur die vom aktuellen Benutzer erstellten Dashboards auf.

Die Anzahl der in jeder Gruppe enthaltenen Dashboards wird neben dem Gruppennamen angezeigt.

Um eine neue Gruppe zu erstellen, klicken Sie auf die Schaltfläche **"+" Neue Dashboard-Gruppe erstellen**. Geben Sie einen Namen für die Gruppe ein und klicken Sie auf **Gruppe erstellen**. Es wird eine leere Gruppe mit diesem Namen erstellt.

Um Dashboards zur Gruppe hinzuzufügen, klicken Sie auf die Gruppe „Alle Dashboards“, um alle Dashboards Ihres Mandanten anzuzeigen, oder klicken Sie auf „Meine Dashboards“, wenn Sie nur die Dashboards sehen möchten, die Ihnen gehören, und führen Sie einen der folgenden Schritte aus:

- Um ein einzelnes Dashboard hinzuzufügen, klicken Sie auf das Menü rechts neben dem Dashboard und wählen Sie *Zur Gruppe hinzufügen*.
- Um einer Gruppe mehrere Dashboards hinzuzufügen, wählen Sie sie aus, indem Sie das Kontrollkästchen neben jedem Dashboard aktivieren. Klicken Sie dann auf die Schaltfläche **Massenaktionen** und wählen Sie *Zur Gruppe hinzufügen*.

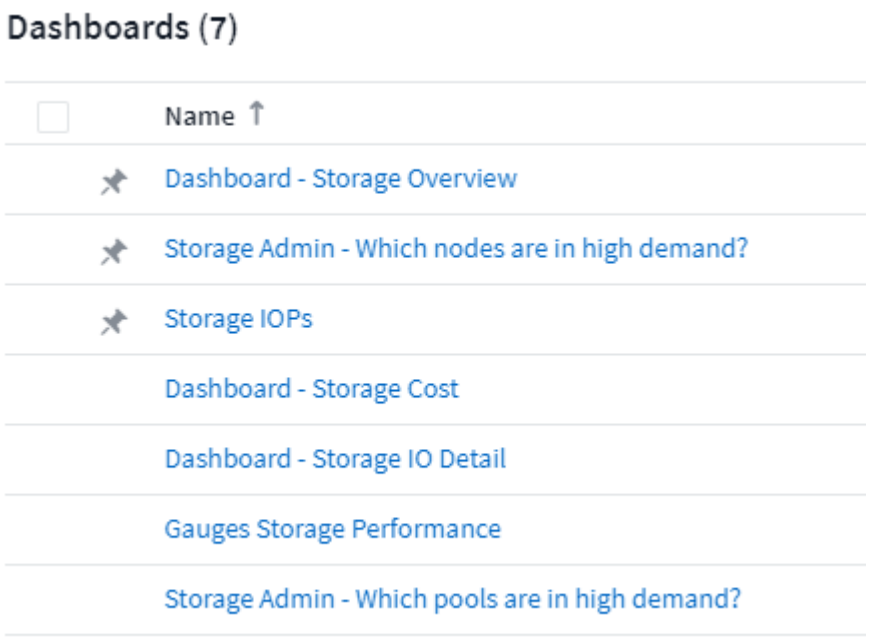
Entfernen Sie Dashboards auf die gleiche Weise aus der aktuellen Gruppe, indem Sie *Aus Gruppe entfernen* auswählen. Sie können keine Dashboards aus der Gruppe „Alle Dashboards“ oder „Meine Dashboards“ entfernen.

Durch das Entfernen eines Dashboards aus einer Gruppe wird das Dashboard nicht aus Data Infrastructure Insights gelöscht. Um ein Dashboard vollständig zu entfernen, wählen Sie das Dashboard aus und klicken Sie auf *Löschen*. Dadurch wird es aus allen Gruppen entfernt, zu denen es gehörte, und steht keinem Benutzer mehr zur Verfügung.

Pinn deine Lieblings-Dashboards an

Sie können Ihre Dashboards weiter verwalten, indem Sie Ihre Favoriten oben in Ihrer Dashboard-Liste anheften. Um ein Dashboard anzuheften, klicken Sie einfach auf die Reißzwecken-Schaltfläche, die angezeigt wird, wenn Sie mit der Maus über ein Dashboard in einer beliebigen Liste fahren.

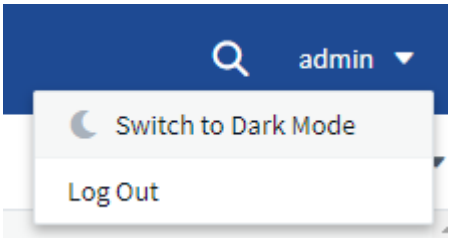
Das Anheften/Lösen des Dashboards ist eine individuelle Benutzereinstellung und unabhängig von der Gruppe (oder den Gruppen), zu der/denen das Dashboard gehört.



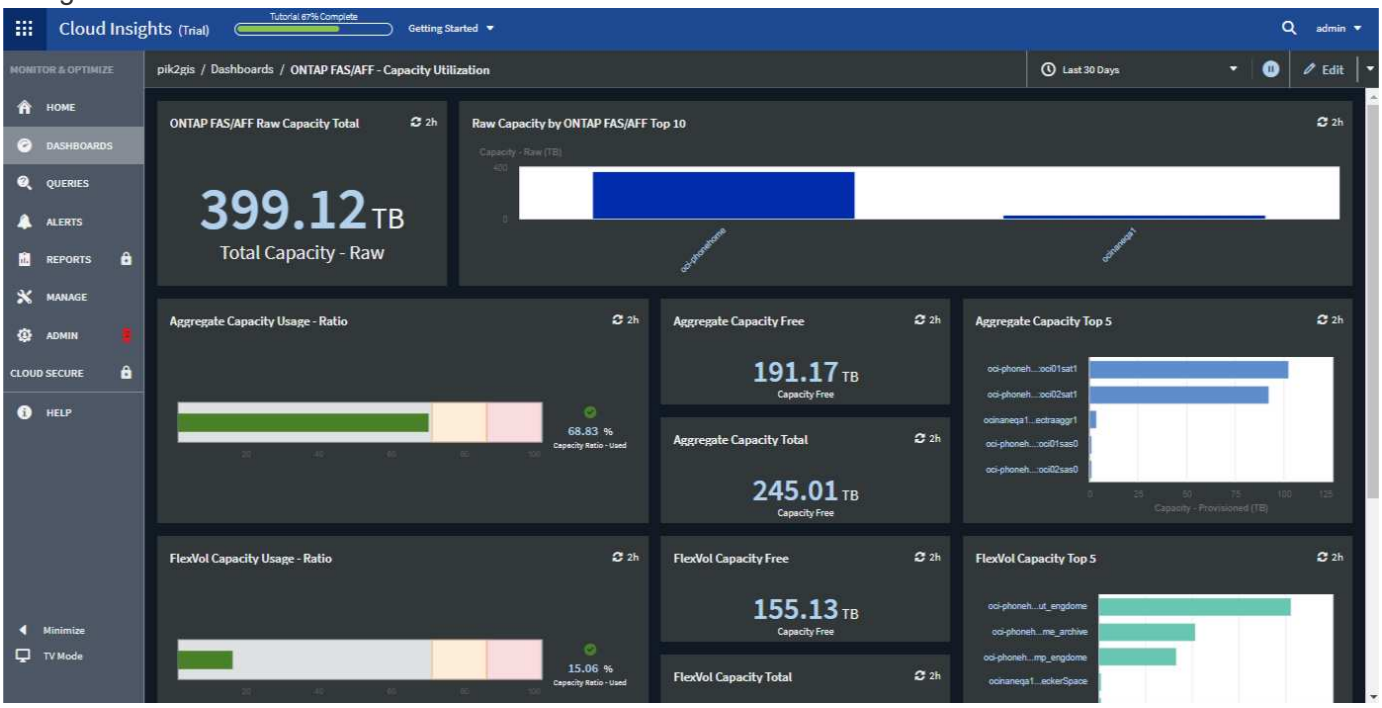
Dunkles Design

Sie können Data Infrastructure Insights entweder mit einem hellen Design (Standard) anzeigen, bei dem die meisten Bildschirme mit einem hellen Hintergrund und dunklem Text angezeigt werden, oder mit einem dunklen Design, bei dem die meisten Bildschirme mit einem dunklen Hintergrund und hellem Text angezeigt werden.

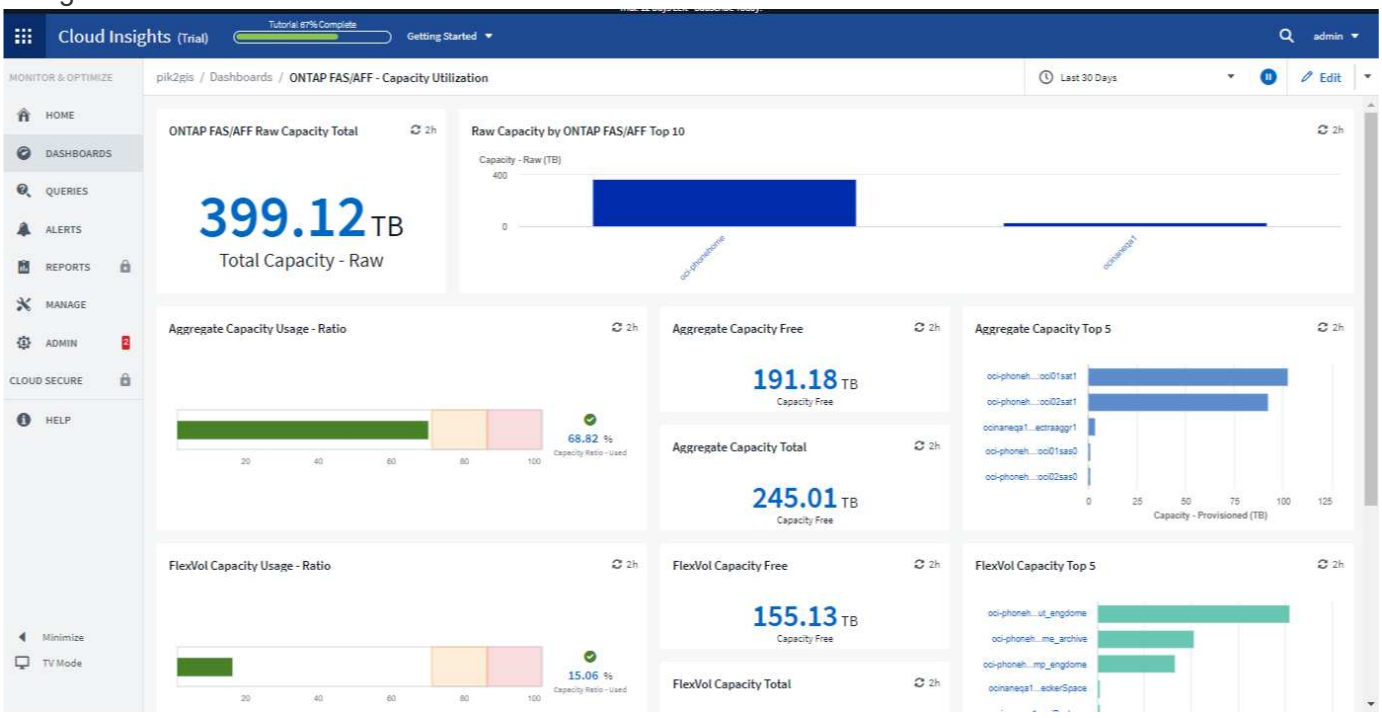
Um zwischen hellen und dunklen Designs zu wechseln, klicken Sie auf die Schaltfläche mit dem Benutzernamen in der oberen rechten Ecke des Bildschirms und wählen Sie das gewünschte Design aus.



Dashboard-Ansicht im dunklen Design:



Dashboard-Ansicht mit hellem Design:



Einige Bildschirmbereiche, wie etwa bestimmte Widget-Diagramme, zeigen auch bei Anzeige im dunklen Design noch immer helle Hintergründe.

Liniendiagramm-Interpolation

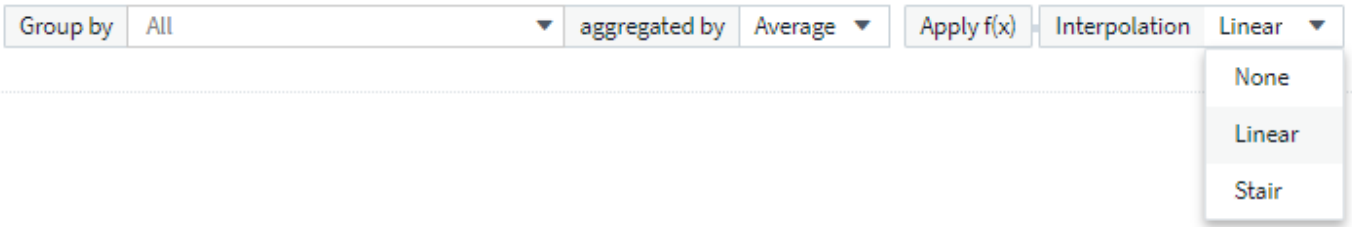
Verschiedene Datensammler fragen ihre Daten oft in unterschiedlichen Intervallen ab. Beispielsweise kann Datensammler A alle 15 Minuten eine Abfrage durchführen, während Datensammler B alle fünf Minuten eine

Abfrage durchführt. Wenn ein Liniendiagramm-Widget (auch Spline-, Flächen- und gestapelte Flächendiagramme) diese Daten aus mehreren Datensammlern in einer einzigen Linie aggregiert (z. B. wenn das Widget nach „alle“ gruppiert) und die Linie alle fünf Minuten aktualisiert, werden die Daten von Sammler B möglicherweise genau angezeigt, während die Daten von Sammler A Lücken aufweisen können, wodurch die Aggregation beeinträchtigt wird, bis Sammler A erneut abfragt.

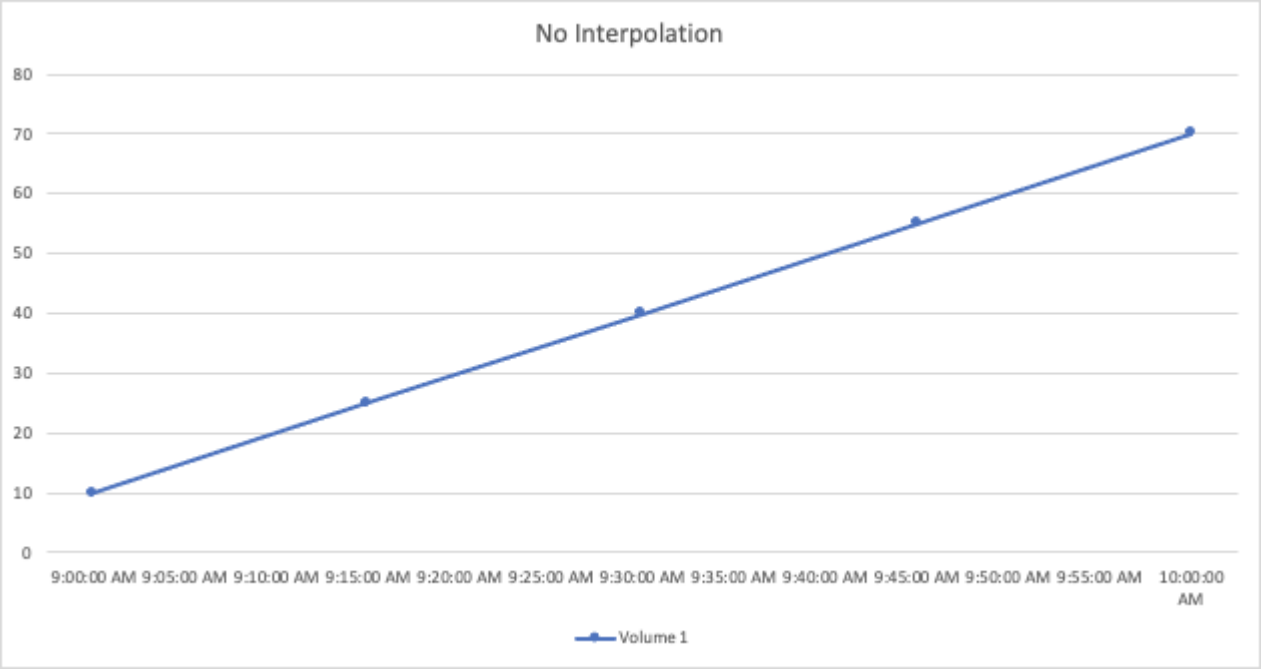
Um dies zu verhindern, interpoliert Data Infrastructure Insights die Daten beim Aggregieren und verwendet die umgebenden Datenpunkte, um eine bestmögliche Schätzung der Daten vorzunehmen, bis die Datensammler eine erneute Abfrage durchführen. Sie können die Objektdaten jedes Datensammlers jederzeit einzeln anzeigen, indem Sie die Gruppierung des Widgets anpassen.

Interpolationsmethoden

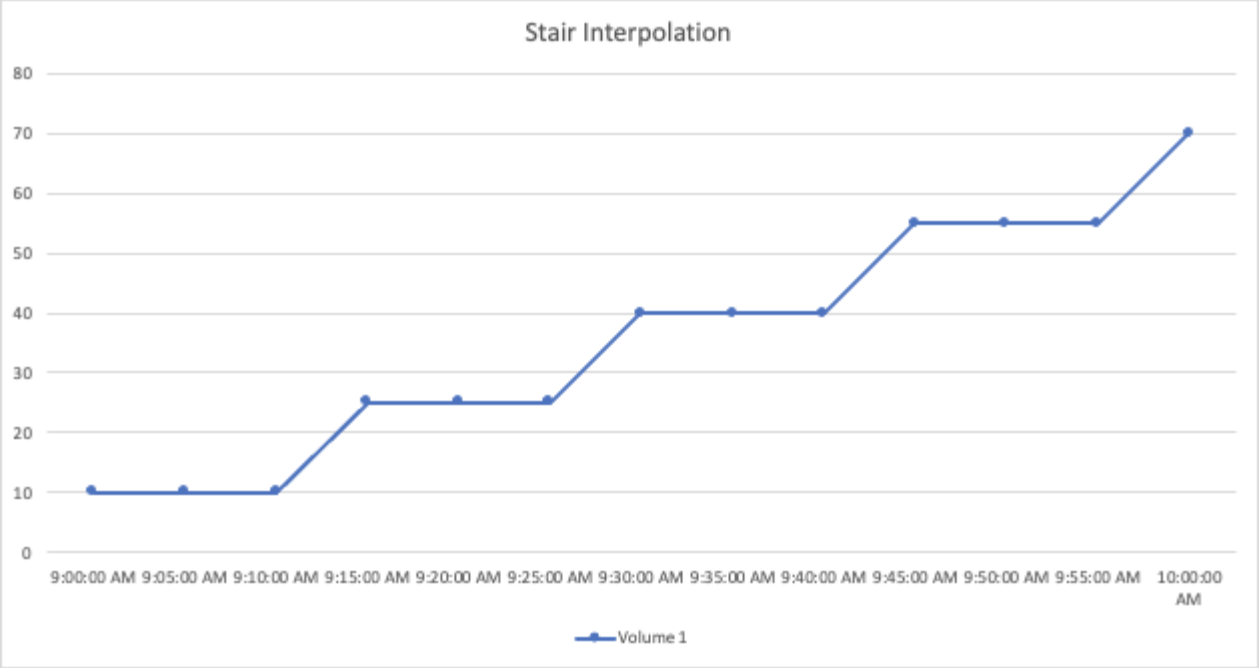
Beim Erstellen oder Ändern eines Liniendiagramms (oder Spline-, Flächen- oder gestapelten Flächendiagramms) können Sie die Interpolationsmethode auf einen von drei Typen einstellen. Wählen Sie im Abschnitt „Gruppieren nach“ die gewünschte Interpolation aus.



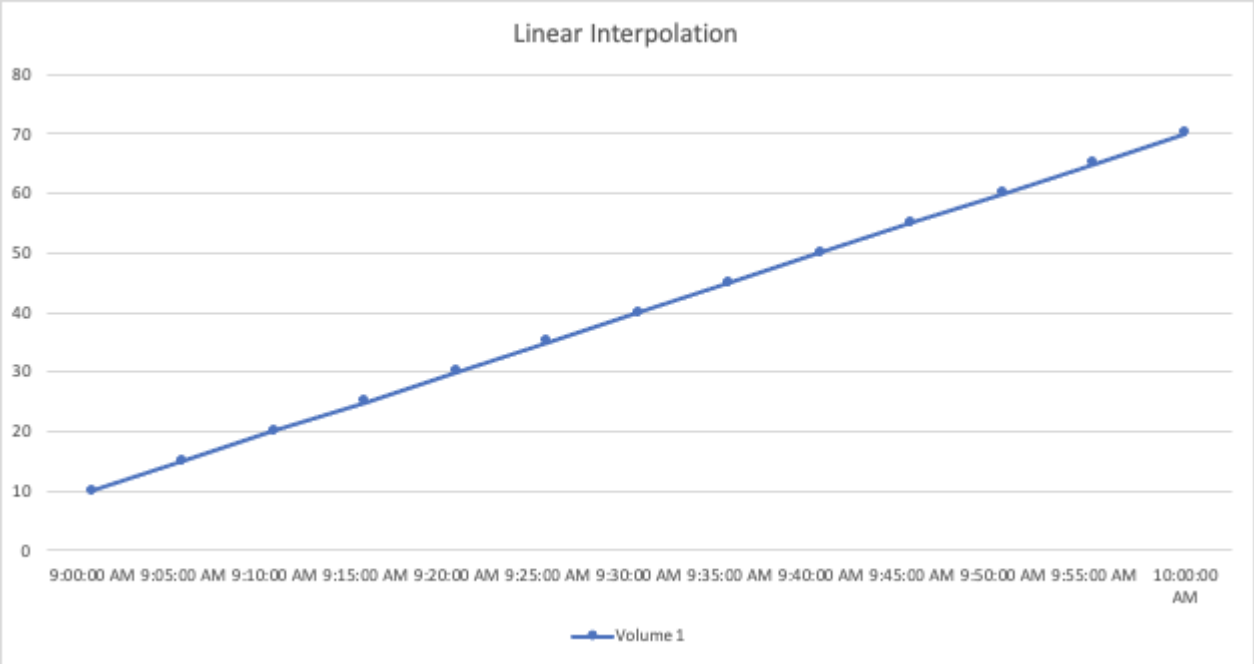
- **Keine**: Nichts tun, d. h. zwischendurch keine Punkte generieren.



- **Treppe**: Aus dem Wert des vorherigen Punkts wird ein Punkt generiert. In einer geraden Linie würde dies als typisches „Treppen“-Layout angezeigt.



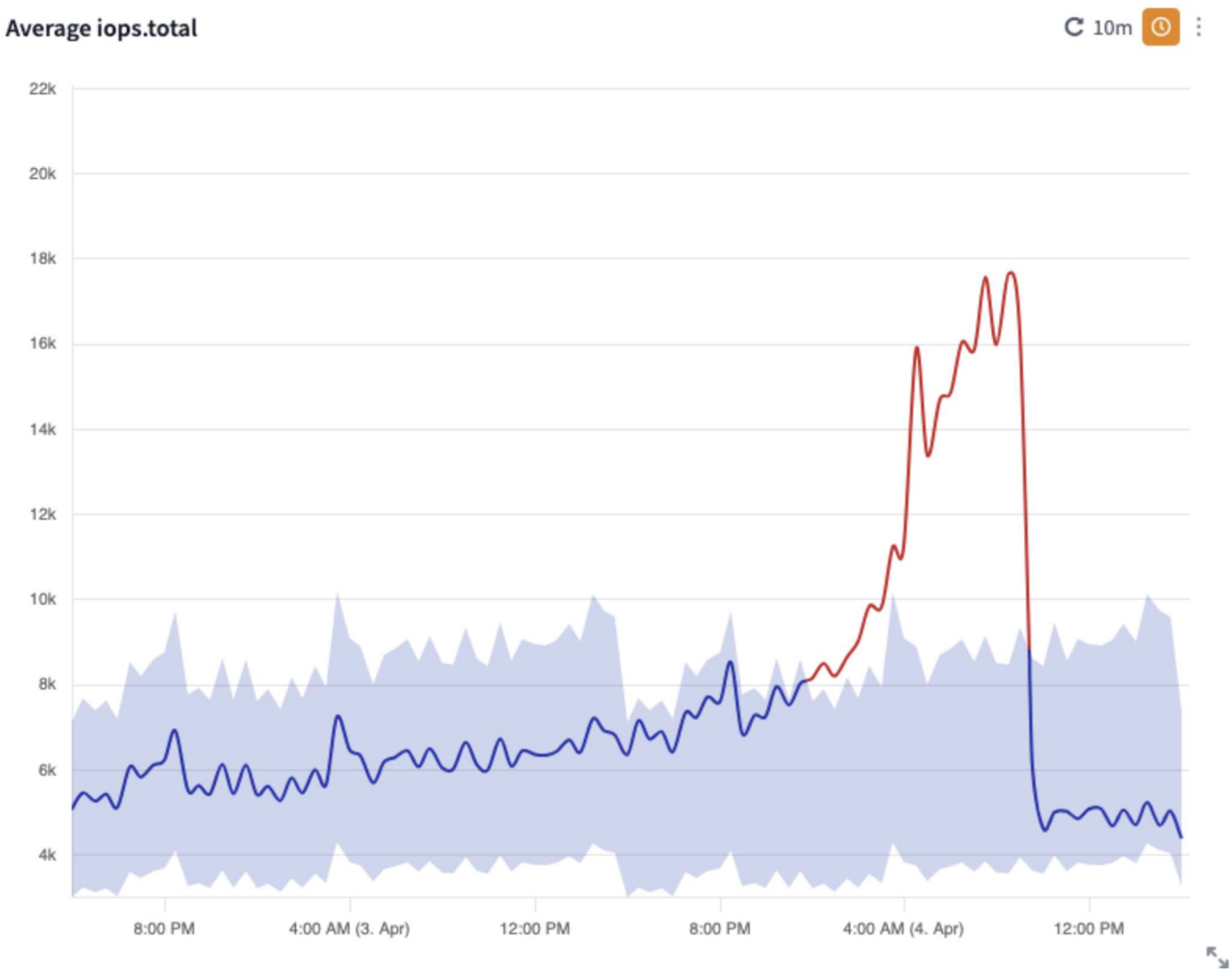
- **Linear**: Ein Punkt wird als Wert zwischen den beiden Verbindungspunkten generiert. Erzeugt eine Linie, die wie die Verbindungslinie zwischen den beiden Punkten aussieht, jedoch mit zusätzlichen (interpolierten) Datenpunkten.



Anomaliegrenzen in Linien-Widgets

Wenn Sie ein Linien- oder Spline-Diagramm-Widget in ein Dashboard oder eine Zielseite einbinden, können Sie das Diagramm im Kontext der **erwarteten Grenzen** für die Daten anzeigen. Sie können sich das so vorstellen, als würden Sie in den Mustern Ihrer Daten nach Anomalien suchen.

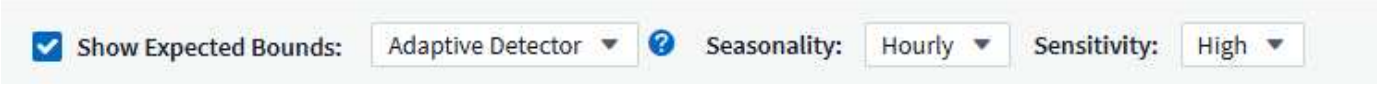
DII verwendet saisonale Daten (stündlich oder täglich), um Ober- und Untergrenzen für die *erwarteten* Werte der Daten zu einem bestimmten Zeitpunkt festzulegen. Wenn die Daten über oder unter diese erwarteten Grenzen steigen, wird dies im Diagramm als Anomalie hervorgehoben.



Um Anomaliegrenzen anzuzeigen, bearbeiten Sie das Widget und wählen Sie *Anomaliegrenzen anzeigen*. Sie können zwischen zwei Erkennungsalgorithmen wählen:

- **Adaptiver Detektor** passt sich schnell an Änderungen an und ist daher hilfreich für detaillierte Untersuchungen.
- **Smooth Detector** minimiert Rauschen und Fehlalarme, filtert kurzfristige Schwankungen heraus und erkennt dennoch signifikante Verschiebungen.

Darüber hinaus können Sie wählen, ob die Saisonalität stündlich oder täglich angezeigt werden soll, und die Empfindlichkeit der Erkennung festlegen. Bei *hoher* Empfindlichkeit werden mehr Grenzüberschreitungen erkannt, bei *niedriger* Empfindlichkeit weniger.



Beachten Sie, dass Sie die erwarteten Grenzen möglicherweise nur dann sehen, wenn das Diagramm auf die Anzeige einer einzelnen Linie eingestellt ist. Wenn Ihre „Gruppieren nach“-Einstellungen oder Filter mehrere Zeilen anzeigen oder wenn Sie mehrere Abfragen für das Widget festgelegt haben, wird die Option zum Anzeigen der erwarteten Grenzen deaktiviert.

Beispiel-Dashboards

Dashboard-Beispiel: Leistung virtueller Maschinen

Der IT-Betrieb steht heute vor zahlreichen Herausforderungen. Von Administratoren wird verlangt, mit weniger mehr zu erreichen, und die vollständige Transparenz Ihrer dynamischen Rechenzentren ist ein Muss. In diesem Beispiel zeigen wir Ihnen, wie Sie ein Dashboard mit Widgets erstellen, die Ihnen betriebliche Einblicke in die Leistung der virtuellen Maschine (VM) auf Ihrem Mandanten geben. Wenn Sie diesem Beispiel folgen und Widgets erstellen, die auf Ihre eigenen spezifischen Anforderungen zugeschnitten sind, können Sie beispielsweise die Backend-Speicherleistung im Vergleich zur Frontend-Leistung virtueller Maschinen visualisieren oder die VM-Latenz im Vergleich zur E/A-Nachfrage anzeigen.

Informationen zu diesem Vorgang

Hier erstellen wir ein Dashboard zur Leistung virtueller Maschinen mit den folgenden Informationen:

- eine Tabelle mit VM-Namen und Leistungsdaten
- ein Diagramm, das die VM-Latenz mit der Speicherlatenz vergleicht
- ein Diagramm, das Lese-, Schreib- und Gesamt-IOPS für VMs zeigt
- ein Diagramm, das den maximalen Durchsatz für Ihre VMs zeigt

Dies ist nur ein einfaches Beispiel. Sie können Ihr Dashboard anpassen, um beliebige Leistungsdaten hervorzuheben und zu vergleichen und so Ihre eigenen betrieblichen Best Practices zu verfolgen.

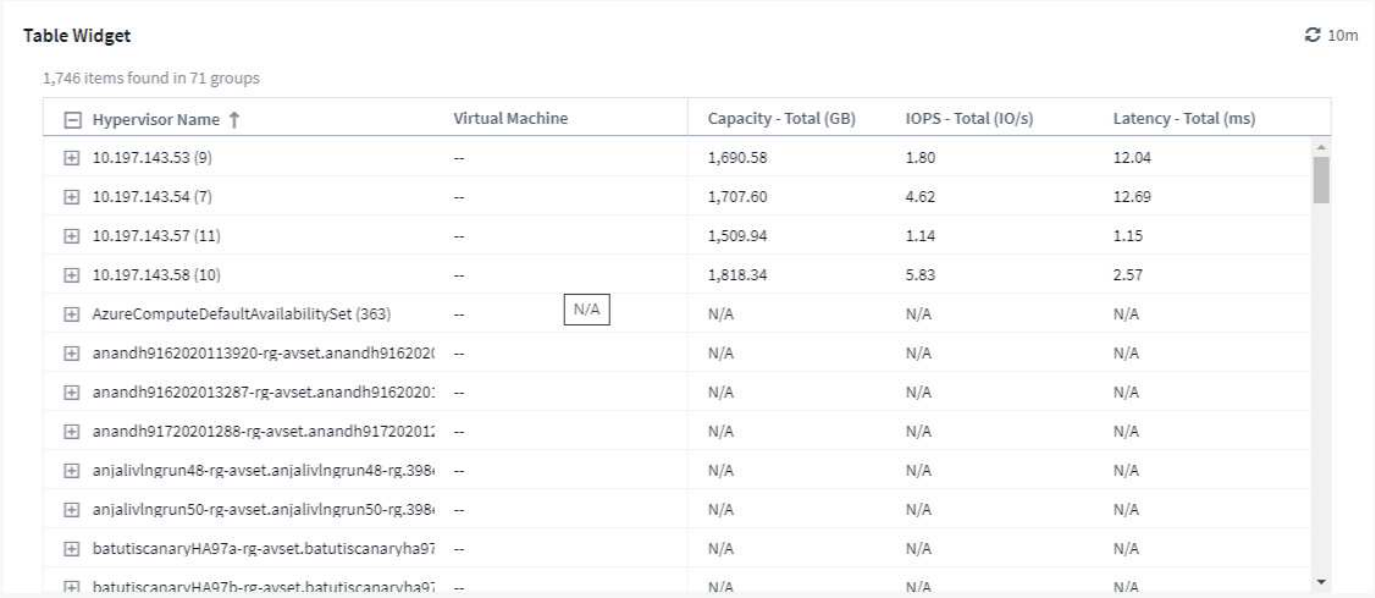
Schritte

1. Melden Sie sich bei Insight als Benutzer mit Administratorberechtigungen an.
2. Wählen Sie im Menü **Dashboards** die Option **[+Neues Dashboard]** aus.

   Die Seite **Neues Dashboard** wird geöffnet.

3. Geben Sie oben auf der Seite einen eindeutigen Namen für das Dashboard ein, beispielsweise „VM-Leistung nach Anwendung“.
4. Klicken Sie auf **Speichern**, um das Dashboard unter dem neuen Namen zu speichern.
5. Beginnen wir mit dem Hinzufügen unserer Widgets. Klicken Sie bei Bedarf auf das Symbol **Bearbeiten**, um den Bearbeitungsmodus zu aktivieren.
6. Klicken Sie auf das Symbol **Widget hinzufügen** und wählen Sie **Tabelle** aus, um dem Dashboard ein neues Tabellen-Widget hinzuzufügen.

   Das Dialogfeld „Widget bearbeiten“ wird geöffnet. Die angezeigten Standarddaten gelten für alle Speicher Ihres Mandanten.



1. Wir können dieses Widget anpassen. Löschen Sie im Feld „Name“ oben „Widget 1“ und geben Sie „Virtual Machine Performance table“ ein.
2. Klicken Sie auf das Dropdown-Menü „Asset-Typ“ und ändern Sie „*Speicher*“ in „Virtuelle Maschine_“.

   Die Tabellendaten ändern sich, um alle virtuellen Maschinen auf Ihrem Mandanten anzuzeigen.

3. Fügen wir der Tabelle einige Spalten hinzu. Klicken Sie rechts auf das Zahnradsymbol und wählen Sie *Hypervisorname*, *IOPS – Gesamt* und *Latenz – Gesamt* aus. Sie können auch versuchen, den Namen in die Suche einzugeben, um schnell das gewünschte Feld anzuzeigen.

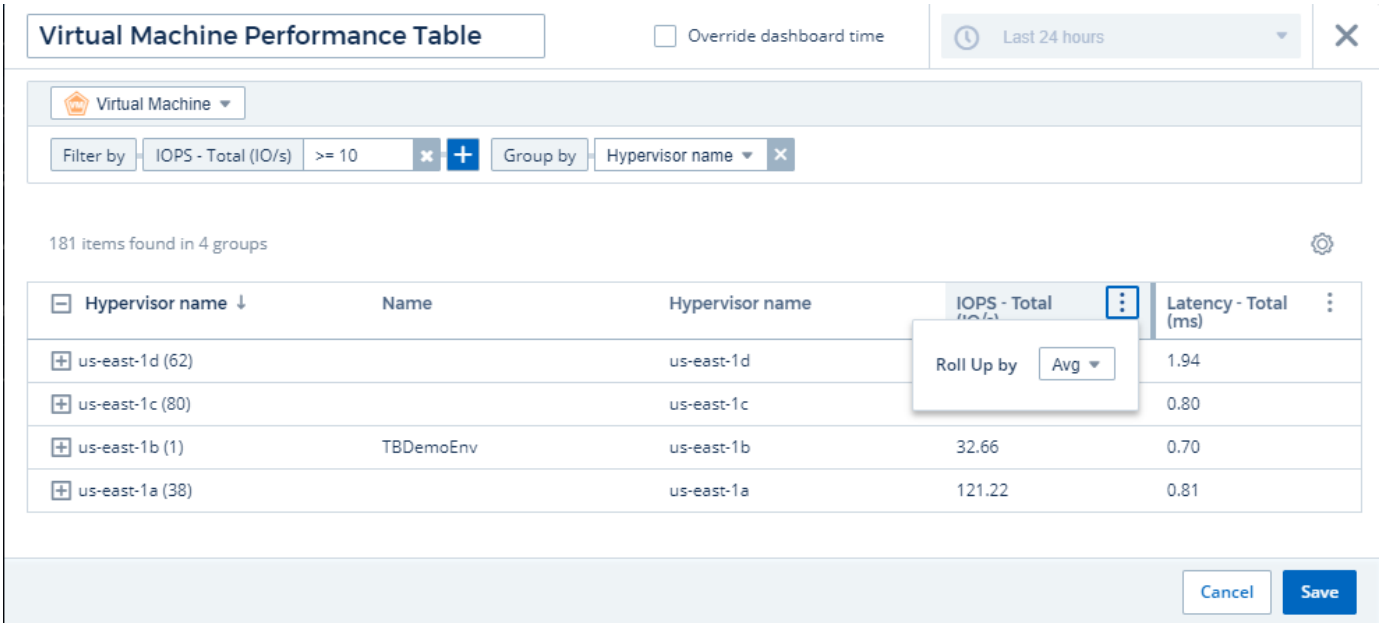
   Diese Spalten werden nun in der Tabelle angezeigt. Sie können die Tabelle nach jeder dieser Spalten sortieren. Beachten Sie, dass die Spalten in der Reihenfolge angezeigt werden, in der sie dem Widget hinzugefügt wurden.

4. Für diese Übung schließen wir VMs aus, die nicht aktiv verwendet werden. Filtern wir also alles heraus, was weniger als 10 IOPS insgesamt hat. Klicken Sie auf die Schaltfläche **[+]** neben **Filtern nach** und wählen Sie *IOPS – Gesamt* aus. Klicken Sie auf **Beliebig** und geben Sie „10“ in das Feld **Von** ein. Lassen Sie das Feld **An** leer. Klicken Sie außerhalb des Filterfelds oder drücken Sie die Eingabetaste, um den Filter festzulegen.

   Die Tabelle zeigt jetzt nur VMs mit 10 oder mehr Gesamt-IOPS.

5. Wir können die Tabelle weiter reduzieren, indem wir die Ergebnisse gruppieren. Klicken Sie auf die Schaltfläche **[+]** neben **Gruppieren nach** und wählen Sie ein Feld zum Gruppieren aus, z. B. *Anwendung* oder *Hypervisorname*. Die Gruppierung wird automatisch angewendet.

   Die Tabellenzeilen werden nun entsprechend Ihrer Einstellung gruppiert. Sie können die Gruppen nach Bedarf erweitern und reduzieren. Gruppierte Zeilen zeigen zusammengefasste Daten für jede Spalte. Bei einigen Spalten können Sie die Rollup-Methode für die jeweilige Spalte auswählen.



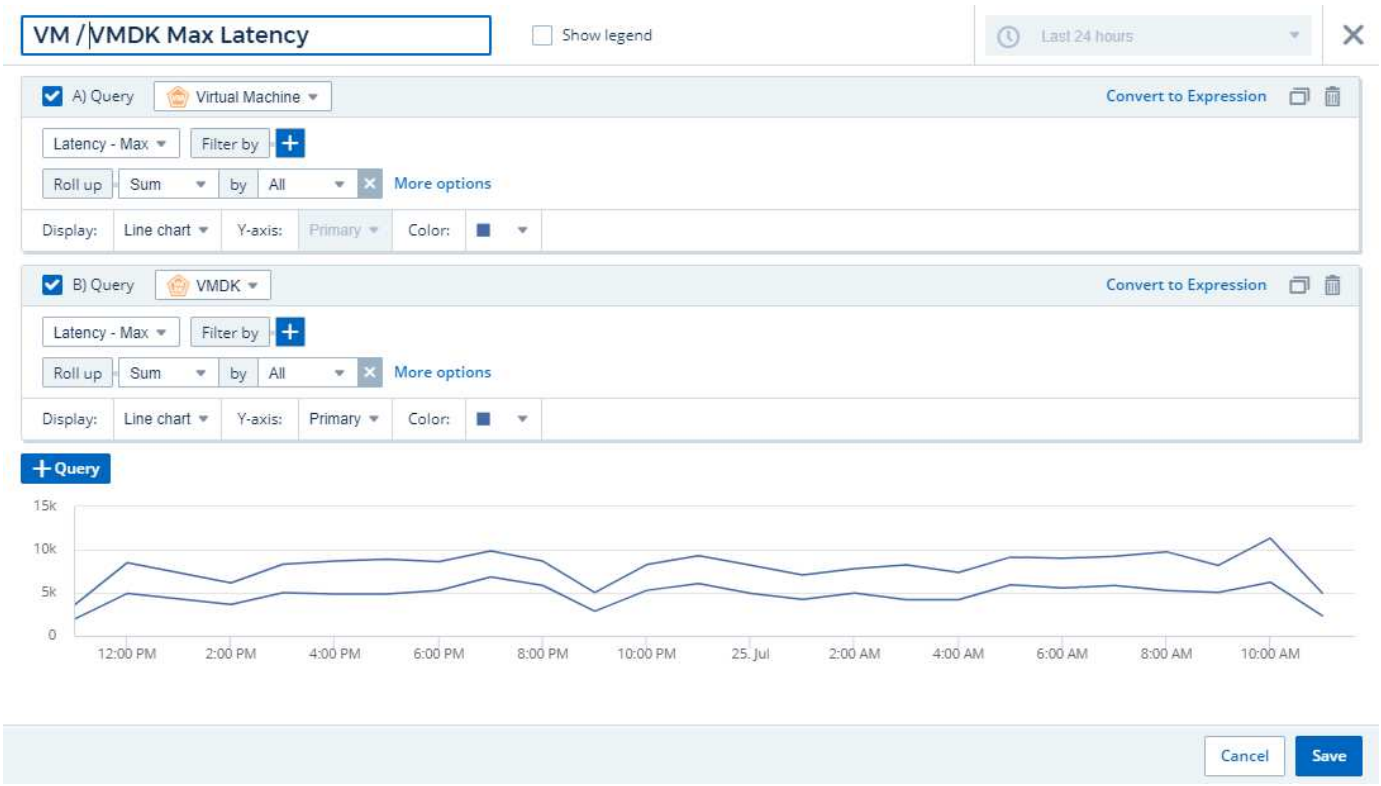
1. Wenn Sie das Tabellen-Widget nach Ihren Wünschen angepasst haben, klicken Sie auf die Schaltfläche **[Speichern]**.

   Das Tabellen-Widget wird im Dashboard gespeichert.

Sie können die Größe des Widgets auf dem Dashboard ändern, indem Sie die untere rechte Ecke ziehen. Machen Sie das Widget breiter, um alle Spalten deutlich anzuzeigen. Klicken Sie auf **Speichern**, um das aktuelle Dashboard zu speichern.

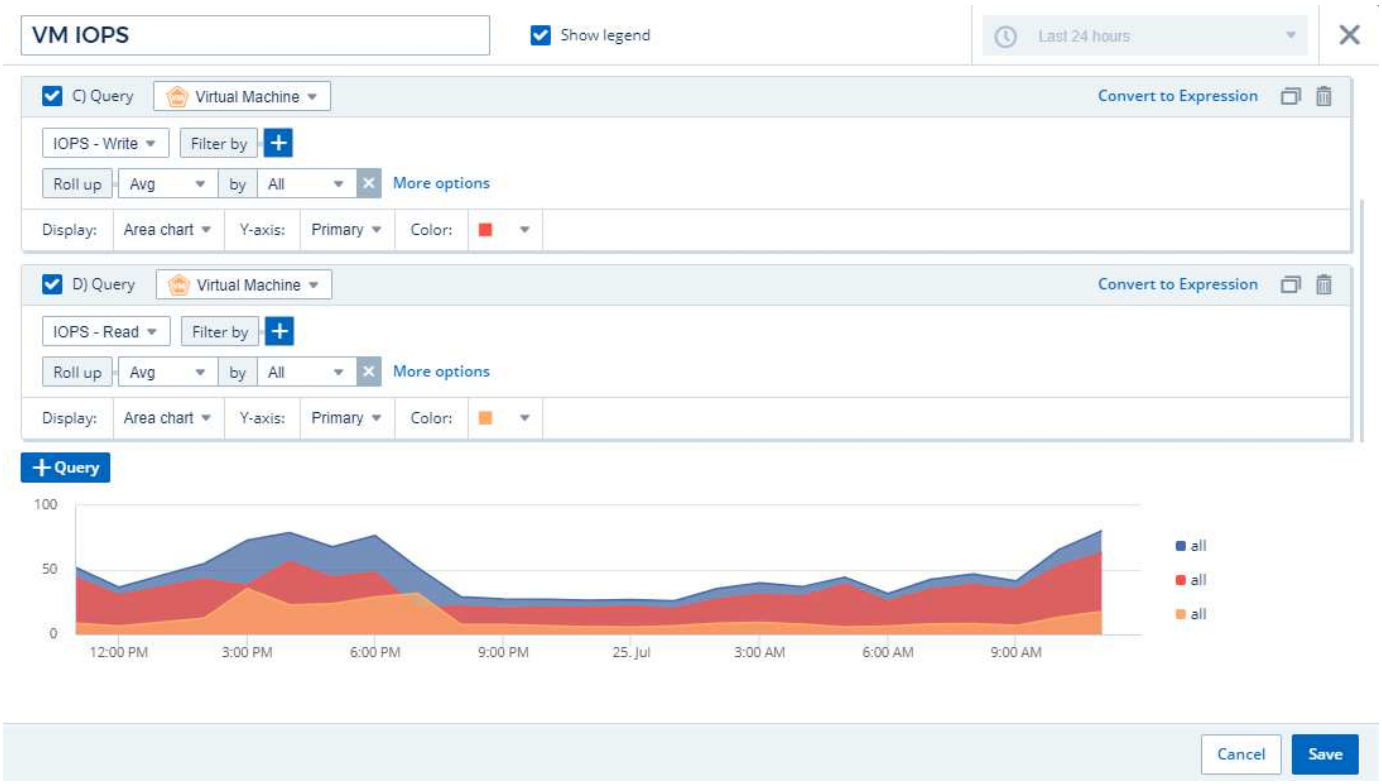
Als Nächstes fügen wir einige Diagramme hinzu, um die Leistung unserer VM anzuzeigen. Erstellen wir ein Liniendiagramm, das die VM-Latenz mit der VMDK-Latenz vergleicht.

1. Klicken Sie bei Bedarf auf das Symbol **Bearbeiten** im Dashboard, um den Bearbeitungsmodus zu aktivieren.
2. Klicken Sie auf das Symbol **[Widget hinzufügen]** und wählen Sie *Liniendiagramm* aus, um dem Dashboard ein neues Liniendiagramm-Widget hinzuzufügen.
3. Das Dialogfeld **Widget bearbeiten** wird geöffnet. Nennen Sie dieses Widget „VM / VMDK Max Latency“
4. Wählen Sie **Virtuelle Maschine** und wählen Sie *Latenz – Max*. Legen Sie die gewünschten Filter fest oder lassen Sie **Filtern nach** leer. Wählen Sie für **Rollup** *Sum* by *All*. Zeigen Sie diese Daten als *Liniendiagramm* an und belassen Sie die *Y-Achse* als *Primär*.
5. Klicken Sie auf die Schaltfläche **[+Abfrage]**, um eine zweite Datenzeile hinzuzufügen. Wählen Sie für diese Zeile *VMDK* und *Latency – Max* aus. Legen Sie die gewünschten Filter fest oder lassen Sie **Filtern nach** leer. Wählen Sie für **Rollup** *Sum* by *All*. Zeigen Sie diese Daten als *Liniendiagramm* an und belassen Sie die *Y-Achse* als *Primär*.
6. Klicken Sie auf **[Speichern]**, um dieses Widget zum Dashboard hinzuzufügen.



Als Nächstes fügen wir ein Diagramm hinzu, das die Lese-, Schreib- und Gesamt-IOPS der VM in einem einzigen Diagramm zeigt.

1. Klicken Sie auf das Symbol **[Widget hinzufügen]** und wählen Sie *Flächendiagramm* aus, um dem Dashboard ein neues Flächendiagramm-Widget hinzuzufügen.
2. Das Dialogfeld „Widget bearbeiten“ wird geöffnet. Nennen Sie dieses Widget „VM IOPS“
3. Wählen Sie **Virtuelle Maschine** und wählen Sie *IOPS – Gesamt*. Legen Sie die gewünschten Filter fest oder lassen Sie **Filtern nach** leer. Wählen Sie für **Aufsummieren** *Summe* nach *Alle*. Zeigen Sie diese Daten als *Flächendiagramm* an und belassen Sie die *Y-Achse* als *Primär*.
4. Klicken Sie auf die Schaltfläche **[+Abfrage]**, um eine zweite Datenzeile hinzuzufügen. Wählen Sie für diese Zeile **Virtual Machine** und dann *IOPS – Lesen*.
5. Klicken Sie auf die Schaltfläche **[+Abfrage]**, um eine dritte Datenzeile hinzuzufügen. Wählen Sie für diese Zeile **Virtual Machine** und dann *IOPS – Write* aus.
6. Klicken Sie auf **Legende anzeigen**, um eine Legende für dieses Widget auf dem Dashboard anzuzeigen.



1. Klicken Sie auf **[Speichern]**, um dieses Widget zum Dashboard hinzuzufügen.

Als Nächstes fügen wir ein Diagramm hinzu, das den VM-Durchsatz für jede mit der VM verknüpfte Anwendung zeigt. Wir werden hierfür die Roll-Up-Funktion verwenden.

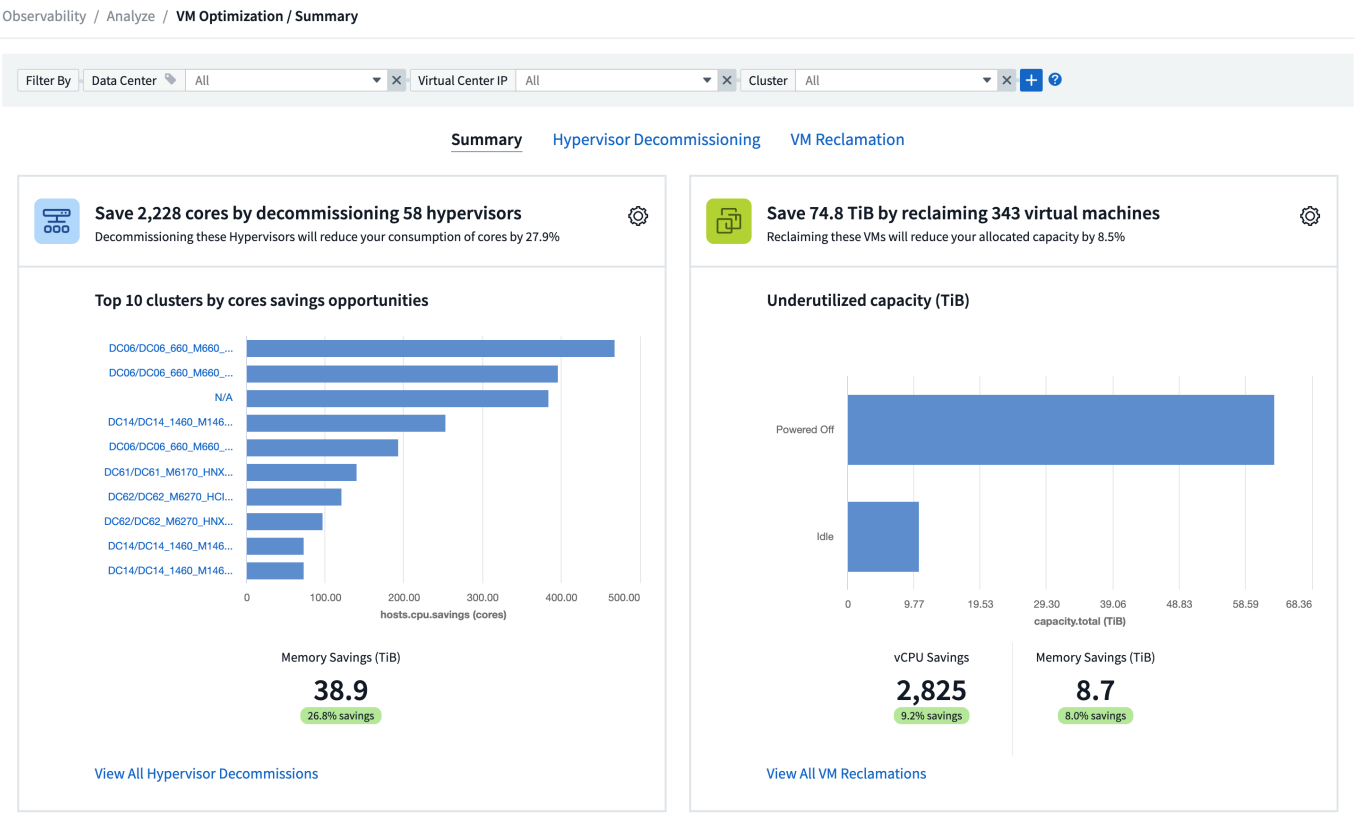
1. Klicken Sie auf das Symbol **[Widget hinzufügen]** und wählen Sie *Liniendiagramm* aus, um dem Dashboard ein neues Liniendiagramm-Widget hinzuzufügen.
2. Das Dialogfeld „Widget bearbeiten“ wird geöffnet. Nennen Sie dieses Widget „VM-Durchsatz nach Anwendung“.
3. Wählen Sie „Virtuelle Maschine“ und dann „Durchsatz – Gesamt“. Legen Sie die gewünschten Filter fest oder lassen Sie das Feld „Filtern nach“ leer. Wählen Sie für Rollup „Max“ und wählen Sie nach „Anwendung“ oder „Name“ aus. Zeigen Sie die Top 10-Anwendungen. Zeigen Sie diese Daten als Liniendiagramm an und belassen Sie die Y-Achse als primär.
4. Klicken Sie auf **[Speichern]**, um dieses Widget zum Dashboard hinzuzufügen.

Sie können Widgets auf dem Dashboard verschieben, indem Sie die Maustaste an einer beliebigen Stelle oben im Widget gedrückt halten und es an eine neue Position ziehen.

Sie können die Größe von Widgets ändern, indem Sie die untere rechte Ecke ziehen.

Denken Sie daran, das Dashboard nach dem Vornehmen Ihrer Änderungen **[Speichern]** zu speichern.

Ihr endgültiges VM-Leistungs-Dashboard sieht ungefähr so aus:



Best Practices für Dashboards und Widgets

Tipps und Tricks, die Ihnen helfen, die leistungsstarken Funktionen von Dashboards und Widgets optimal zu nutzen.

Die richtige Metrik finden

Data Infrastructure Insights erfasst Zähler und Metriken unter Verwendung von Namen, die sich manchmal von Datensammler zu Datensammler unterscheiden.

Bedenken Sie bei der Suche nach der richtigen Metrik oder dem richtigen Zähler für Ihr Dashboard-Widget, dass die gewünschte Metrik möglicherweise einen anderen Namen hat als den, an den Sie denken. Während Dropdown-Listen in Data Infrastructure Insights normalerweise alphabetisch geordnet sind, kann es vorkommen, dass ein Begriff nicht dort in der Liste angezeigt wird, wo er Ihrer Meinung nach hingehört. Beispielsweise erscheinen Begriffe wie „Rohkapazität“ und „genutzte Kapazität“ in den meisten Listen nicht zusammen.

Best Practice: Verwenden Sie die Suchfunktion in Feldern wie „Filtern nach“ oder an Stellen wie der Spaltenauswahl, um das Gesuchte zu finden. Wenn Sie beispielsweise nach „cap“ suchen, werden alle Metriken angezeigt, deren Name „capacity“ enthält, unabhängig davon, wo sie in der Liste vorkommen. Sie können dann ganz einfach die gewünschten Metriken aus dieser kürzeren Liste auswählen.

Hier sind einige alternative Ausdrücke, die Sie bei der Suche nach Metriken ausprobieren können:

Wenn Sie Folgendes finden möchten:	Versuchen Sie auch, nach Folgendem zu suchen:
CPU	Prozessor

Kapazität	Genutzte Kapazität Rohkapazität Bereitgestellte Kapazität Speicherpoolkapazität <anderer Assettyp>-Kapazität Geschriebene Kapazität
Festplattengeschwindigkeit	Niedrigste Festplattengeschwindigkeit Festplattentyp mit der geringsten Leistung
Gastgeber	Hypervisor-Hosts
Hypervisor	Host ist Hypervisor
Mikrocode	Firmware
Name	Alias Hypervisorname Speichername <anderer Assettyp> Name Einfacher Name Ressourcenname Fabric-Alias
Lesen / Schreiben	Teilweise R/W Ausstehende Schreibvorgänge IOPS – Schreibkapazität Latenz – Lesen Cache-Auslastung – Lesen
Virtuelle Maschine	VM ist virtuell

Dies ist keine vollständige Liste. Dies sind lediglich Beispiele für mögliche Suchbegriffe.

Die richtigen Vermögenswerte finden

Die Assets, auf die Sie in Widget-Filtern und -Suchen verweisen können, variieren von Asset-Typ zu Asset-Typ.

In Dashboards und Asset-Seiten bestimmt der Asset-Typ, um den Sie Ihr Widget erstellen, die anderen Asset-Typ-Zähler, nach denen Sie filtern oder eine Spalte hinzufügen können. Beachten Sie beim Erstellen Ihres Widgets Folgendes:

Dieser Asset-Typ/Zähler:	Kann nach diesen Assets gefiltert werden:
Virtuelle Maschine	VMDK
Datenspeicher	Internes Volume VMDK-Volume der virtuellen Maschine
Hypervisor	Virtuelle Maschine ist Hypervisor-Host
Gastgeber	Internes Volume Volume Cluster Host Virtuelle Maschine
Stoff	Hafen

Dies ist keine vollständige Liste.

Best Practice: Wenn Sie nach einem bestimmten Asset-Typ filtern, der nicht in der Liste angezeigt wird, versuchen Sie, Ihre Abfrage um einen alternativen Asset-Typ herum aufzubauen.

Streudiagramm-Beispiel: Kennen Sie Ihre Achse

Durch Ändern der Reihenfolge der Zähler in einem Streudiagramm-Widget werden die Achsen geändert, auf denen die Daten angezeigt werden.

Informationen zu diesem Vorgang

In diesem Beispiel wird ein Streudiagramm erstellt, mit dem Sie VMs mit geringer Leistung und hoher Latenz im Vergleich zu niedrigen IOPS erkennen können.

Schritte

1. Erstellen oder öffnen Sie ein Dashboard im Bearbeitungsmodus und fügen Sie ein **Streudiagramm**-Widget hinzu.
2. Wählen Sie einen Asset-Typ aus, beispielsweise *Virtuelle Maschine*.
3. Wählen Sie den ersten Zähler aus, den Sie darstellen möchten. Wählen Sie für dieses Beispiel *Latenz – Gesamt*.

   Latenz – Gesamt wird entlang der X-Achse des Diagramms dargestellt.

4. Wählen Sie den zweiten Zähler aus, den Sie darstellen möchten. Wählen Sie für dieses Beispiel *IOPS – Gesamt* aus.

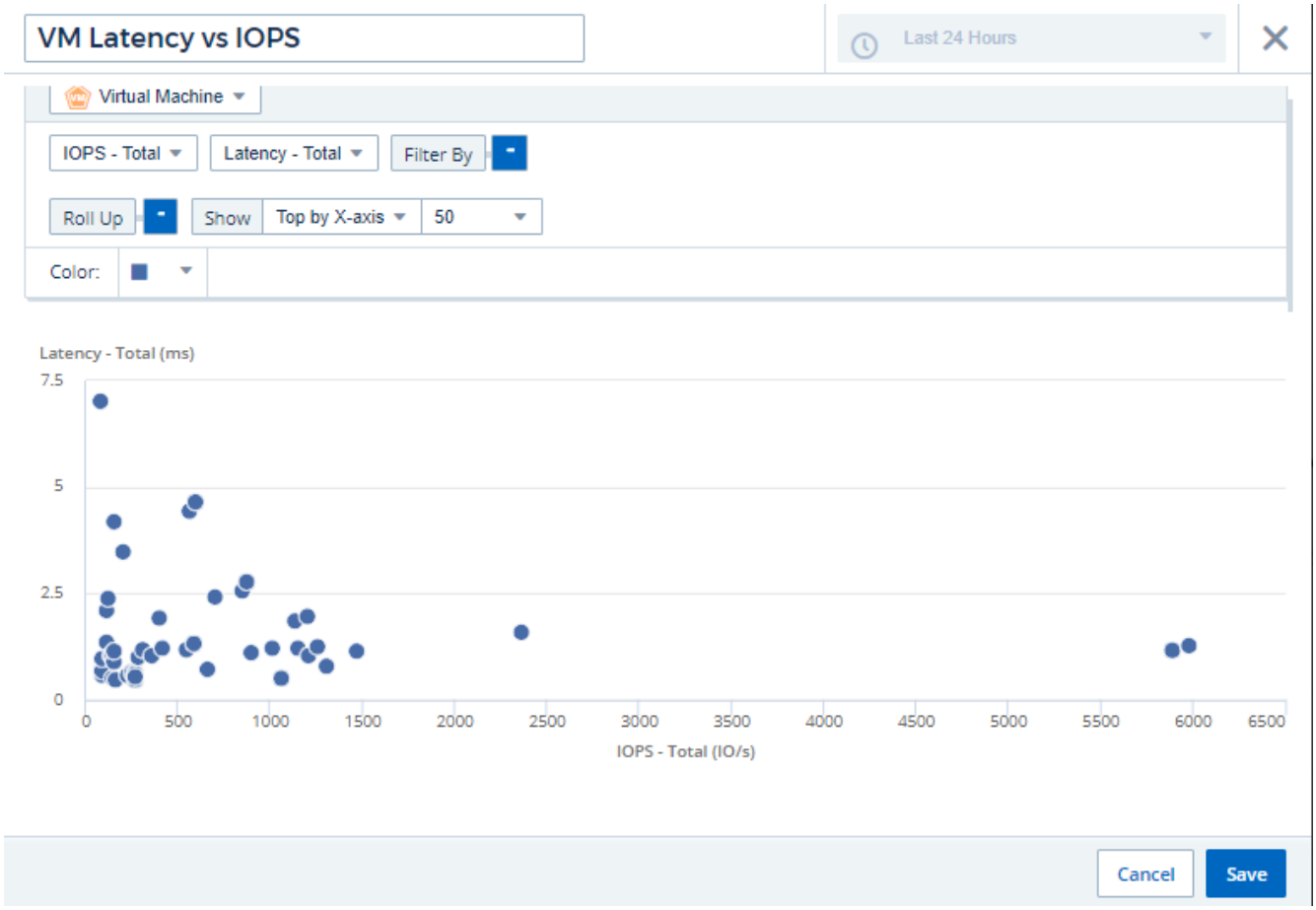
   IOPS – Gesamt wird im Diagramm entlang der Y-Achse dargestellt. VMs mit höherer Latenz werden auf der rechten Seite des Diagramms angezeigt. Es werden nur die 100 VMs mit der höchsten Latenz angezeigt, da die Einstellung **Top nach X-Achse** aktuell ist.

5. Kehren Sie nun die Reihenfolge der Zähler um, indem Sie den ersten Zähler auf *IOPS – Gesamt* und den zweiten auf *Latenz – Gesamt* setzen.

   Im Diagramm wird nun die *Latenz – Gesamt* entlang der Y-Achse und die *IOPS – Gesamt* entlang der X-Achse dargestellt. VMs mit höheren IOPS werden jetzt auf der rechten Seite des Diagramms angezeigt.

   Beachten Sie, dass das Widget jetzt die 100 VMs mit den höchsten IOPS anzeigt, da wir die Einstellung

Top by X-Axis nicht geändert haben, da diese derzeit entlang der X-Achse dargestellt werden.



Sie können für das Diagramm auswählen, ob die obersten N der X-Achse, die obersten N der Y-Achse, die untersten N der X-Achse oder die untersten N der Y-Achse angezeigt werden sollen. In unserem letzten Beispiel zeigt das Diagramm die Top 100 VMs mit den höchsten Gesamt-IOPS. Wenn wir es in **Top nach Y-Achse** ändern, zeigt das Diagramm erneut die 100 VMs mit der höchsten Gesamtlatenz an.

Beachten Sie, dass Sie in einem Streudiagramm auf einen Punkt klicken können, um zur Asset-Seite für diese Ressource zu gelangen.

Arbeiten mit Abfragen

In Abfragen verwendete Assets

Mithilfe von Abfragen können Sie Ihr Netzwerk überwachen und Fehler beheben, indem Sie die Assets und Metriken Ihres Mandanten auf granularer Ebene anhand vom Benutzer ausgewählter Kriterien (z. B. Anmerkungen) durchsuchen.

Beachten Sie, dass Anmerkungsregeln, die Anmerkungen automatisch Assets zuweisen, eine Abfrage *erfordern*.

Sie können die physischen oder virtuellen Inventarressourcen (und die zugehörigen Metriken) Ihres Mandanten oder die mit der Integration bereitgestellten Metriken wie Kubernetes oder ONTAP Advanced Data abfragen.

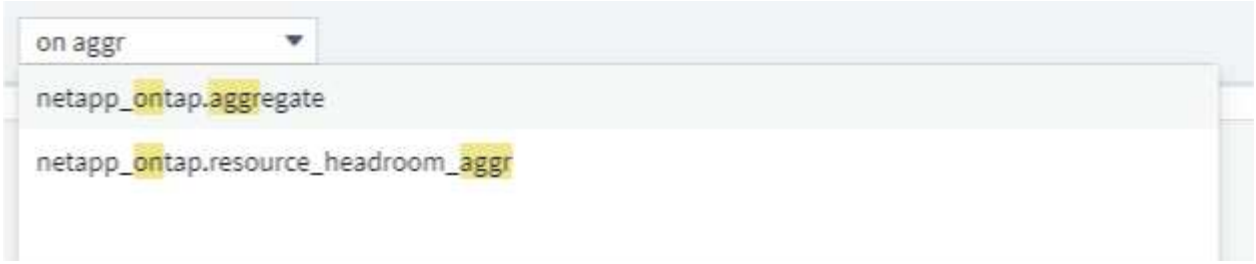
Inventarvermögen

Die folgenden Asset-Typen können in Abfragen, Dashboard-Widgets und benutzerdefinierten Asset-Landingpages verwendet werden. Die für Filter, Ausdrücke und Anzeigen verfügbaren Felder und Zähler variieren je nach Asset-Typ. Nicht alle Assets können in allen Widget-Typen verwendet werden.

- Anwendung
- Datenspeicher
- Scheibe
- Stoff
- Generisches Gerät
- Gastgeber
- Internes Volumen
- iSCSI-Sitzung
- iSCSI-Netzwerkportal
- Weg
- Hafen
- Qtree
- Quote
- Aktie
- Storage
- Speicherknoten
- Speicherpool
- Virtuelle Speichermaschine (SVM)
- Schalten
- Band
- VMDK
- Virtuelle Maschine
- Volumen
- Zone
- Zonenmitglied

Integrationsmetriken

Zusätzlich zur Abfrage von Inventarressourcen und den zugehörigen Leistungsmetriken können Sie auch **Integrationsdaten**-Metriken abfragen, wie sie beispielsweise von Kubernetes oder Docker generiert oder mit ONTAP Advanced Metrics bereitgestellt werden.



Erstellen von Abfragen

Mithilfe von Abfragen können Sie die Assets Ihres Mandanten auf granularer Ebene durchsuchen, die gewünschten Daten filtern und die Ergebnisse nach Ihren Wünschen sortieren.

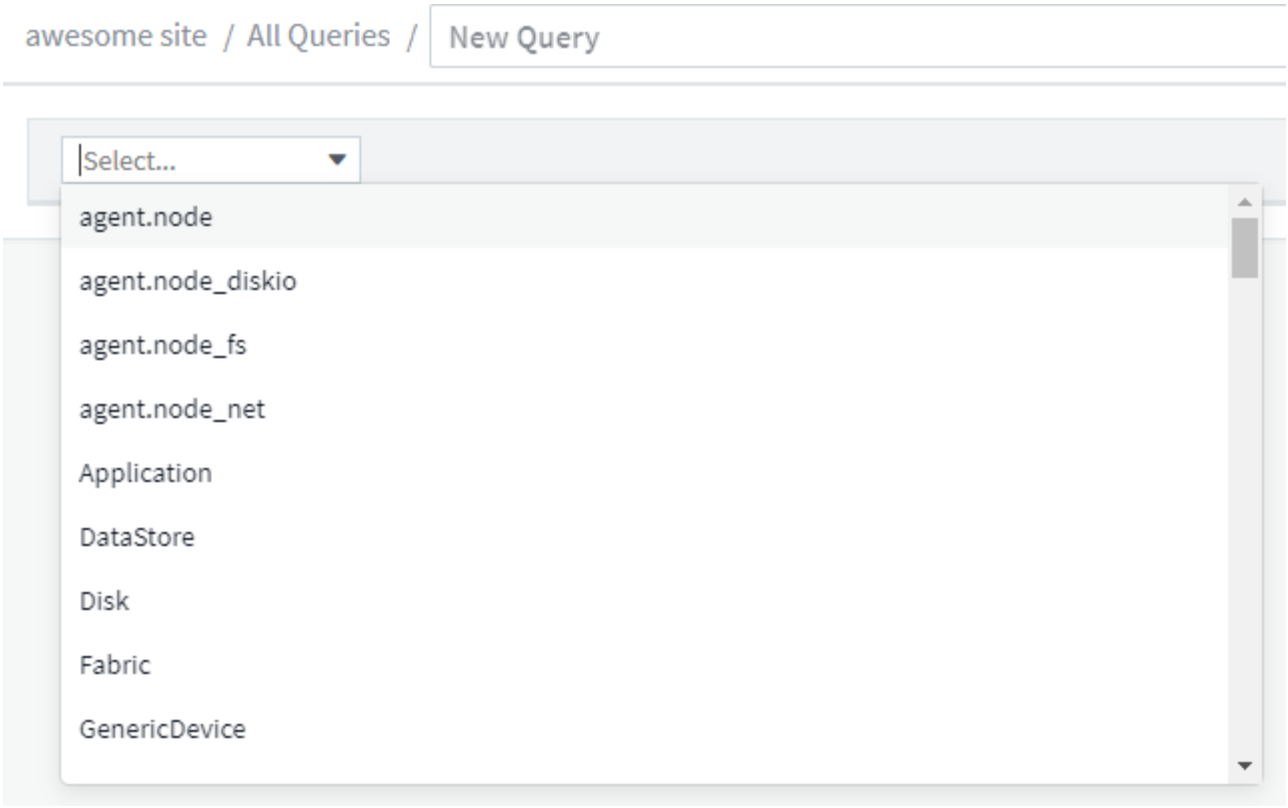
Sie können beispielsweise eine Abfrage für *Volumes* erstellen, einen Filter hinzufügen, um bestimmte *Speicher* zu finden, die mit den ausgewählten Volumes verknüpft sind, einen weiteren Filter hinzufügen, um eine bestimmte *Annotation* wie „Tier 1“ auf den ausgewählten Speichern zu finden, und schließlich einen weiteren Filter hinzufügen, um alle Speicher mit *IOPS – Lesen (IO/s)* größer als 25 zu finden. Wenn die Ergebnisse angezeigt werden, können Sie die mit der Abfrage verknüpften Informationsspalten in aufsteigender oder absteigender Reihenfolge sortieren.

Hinweis: Wenn ein neuer Datensammler hinzugefügt wird, der Assets erfasst, oder wenn Anmerkungen oder Anwendungszuweisungen vorgenommen werden, können Sie diese neuen Assets, Anmerkungen oder Anwendungen erst abfragen, nachdem die Abfragen indiziert wurden. Die Indizierung erfolgt in regelmäßigen Abständen oder während bestimmter Ereignisse, beispielsweise beim Ausführen von Anmerkungsregeln.

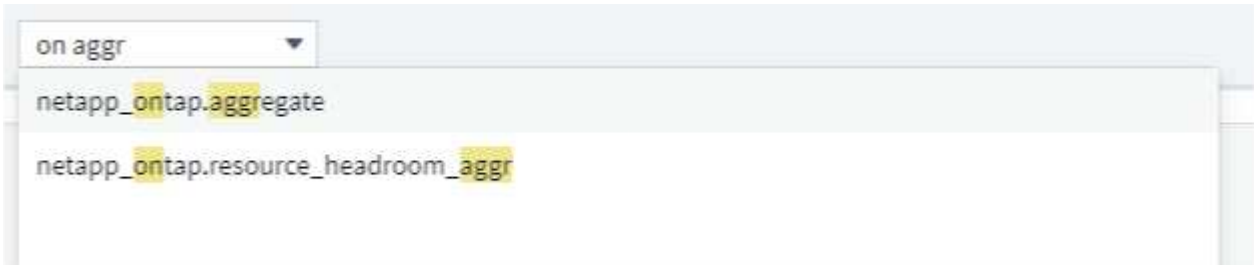
Das Erstellen einer Abfrage ist ganz einfach:

1. Navigieren Sie zu **Abfragen > *+Neue Abfrage**.
2. Wählen Sie aus der Liste „Auswählen …“ den Objekttyp aus, nach dem Sie suchen möchten. Sie können durch die Liste scrollen oder mit der Eingabe beginnen, um schneller zu finden, wonach Sie suchen.

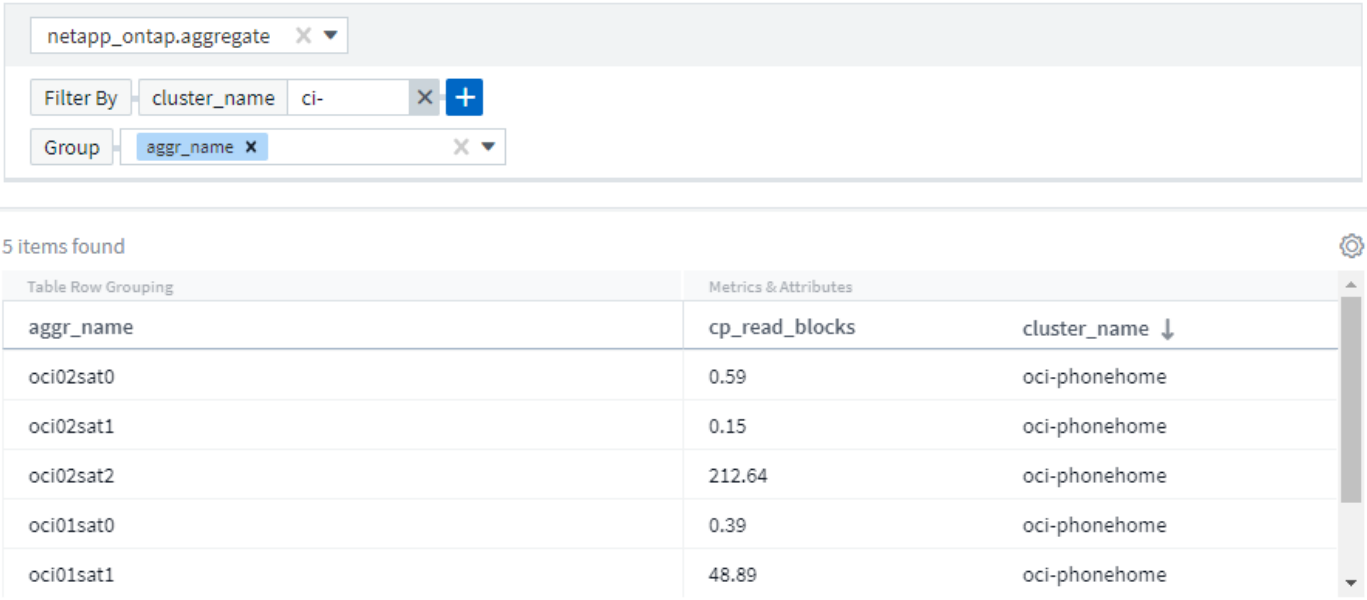
Scrollliste:



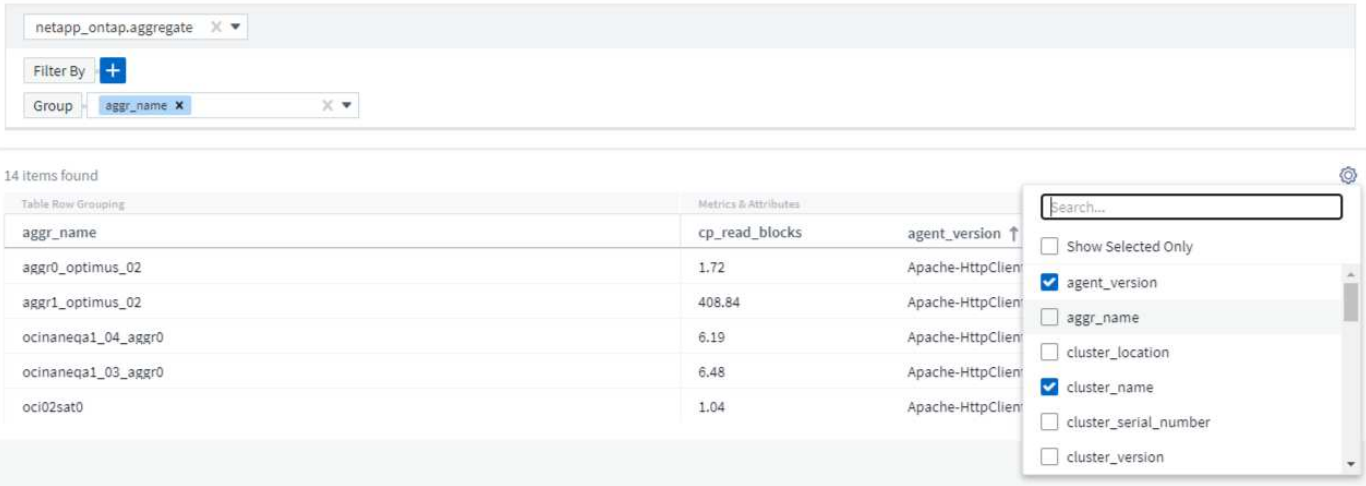
Zum Suchen eingeben:



Sie können Filter hinzufügen, um Ihre Abfrage weiter einzugrenzen, indem Sie im Feld **Filtern nach** auf die Schaltfläche **+** klicken. Gruppieren Sie Zeilen nach Objekt oder Attribut. Wenn Sie mit Integrationsdaten (Kubernetes, ONTAP Advanced Metrics usw.) arbeiten, können Sie bei Bedarf nach mehreren Attributen gruppieren.



Die Abfrageergebnisliste zeigt je nach gesuchtem Objekttyp eine Reihe von Standardspalten. Um Spalten hinzuzufügen, zu entfernen oder zu ändern, klicken Sie auf das Zahnradsymbol rechts neben der Tabelle. Die verfügbaren Spalten variieren je nach Asset-/Metriktyp.



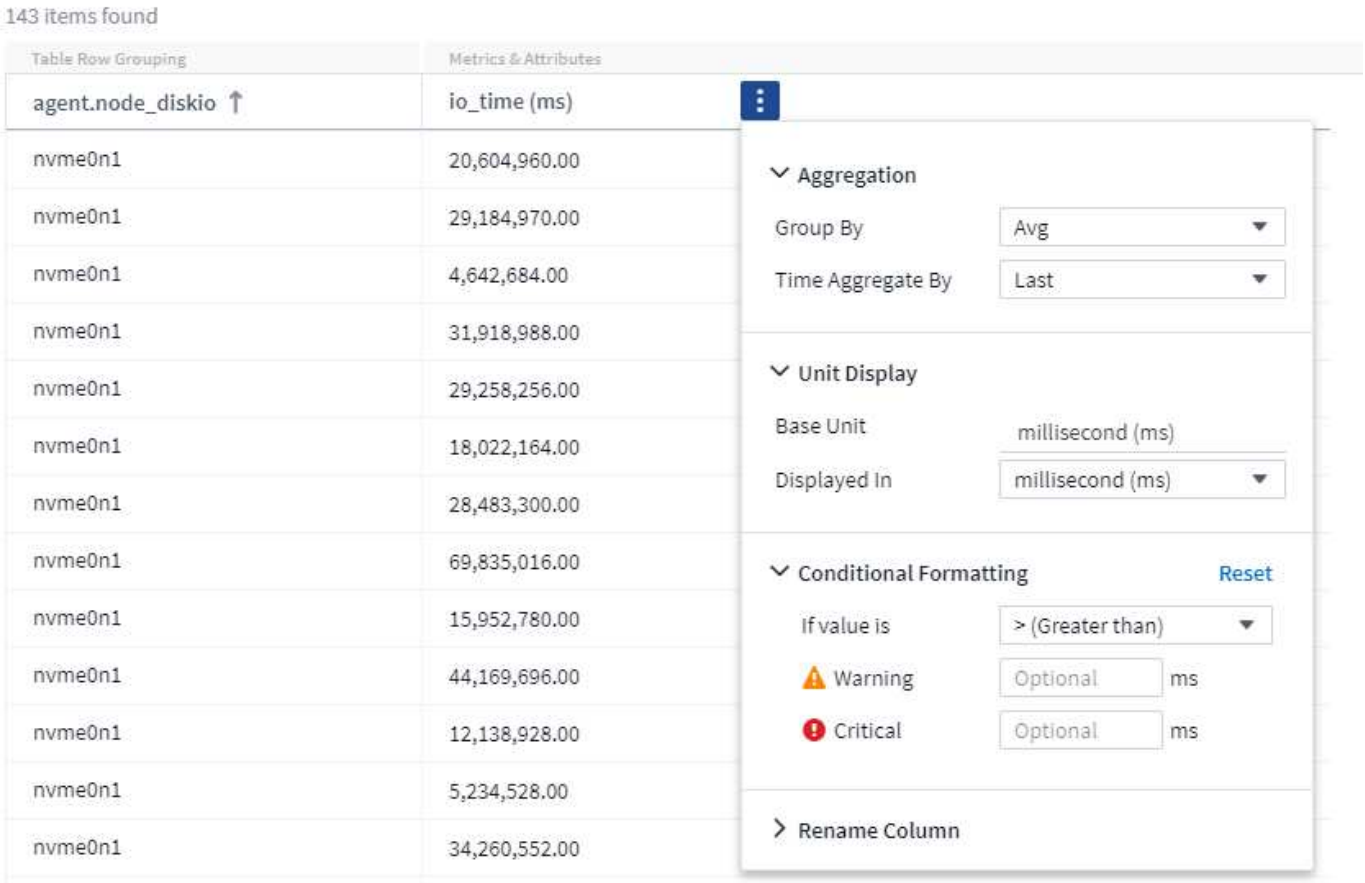
Sehen Sie es in Aktion

"Erkunden und Analysieren mit Abfragen in Data Infrastructure Insights (Video)"

Auswählen von Aggregation, Einheiten und bedingter Formatierung

Aggregation und Einheiten

Bei „Wert“-Spalten können Sie Ihre Abfrageergebnisse weiter verfeinern, indem Sie auswählen, wie die angezeigten Werte aggregiert werden, und indem Sie die Einheiten auswählen, in denen diese Werte angezeigt werden. Diese Optionen finden Sie, indem Sie das Menü mit den drei Punkten in der oberen Ecke einer Spalte auswählen.



Einheiten

Sie können die Einheiten auswählen, in denen die Werte angezeigt werden sollen. Wenn die ausgewählte Spalte beispielsweise die Rohkapazität anzeigt und die Werte in GiB angezeigt werden, Sie sie aber lieber als TiB anzeigen möchten, wählen Sie einfach TiB aus der Dropdown-Liste „Einheitenanzeige“ aus.

Aggregation

Wenn die angezeigten Werte aus den zugrunde liegenden Daten als „Durchschnitt“ aggregiert werden, Sie aber lieber die Summe aller Werte anzeigen möchten, wählen Sie „Summe“ entweder aus der Dropdown-Liste „Gruppieren nach“ (wenn Sie möchten, dass alle gruppierten Werte die Summen anzeigen) oder aus der Dropdown-Liste „Zeitaggregieren nach“ (wenn Sie möchten, dass die Zeilenwerte Summen der zugrunde liegenden Daten anzeigen).

Sie können gruppierte Datenpunkte nach *Durchschnitt, Maximum, Minimum oder Summe* aggregieren.

Sie können einzelne Zeilendaten nach *Durchschnitt, zuletzt erfasstem Datenpunkt, Maximum, Minimum oder Summe* aggregieren.

Bedingte Formatierung

Mit der bedingten Formatierung können Sie Schwellenwerte der Warn- und kritischen Stufen in der Liste der Abfrageergebnisse hervorheben, sodass Ausreißer und außergewöhnliche Datenpunkte sofort sichtbar werden.

Die bedingte Formatierung wird für jede Spalte separat festgelegt. Sie können beispielsweise einen Schwellenwertsatz für eine Kapazitätsspalte und einen anderen Satz für eine Durchsatzspalte auswählen.

Spalte umbenennen

Durch das Umbenennen einer Spalte wird der angezeigte Name in der Abfrageergebnisliste geändert. Der neue Spaltenname wird auch in der resultierenden Datei angezeigt, wenn Sie die Abfrageliste in das CSV-Format exportieren.

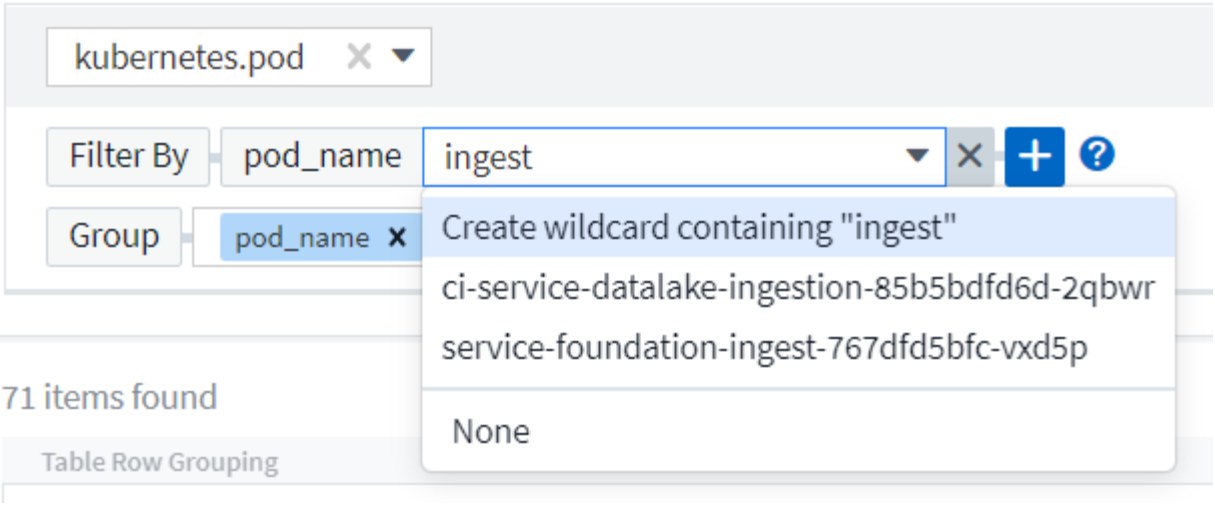
Speichern

Nachdem Sie Ihre Abfrage so konfiguriert haben, dass die gewünschten Ergebnisse angezeigt werden, können Sie auf die Schaltfläche **Speichern** klicken, um die Abfrage für die zukünftige Verwendung zu speichern. Geben Sie ihm einen aussagekräftigen und eindeutigen Namen.

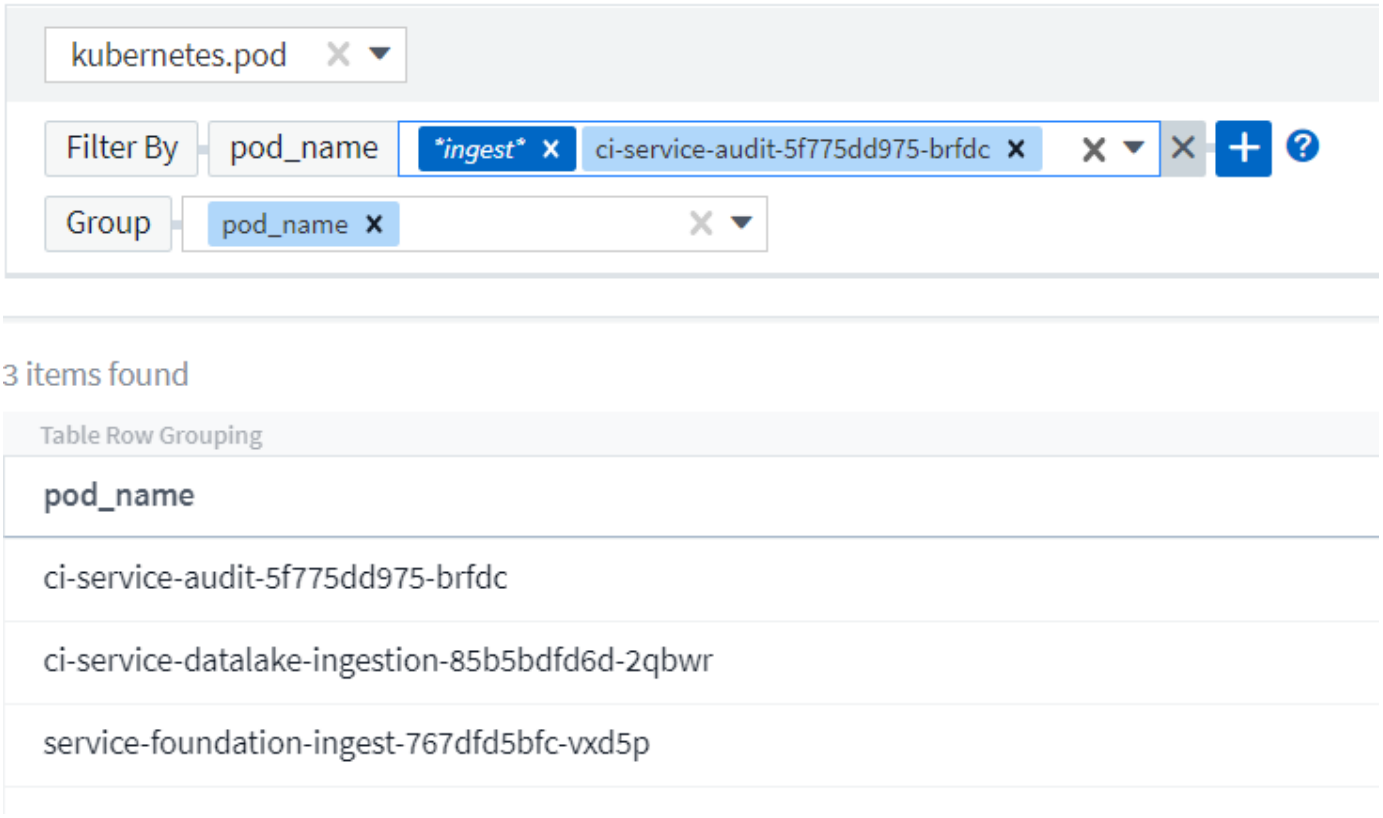
Mehr zum Filtern

Platzhalter und Ausdrücke

Wenn Sie in Abfragen oder Dashboard-Widgets nach Text oder Listenwerten filtern, wird Ihnen beim Eintippen die Option angezeigt, einen **Platzhalterfilter** basierend auf dem aktuellen Text zu erstellen. Wenn Sie diese Option auswählen, werden alle Ergebnisse zurückgegeben, die mit dem Platzhalterausdruck übereinstimmen. Sie können **Ausdrücke** auch mit NOT oder OR erstellen oder die Option „Keine“ auswählen, um nach Nullwerten im Feld zu filtern.



Filter, die auf Platzhaltern oder Ausdrücken basieren (z. B. NICHT, ODER, „Keine“ usw.), werden im Filterfeld dunkelblau angezeigt. Elemente, die Sie direkt aus der Liste auswählen, werden hellblau angezeigt.



Beachten Sie, dass die Platzhalter- und Ausdrucksfilterung mit Text oder Listen funktioniert, jedoch nicht mit Zahlen, Datumsangaben oder Booleschen Werten.

Filter verfeinern

Sie können Ihren Filter folgendermaßen verfeinern:

Filter	Was es bewirkt	Beispiel	Ergebnis

* (Sternchen)	ermöglicht Ihnen die Suche nach allem	vol*rhel	gibt alle Ressourcen zurück, die mit „vol“ beginnen und mit „rhel“ enden
? (Fragezeichen)	ermöglicht die Suche nach einer bestimmten Anzahl von Zeichen	BOS-PRD??-S12	gibt BOS-PRD***12***-S12, BOS-PRD***23***-S12 usw. zurück
ODER	ermöglicht Ihnen die Angabe mehrerer Entitäten	FAS2240 ODER CX600 ODER FAS3270	gibt einen der folgenden Werte zurück: FAS2440, CX600 oder FAS3270
NICHT	ermöglicht es Ihnen, Text aus den Suchergebnissen auszuschließen	NICHT EMV*	gibt alles zurück, was nicht mit "EMC" beginnt
Keiner	sucht in allen Feldern nach NULL-Werten	*Keiner*	gibt Ergebnisse zurück, bei denen das Zielfeld leer ist
Nicht *	sucht nach NULL-Werten in *Nur-Text*-Feldern	Nicht *	gibt Ergebnisse zurück, bei denen das Zielfeld leer ist

Wenn Sie eine Filterzeichenfolge in doppelte Anführungszeichen setzen, behandelt Insight alles zwischen dem ersten und letzten Anführungszeichen als exakte Übereinstimmung. Alle Sonderzeichen oder Operatoren innerhalb der Anführungszeichen werden als Literale behandelt. Wenn Sie beispielsweise nach „*“ filtern, werden Ergebnisse zurückgegeben, die ein Sternchen sind. Das Sternchen wird in diesem Fall nicht als Platzhalter behandelt. Die Operatoren OR und NOT werden auch als Literalzeichenfolgen behandelt, wenn sie in doppelte Anführungszeichen eingeschlossen sind.

Filtern nach Booleschen Werten

Beim Filtern nach einem Booleschen Wert werden Ihnen möglicherweise die folgenden Filteroptionen angezeigt:

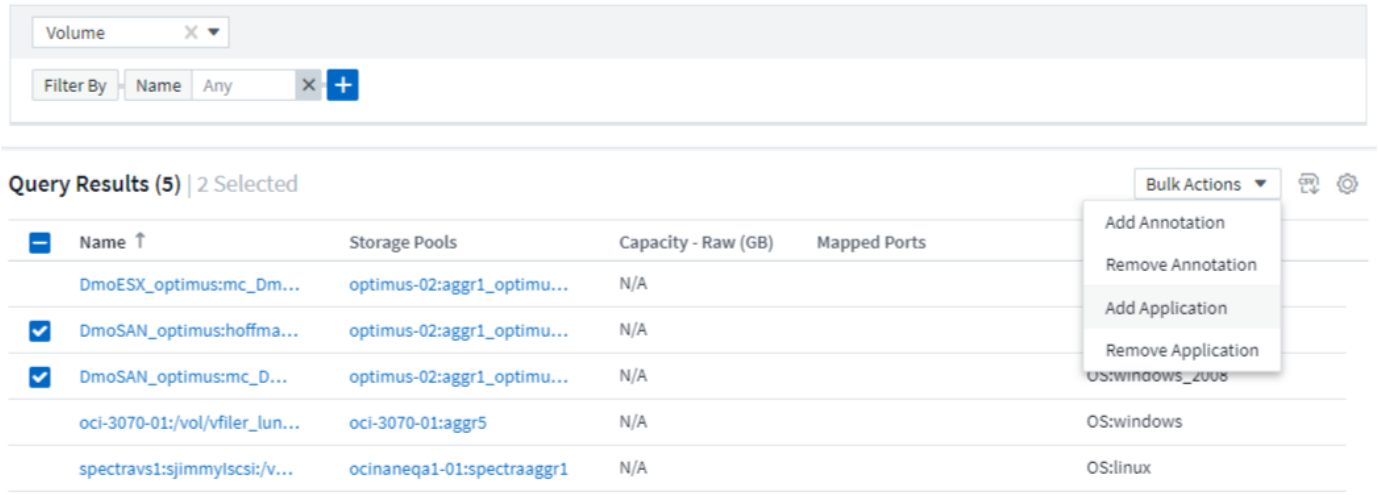
- **Beliebig**: Dies gibt *alle* Ergebnisse zurück, einschließlich der Ergebnisse, die auf „Ja“, „Nein“ oder gar nicht festgelegt sind.
- **Ja**: Gibt nur „Ja“-Ergebnisse zurück. Beachten Sie, dass DII in den meisten Tabellen „Ja“ als Häkchen anzeigt. Die Werte können auf „True“, „On“ usw. gesetzt werden; DII behandelt alle diese Werte als „Yes“.
- **Nein**: Gibt nur „Nein“-Ergebnisse zurück. Beachten Sie, dass DII in den meisten Tabellen „Nein“ als „X“ anzeigt. Die Werte können auf „Falsch“, „Aus“ usw. gesetzt werden; DII behandelt alle diese Werte als „Nein“.
- **Keine**: Gibt nur Ergebnisse zurück, bei denen der Wert überhaupt nicht festgelegt wurde. Auch als „Null“-Werte bezeichnet.

Was mache ich jetzt, da ich Abfrageergebnisse habe?

Durch Abfragen können auf einfache Weise Anmerkungen hinzugefügt oder Anwendungen Assets zugewiesen werden. Beachten Sie, dass Sie Ihren Inventarressourcen (Festplatte, Speicher usw.) nur Anwendungen oder Anmerkungen zuweisen können. Integrationsmetriken können keine Anmerkungen oder Anwendungszuweisungen übernehmen.

Um den aus Ihrer Abfrage resultierenden Assets eine Anmerkung oder Anwendung zuzuweisen, wählen Sie

einfach das/die Asset(s) mithilfe der Kontrollkästchenspalte links in der Ergebnistabelle aus und klicken Sie dann rechts auf die Schaltfläche **Massenaktionen**. Wählen Sie die gewünschte Aktion aus, die auf die ausgewählten Assets angewendet werden soll.



Anmerkungsregeln erfordern eine Abfrage

Wenn Sie konfigurieren"Anmerkungsregeln" , jeder Regel muss eine zugrunde liegende Abfrage zugrunde liegen, mit der gearbeitet werden kann. Aber wie Sie oben gesehen haben, können Abfragen so weit oder so eng gefasst werden, wie Sie es benötigen.

Anzeigen von Abfragen

Sie können Ihre Abfragen anzeigen, um Ihre Vermögenswerte zu überwachen und die Anzeige der mit Ihren Vermögenswerten verbundenen Daten in Ihren Abfragen zu ändern.

Schritte

1. Melden Sie sich bei Ihrem Data Infrastructure Insights Mandanten an.
2. Klicken Sie auf **Abfragen** und wählen Sie **Alle Abfragen anzeigen**. Sie können die Anzeige von Abfragen wie folgt ändern:
3. Sie können Text in das Filterfeld eingeben, um nach bestimmten Abfragen zu suchen.
4. Sie können die Sortierreihenfolge der Spalten in der Abfragetabelle entweder aufsteigend (Pfeil nach oben) oder absteigend (Pfeil nach unten) ändern, indem Sie auf den Pfeil in der Spaltenüberschrift klicken.
5. Um die Größe einer Spalte zu ändern, bewegen Sie die Maus über die Spaltenüberschrift, bis ein blauer Balken angezeigt wird. Platzieren Sie die Maus über der Leiste und ziehen Sie sie nach rechts oder links.
6. Um eine Spalte zu verschieben, klicken Sie auf die Spaltenüberschrift und ziehen Sie sie nach rechts oder links.

Beachten Sie beim Durchblättern der Abfrageergebnisse, dass sich die Ergebnisse ändern können, da Data Infrastructure Insights Ihre Datensammler automatisch abfragt. Dies kann dazu führen, dass einige Elemente fehlen oder einige Elemente je nach Sortierung in der falschen Reihenfolge angezeigt werden.

Exportieren von Abfrageergebnissen in eine CSV-Datei

Sie können die Ergebnisse jeder Abfrage in eine CSV-Datei exportieren, sodass Sie die Daten analysieren oder in eine andere Anwendung importieren können.

Schritte

1. Melden Sie sich bei Data Infrastructure Insights an.
2. Klicken Sie auf **Abfragen** und wählen Sie **Alle Abfragen anzeigen**.

   Die Seite „Abfragen“ wird angezeigt.

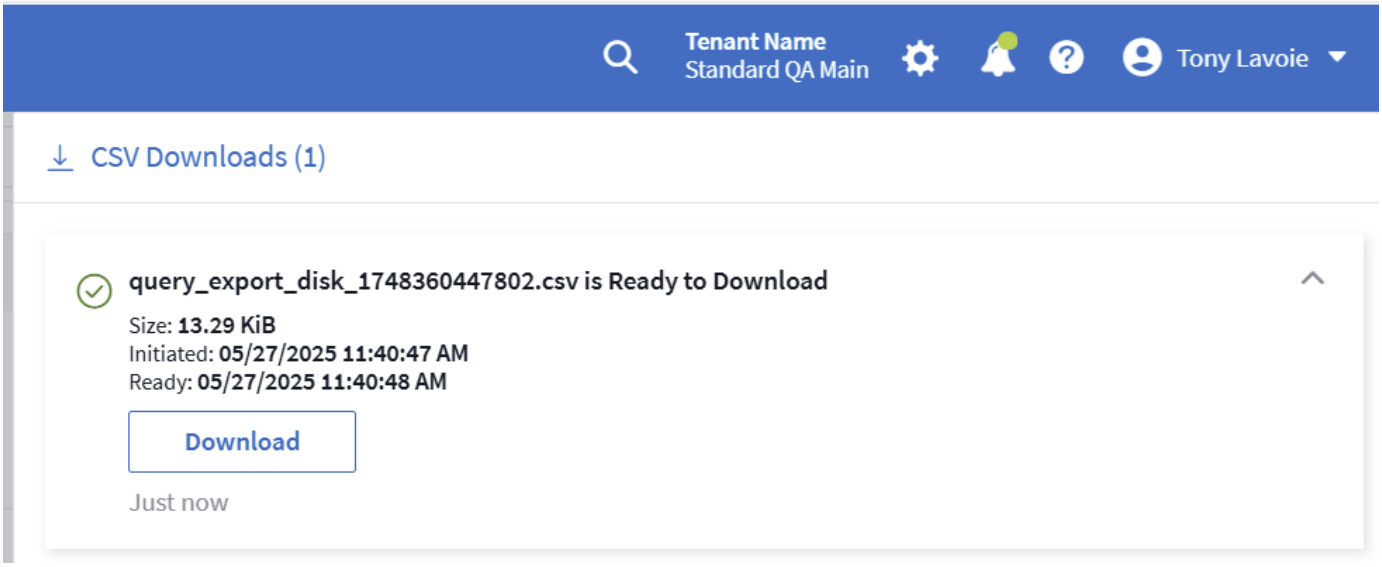
3. Klicken Sie auf eine Abfrage.
4. Klicken um die Abfrageergebnisse in eine CSV-Datei zu exportieren.

Der Export in .CSV ist auch im Menü „Drei Punkte“ in Dashboard-Tabellen-Widgets sowie in den meisten Landingpage-Tabellen verfügbar.

Asynchroner Export

Das Exportieren von Daten in das CSV-Format kann je nach der zu exportierenden Datenmenge zwischen einigen Sekunden und mehreren Stunden dauern. Data Infrastructure Insights exportiert diese Daten asynchron, sodass Sie weiterarbeiten können, während die CSV-Datei kompiliert wird.

Zeigen Sie Ihre CSV-Exporte an und laden Sie sie herunter, indem Sie in der oberen rechten Symbolleiste das Glockensymbol auswählen.



Die exportierten Daten spiegeln die aktuelle Filterung, die angezeigten Spalten und Spaltennamen wider.

Kommas in Asset-Namen

Hinweis: Wenn in einem Asset-Namen ein Komma erscheint, wird der Name beim Export in Anführungszeichen gesetzt, wodurch der Asset-Name und das richtige CSV-Format erhalten bleiben.

Zeitformat oder kein Zeitformat?

Wenn Sie eine exportierte CSV-Datei mit Excel öffnen und ein Objektname oder ein anderes Feld im Format NN:NN (zwei Ziffern gefolgt von einem Doppelpunkt und zwei weiteren Ziffern) vorliegt, interpretiert Excel diesen Namen manchmal als Zeitformat statt als Textformat. Dies kann dazu führen, dass Excel in diesen Spalten falsche Werte anzeigt. Beispielsweise würde ein Objekt mit dem Namen „81:45“ in Excel als „81:45:00“ angezeigt.

Um dieses Problem zu umgehen, importieren Sie die CSV-Datei mit den folgenden Schritten in Excel:

1. Öffnen Sie ein neues Blatt in Excel.
2. Wählen Sie auf der Registerkarte „Daten“ die Option „Aus Text“.
3. Suchen Sie die gewünschte CSV-Datei und klicken Sie auf „Importieren“.
4. Wählen Sie im Importassistenten „Getrennt“ und klicken Sie auf „Weiter“.
5. Wählen Sie „Komma“ als Trennzeichen und klicken Sie auf „Weiter“.
6. Wählen Sie die gewünschten Spalten aus und wählen Sie „Text“ als Spaltendatenformat.
7. Klicken Sie auf Fertig stellen.

   Ihre Objekte sollten in Excel im richtigen Format angezeigt werden.

Ändern oder Löschen einer Abfrage

Sie können die mit einer Abfrage verknüpften Kriterien ändern, wenn Sie die Suchkriterien für die abgefragten Assets ändern möchten.

Ändern einer Abfrage

Schritte

1. Klicken Sie auf **Erkunden** und wählen Sie **Alle Metrikabfragen** aus.

   Die Seite „Abfragen“ wird angezeigt.

2. Klicken Sie auf den Abfragenamen
3. Um der Abfrage ein Kriterium hinzuzufügen, klicken Sie auf das Spaltensymbol und wählen Sie eine Metrik oder ein Attribut aus der Liste aus.

Wenn Sie alle erforderlichen Änderungen vorgenommen haben, führen Sie einen der folgenden Schritte aus:

- Klicken Sie auf die Schaltfläche **Speichern**, um die Abfrage unter dem ursprünglich verwendeten Namen zu speichern.
- Klicken Sie auf das Dropdown-Menü neben der Schaltfläche **Speichern** und wählen Sie **Speichern unter**, um die Abfrage unter einem anderen Namen zu speichern. Dadurch wird die ursprüngliche Abfrage nicht überschrieben.
- Klicken Sie auf das Dropdown-Menü neben der Schaltfläche **Speichern** und wählen Sie **Umbenennen**, um den ursprünglich verwendeten Abfragenamen zu ändern. Dadurch wird die ursprüngliche Abfrage überschrieben.
- Klicken Sie auf das Dropdown-Menü neben der Schaltfläche **Speichern** und wählen Sie **Änderungen verwerfen**, um die Abfrage auf die zuletzt gespeicherten Änderungen zurückzusetzen.

Löschen einer Abfrage

Um eine Abfrage zu löschen, klicken Sie auf **Abfragen**, wählen Sie **Alle Abfragen anzeigen** und führen Sie einen der folgenden Schritte aus:

1. Klicken Sie auf das Drei-Punkte-Menü rechts neben der Abfrage und klicken Sie auf **Löschen**.
2. Klicken Sie auf den Abfragenamen und wählen Sie **Löschen** aus dem Dropdown-Menü **Speichern**.

Zuweisen mehrerer Anwendungen zu oder Entfernen mehrerer Anwendungen von Assets

Sie können mehrere"Anwendungen" Sie können mehrere Anwendungen mithilfe einer Abfrage zu Assets hinzufügen oder daraus entfernen, anstatt sie manuell zuweisen oder entfernen zu müssen.

Mit diesen Schritten können Sie hinzufügen oder entfernen"Anmerkungen" auf die gleiche Weise.

Bevor Sie beginnen

Sie müssen bereits eine Abfrage erstellt haben, die alle Assets findet, die Sie bearbeiten möchten.

Schritte

1. Klicken Sie auf **Erkunden** und wählen Sie **Metrikabfragen** aus.

   Die Seite „Abfragen“ wird angezeigt.

2. Klicken Sie auf den Namen der Abfrage, die die Assets findet.

   Die Liste der mit der Abfrage verknüpften Assets wird angezeigt.

3. Wählen Sie die gewünschten Assets in der Liste aus oder klicken Sie auf das obere Kontrollkästchen, um „Alle“ auszuwählen.

   Das Dropdown-Menü „Massenaktionen“ wird angezeigt.

4. Um den ausgewählten Assets eine Anwendung hinzuzufügen, klicken Sie auf Massenaktionen und wählen Sie **Anwendung hinzufügen**.
5. Wählen Sie eine oder mehrere Anwendungen aus.

   Sie können mehrere Anwendungen für Hosts, interne Volumes, Qtrees und virtuelle Maschinen auswählen. Für ein Volume oder eine Freigabe können Sie jedoch nur eine Anwendung auswählen.

6. Klicken Sie auf **Speichern**.
7. Um eine den Assets zugewiesene Anwendung zu entfernen, klicken Sie auf „Massenaktionen“ und wählen Sie „Anwendung entfernen“ aus.
8. Wählen Sie die Anwendung(en) aus, die Sie entfernen möchten.
9. Klicken Sie auf **Löschen**.

Alle neuen Anwendungen, die Sie zuweisen, überschreiben alle Anwendungen auf dem Asset, die von einem anderen Asset abgeleitet wurden. Beispielsweise erben Volumes Anwendungen von Hosts, und wenn einem Volume neue Anwendungen zugewiesen werden, hat die neue Anwendung Vorrang vor der abgeleiteten

Anwendung.

Nachdem Sie bei einer Massenhinzufügungsaktion auf *Speichern* oder bei einer Massenlöschaktion auf *Entfernen* geklickt haben, werden Sie von Data Infrastructure Insights darüber informiert, dass die Aktion einige Zeit in Anspruch nehmen wird. Sie können diese Meldung ignorieren; die Aktion wird im Hintergrund fortgesetzt.

In Umgebungen mit einer großen Menge verwandter Assets kann die Vererbung von Anwendungszuweisungen zu diesen Assets mehrere Minuten dauern. Bitte rechnen Sie mit einer längeren Vererbungszeit, wenn Sie über viele zusammenhängende Vermögenswerte verfügen.

Tabellenwerte kopieren

Sie können Werte in Tabellen in die Zwischenablage kopieren, um sie in Suchfeldern oder anderen Anwendungen zu verwenden.

Informationen zu diesem Vorgang

Es gibt zwei Methoden, mit denen Sie Werte aus Tabellen oder Abfrageergebnissen in die Zwischenablage kopieren können.

Schritte

1. Methode 1: Markieren Sie den gewünschten Text mit der Maus, kopieren Sie ihn und fügen Sie ihn in Suchfelder oder andere Anwendungen ein.
2. Methode 2: Bewegen Sie bei Einzelwertfeldern den Mauszeiger über das Feld und klicken Sie auf das angezeigte Zwischenablagesymbol. Der Wert wird zur Verwendung in Suchfeldern oder anderen Anwendungen in die Zwischenablage kopiert.

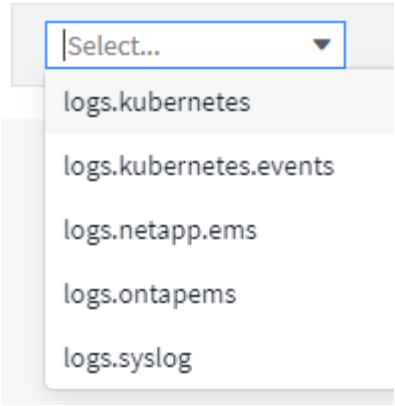
   Beachten Sie, dass mit dieser Methode nur Werte kopiert werden können, die Links zu Assets sind. Nur Felder, die einzelne Werte enthalten (also keine Listen sind), verfügen über das Kopiersymbol.

Protokoll-Explorer

Der Data Infrastructure Insights Log Explorer ist ein leistungsstarkes Tool zum Abfragen von Systemprotokollen. Zusätzlich zur Unterstützung bei Untersuchungen können Sie auch eine Protokollabfrage in einem Monitor speichern, um Warnungen bereitzustellen, wenn diese bestimmten Protokollauslöser aktiviert werden.

Um mit der Untersuchung der Protokolle zu beginnen, klicken Sie auf **Protokollabfragen > +Neue Protokollabfrage**.

Wählen Sie ein verfügbares Protokoll aus der Liste aus.

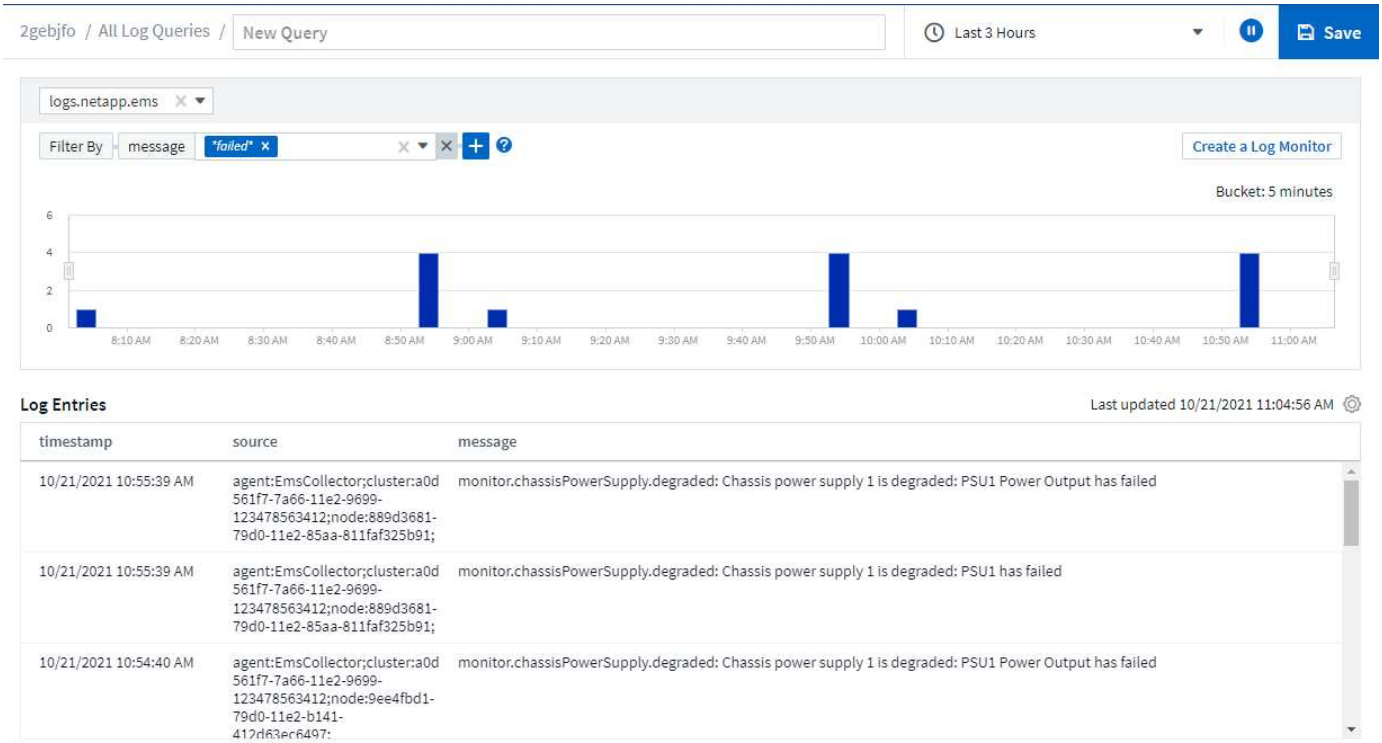


Die für die Abfrage verfügbaren Protokolltypen können je nach Umgebung variieren. Im Laufe der Zeit können weitere Protokolltypen hinzugefügt werden.

Sie können Filter setzen, um die Ergebnisse der Abfrage weiter zu verfeinern. Um beispielsweise alle Protokollmeldungen zu finden, die einen Fehler anzeigen, legen Sie einen Filter für *Meldungen* fest, die das Wort „fehlgeschlagen“ enthalten.

Sie können mit der Eingabe des gewünschten Textes in das Filterfeld beginnen. Data Infrastructure Insights fordert Sie während der Eingabe auf, eine Platzhaltersuche mit der Zeichenfolge zu erstellen.

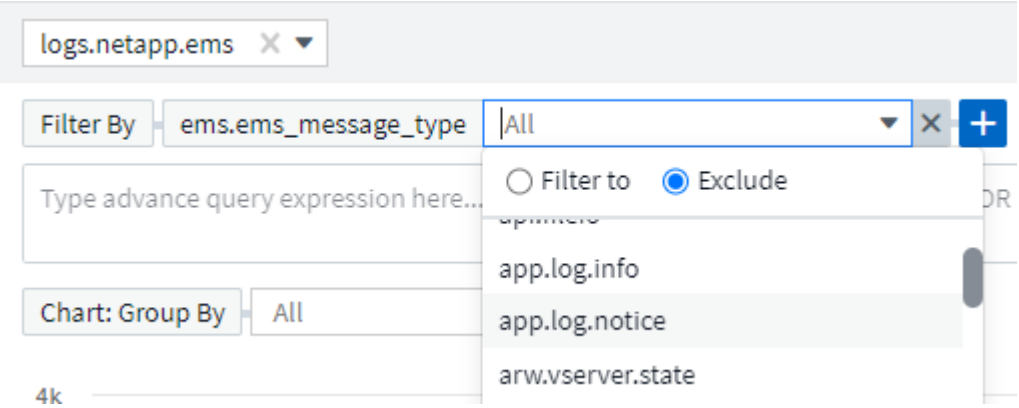
Die Ergebnisse werden in einem Diagramm angezeigt, das die Anzahl der Protokollinstanzen in jedem angezeigten Zeitraum zeigt. Unter dem Diagramm befinden sich die Protokolleinträge selbst. Das Diagramm und die Einträge werden basierend auf dem ausgewählten Zeitraum automatisch aktualisiert.



Filtern

Einschließen / Ausschließen

Beim Filtern der Protokolle können Sie wählen, ob Sie die eingegebenen Zeichenfolgen **einschließen** (d. h. „Filtern nach“) oder **ausschließen** möchten. Ausgeschlossene Zeichenfolgen werden im vervollständigten Filter als „NOT <string>“ angezeigt.



Filter, die auf Platzhaltern oder Ausdrücken basieren (z. B. NICHT, ODER, „Keine“ usw.), werden im Filterfeld dunkelblau angezeigt. Elemente, die Sie direkt aus der Liste auswählen, werden hellblau angezeigt.

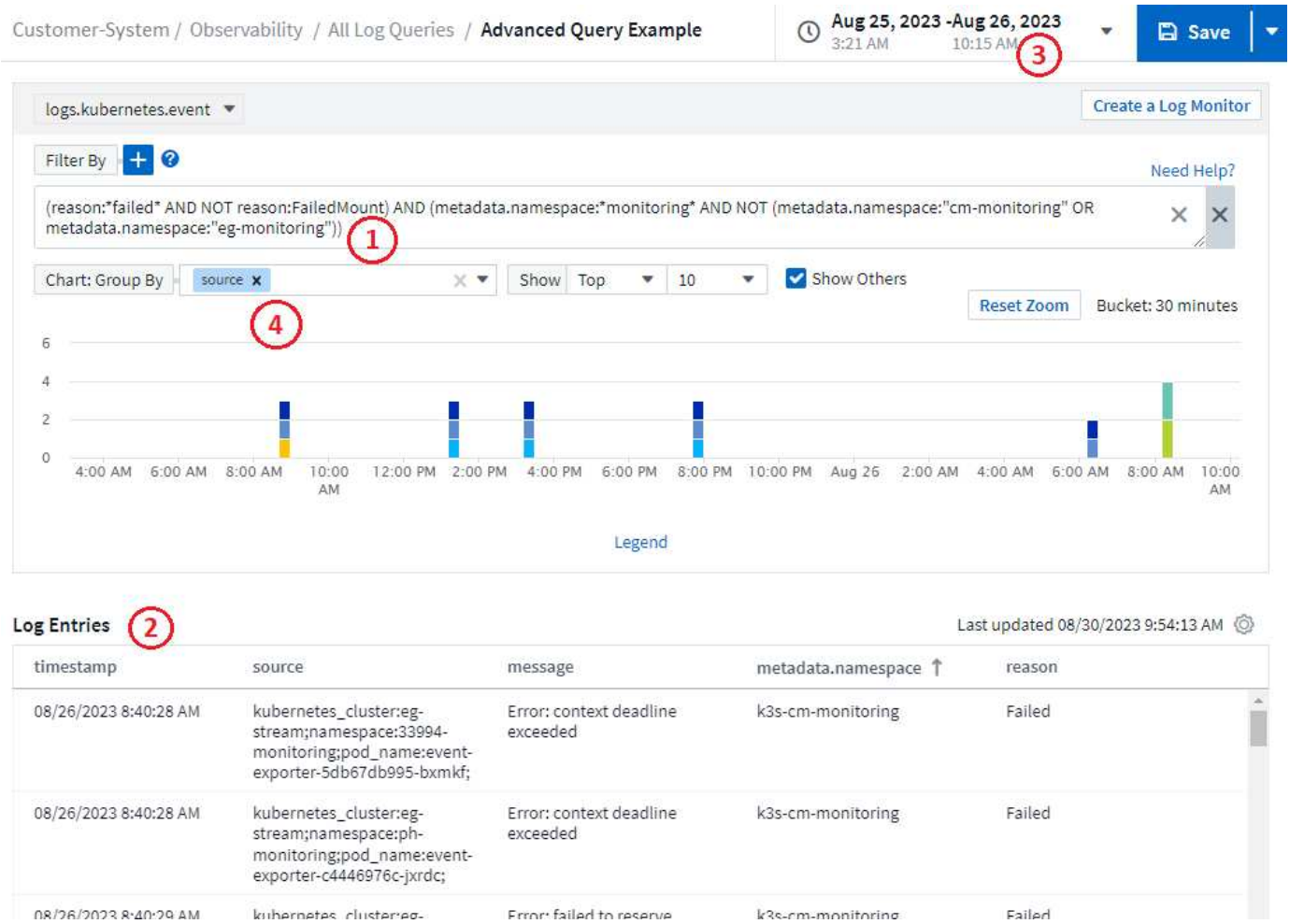
Sie können jederzeit auf „Protokollmonitor erstellen“ klicken, um einen neuen Monitor basierend auf dem aktuellen Filter zu erstellen.

Erweiterte Filterung

Wenn Sie in Abfragen oder Dashboard-Widgets nach Text oder Listenwerten filtern, wird Ihnen beim Eintippen die Option angezeigt, einen **Platzhalterfilter** basierend auf dem aktuellen Text zu erstellen. Wenn Sie diese Option auswählen, werden alle Ergebnisse zurückgegeben, die mit dem Platzhalterausdruck übereinstimmen. Sie können auch Ausdrücke mit NOT, AND oder OR erstellen oder die Option „Keine“ auswählen, um nach Nullwerten zu filtern.

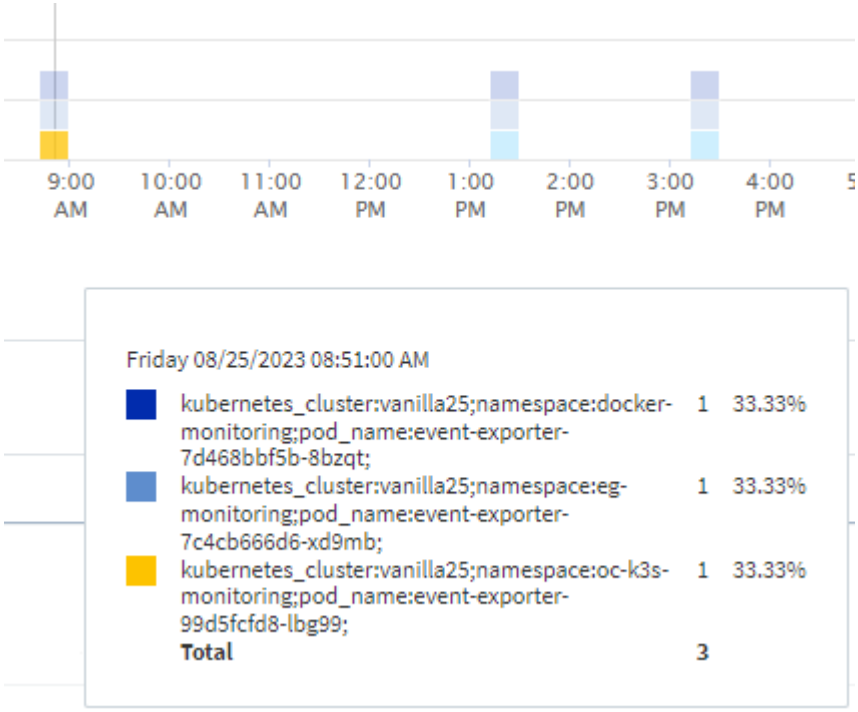
Denken Sie daran, Ihre Abfrage frühzeitig und häufig zu speichern, während Sie Ihre Filterung erstellen. Bei der erweiterten Abfrage handelt es sich um eine Zeichenfolgeneingabe in „freier Form“, und beim Erstellen können Analysefehler auftreten.

Sehen Sie sich dieses Bildschirmbild an, das gefilterte Ergebnisse für eine erweiterte Abfrage des *logs.kubernetes.event*-Protokolls zeigt. Auf dieser Seite ist eine Menge los, was unter dem Bild erklärt wird:



1. Diese erweiterte Abfragezeichenfolge filtert nach Folgendem:
   - Filtern Sie nach Protokolleinträgen mit einem *Grund*, der das Wort „fehlgeschlagen“ enthält, aber nicht nach Einträgen mit dem spezifischen Grund „FailedMount“.
   - Schließen Sie alle Einträge ein, die auch einen *metadata.namespace* mit dem Wort „monitoring“ enthalten, schließen Sie jedoch die spezifischen Namespaces „cm-monitoring“ oder „eg-monitoring“ aus.

     Beachten Sie, dass im obigen Fall sowohl „cm-monitoring“ als auch „eg-monitoring“ einen Bindestrich („-“) enthalten. Daher müssen die Zeichenfolgen in Anführungszeichen gesetzt werden, da sonst ein Analysefehler angezeigt wird. Zeichenfolgen, die keine Bindestriche, Leerzeichen usw. enthalten, müssen nicht in Anführungszeichen gesetzt werden. Versuchen Sie im Zweifelsfall, die Zeichenfolge in Anführungszeichen zu setzen.
2. Die Ergebnisse des aktuellen Filters, einschließlich aller „Filtern nach“-Werte UND des erweiterten Abfragefilters, werden in der Ergebnisliste angezeigt. Die Liste kann nach allen angezeigten Spalten sortiert werden. Um zusätzliche Spalten anzuzeigen, wählen Sie das Zahnradsymbol aus.
3. Das Diagramm wurde vergrößert, um nur Protokollergebnisse anzuzeigen, die innerhalb eines bestimmten Zeitrahmens aufgetreten sind. Der hier angezeigte Zeitbereich spiegelt die aktuelle Zoomstufe wider. Wählen Sie die Schaltfläche *Zoom zurücksetzen*, um die Zoomstufe wieder auf den aktuellen Data Infrastructure Insights -Zeitbereich zurückzusetzen.
4. Die Diagrammergebnisse wurden nach dem Feld *Quelle* gruppiert. Das Diagramm zeigt die Ergebnisse in jeder Spalte, gruppiert nach Farben. Wenn Sie mit der Maus über eine Spalte im Diagramm fahren, werden einige Details zu den jeweiligen Einträgen angezeigt.



Filter verfeinern

Sie können Ihren Filter folgendermaßen verfeinern:

Filter	Was es bewirkt
* (Sternchen)	ermöglicht Ihnen die Suche nach allem
? (Fragezeichen)	ermöglicht die Suche nach einer bestimmten Anzahl von Zeichen
ODER	ermöglicht Ihnen die Angabe mehrerer Entitäten
NICHT	ermöglicht es Ihnen, Text aus den Suchergebnissen auszuschließen
Keiner	sucht in allen Feldern nach NULL-Werten
Nicht *	sucht nach NULL-Werten in *Nur-Text*-Feldern

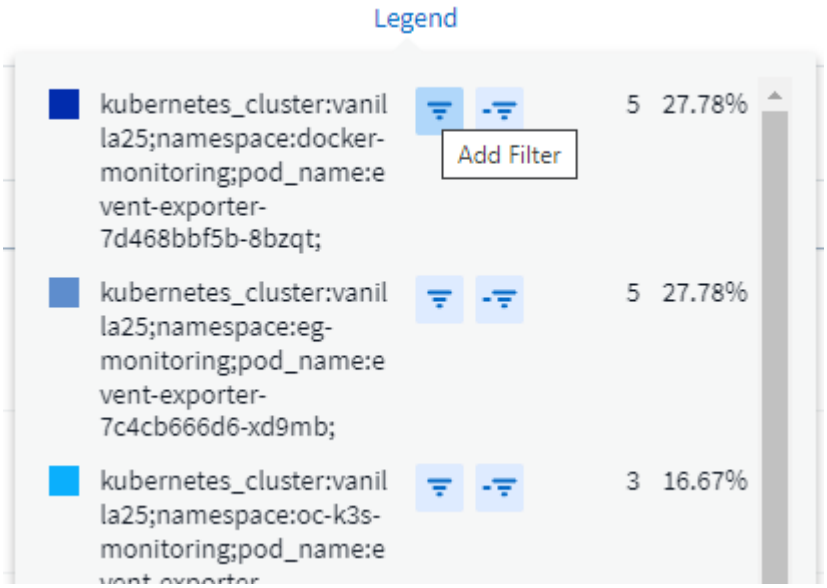
Wenn Sie eine Filterzeichenfolge in doppelte Anführungszeichen setzen, behandelt Insight alles zwischen dem ersten und letzten Anführungszeichen als exakte Übereinstimmung. Alle Sonderzeichen oder Operatoren innerhalb der Anführungszeichen werden als Literale behandelt. Wenn Sie beispielsweise nach „*“ filtern, werden Ergebnisse zurückgegeben, die ein Sternchen sind. Das Sternchen wird in diesem Fall nicht als Platzhalter behandelt. Die Operatoren OR und NOT werden auch als Literalzeichenfolgen behandelt, wenn sie in doppelte Anführungszeichen eingeschlossen sind.

Sie können einen einfachen Filter mit einem erweiterten Abfragefilter kombinieren. Der resultierende Filter ist ein „UND“ der beiden.

Die Chart-Legende

Auch die *Legende* unter dem Diagramm hält einige Überraschungen bereit. Für jedes in der Legende angezeigte Ergebnis (basierend auf dem aktuellen Filter) haben Sie die Möglichkeit, nur Ergebnisse für diese

Zeile anzuzeigen (Filter hinzufügen) oder alle Ergebnisse anzuzeigen, die NICHT für diese Zeile gelten (Ausschlussfilter hinzufügen). Das Diagramm und die Liste der Protokolleinträge werden aktualisiert, um die Ergebnisse basierend auf Ihrer Auswahl anzuzeigen. Um diese Filterung zu entfernen, öffnen Sie die Legende erneut und wählen Sie das [X] aus, um den legendenbasierten Filter zu löschen.

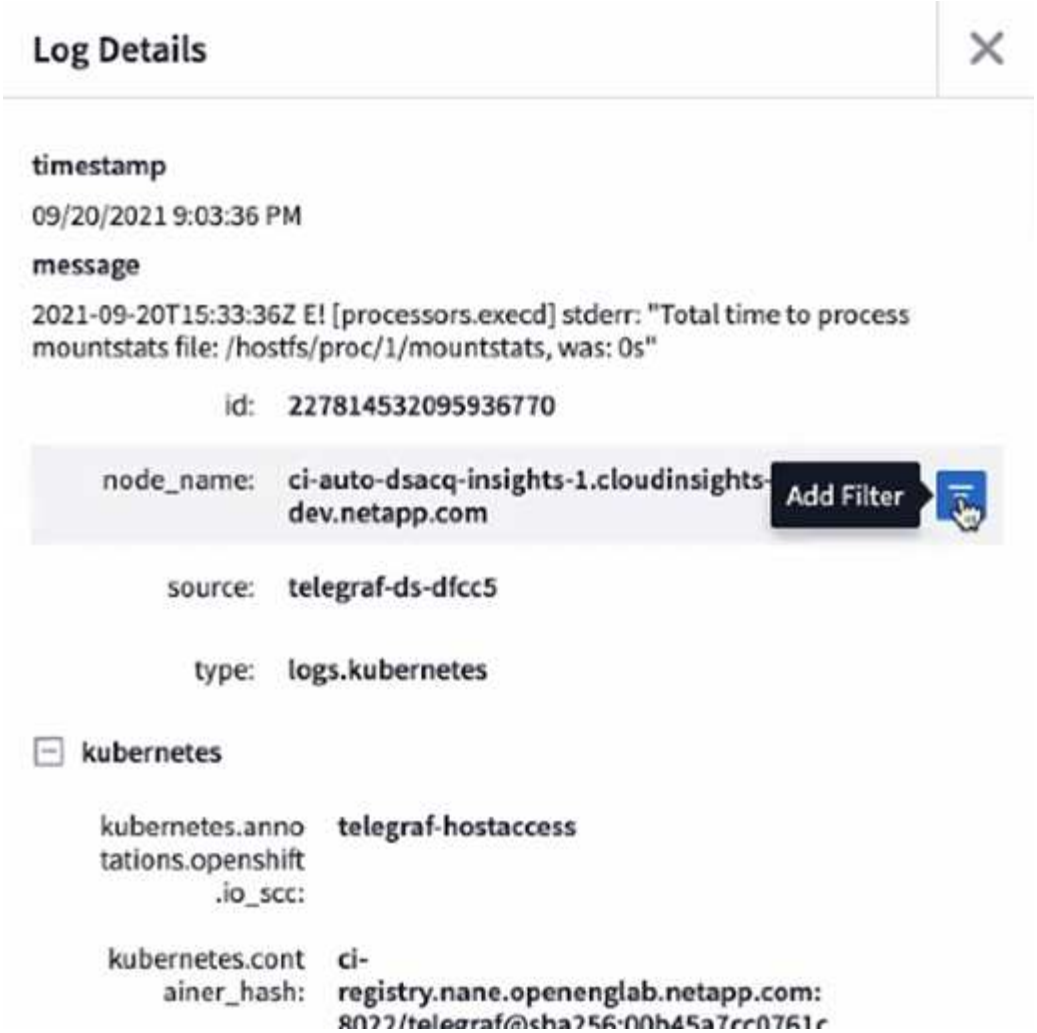


Protokolldetails

Wenn Sie irgendwo in der Liste auf einen Protokolleintrag klicken, wird ein Detailbereich für diesen Eintrag geöffnet. Hier können Sie weitere Informationen zur Veranstaltung finden.

Klicken Sie auf „Filter hinzufügen“, um das ausgewählte Feld zum aktuellen Filter hinzuzufügen. Die Liste der Protokolleinträge wird basierend auf dem neuen Filter aktualisiert.

Beachten Sie, dass einige Felder nicht als Filter hinzugefügt werden können. In diesen Fällen ist das Symbol „Filter hinzufügen“ nicht verfügbar.



Fehlerbehebung

Hier finden Sie Vorschläge zur Behebung von Problemen mit Protokollabfragen.

Problem:	Versuchen Sie Folgendes:
Ich sehe keine „Debug“-Meldungen in meiner Protokollabfrage	Debug-Protokollnachrichten werden nicht erfasst. Um die gewünschten Nachrichten zu erfassen, ändern Sie den Schweregrad der entsprechenden Nachricht auf die Ebene „Information“, „Fehler“, „Alarm“, „Notfall“ oder „Hinweis“.

Identifizieren inaktiver Geräte

Um die richtige Größe zu finden und ungenutzte Infrastruktur freizugeben, ist es entscheidend, die vorhandenen Ressourcen und deren Nutzer zu identifizieren. Sie können nicht ausgelastete Ressourcen problemlos neu zuweisen oder außer Betrieb nehmen und unnötige Käufe vermeiden.

Führen Sie die folgenden Schritte aus, um inaktive Assets zu identifizieren.

Schritte

- Navigieren Sie zu **Observability > Explore → +Neue Metrikabfrage**.
- Wählen Sie *Speicher* aus der Dropdown-Liste.
- Klicken Sie auf das Zahnrad und fügen Sie *isActive* als Spalte hinzu.

  Zeilen mit einem Häkchen sind aktiv. „X“ zeigt inaktive Geräte an.

Um inaktive Geräte zu entfernen, wählen Sie einfach die zu entfernenden Geräte aus und wählen Sie im Dropdown-Menü **Massenaktionen** die Option *Inaktive Geräte löschen*.

Einblicke

Einblicke

Mithilfe von Insights können Sie beispielsweise die Ressourcennutzung und ihre Auswirkungen auf andere Ressourcen untersuchen oder die Zeit bis zur Fertigstellung analysieren.

Es stehen zahlreiche Einblicke zur Verfügung. Navigieren Sie zu **Dashboards > Insights**, um einzutauchen. Sie können aktive Insights (aktuell auftretende Insights) auf der Hauptregisterkarte oder inaktive Insights auf der Registerkarte *Inaktive Insights* anzeigen. Inaktive Erkenntnisse sind Erkenntnisse, die zuvor aktiv waren, aber nicht mehr auftreten.

Erkenntnistypen

Gemeinsam genutzte Ressourcen unter Stress

Workloads mit hoher Auswirkung können die Leistung anderer Workloads in einer gemeinsam genutzten Ressource beeinträchtigen. Dadurch wird die gemeinsam genutzte Ressource belastet. Data Infrastructure Insights bietet Tools, mit denen Sie die Ressourcensättigung und die Auswirkungen auf Ihren Mandanten untersuchen können."Weitere Informationen"

Kubernetes-Namespaces haben nicht mehr genügend Speicherplatz

Die Einblicke in „Kubernetes-Namespaces, denen der Speicherplatz ausgeht“ geben Ihnen einen Überblick über die Workloads in Ihren Kubernetes-Namespaces, bei denen das Risiko besteht, dass ihnen der Speicherplatz ausgeht, und enthalten eine Schätzung der verbleibenden Tage, bis jeder Speicherplatz voll ist."Weitere Informationen"

ONTAP Cold Storage zurückgewinnen

Der *Reclaim ONTAP Cold Storage* Insight bietet Daten zur Kaltkapazität, zu potenziellen Kosten-/Stromeinsparungen und empfohlenen Aktionselementen für Volumes auf ONTAP Systemen."Weitere Informationen"

> Dies ist eine *Vorschau*-Funktion und kann sich im Laufe der Zeit ändern, wenn Verbesserungen vorgenommen werden. "Mehr erfahren" Informationen zu den Vorschaufunktionen von Data Infrastructure Insights .

Einblicke: Gemeinsam genutzte Ressourcen unter Druck

Workloads mit hoher Auswirkung können die Leistung anderer Workloads in einer

gemeinsam genutzten Ressource beeinträchtigen. Dadurch wird die gemeinsam genutzte Ressource belastet. Data Infrastructure Insights bietet Tools, mit denen Sie die Ressourcensättigung und die Auswirkungen auf Ihren Mandanten untersuchen können.

Terminologie

Wenn es um Arbeitsbelastung oder Ressourcenauswirkungen geht, sind die folgenden Definitionen hilfreich.

Eine **anspruchsvolle Arbeitslast** ist eine Arbeitslast, die sich derzeit auf andere Ressourcen im gemeinsam genutzten Speicherpool auswirkt. Diese Workloads führen beispielsweise zu höheren IOPS und reduzieren so die IOPS in den betroffenen Workloads. Anspruchsvolle Arbeitslasten werden manchmal als *arbeitsintensive Arbeitslasten* bezeichnet.

Eine **betroffene Arbeitslast** ist eine Arbeitslast, die von einer Arbeitslast mit hohem Verbrauch im gemeinsam genutzten Speicherpool betroffen ist. Bei diesen Workloads kommt es aufgrund der anspruchsvollen Workloads zu reduzierten IOPS und/oder einer höheren Latenz.

Beachten Sie: Wenn Data Infrastructure Insights die führende Rechenarbeitslast nicht ermittelt hat, wird das Volume oder das interne Volume selbst als Arbeitslast erkannt. Dies gilt sowohl für anspruchsvolle als auch für beeinträchtigte Arbeitslasten.

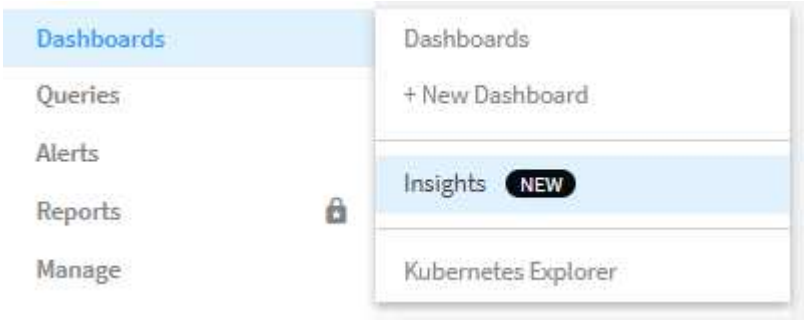
Shared Resource Saturation ist das Verhältnis der beeinflussenden IOPS zum *Basiswert*.

Baseline wird als der maximal gemeldete Datenpunkt für jede Arbeitslast in der Stunde unmittelbar vor der erkannten Sättigung definiert.

Eine **Konfliktsituation** oder **Sättigung** tritt auf, wenn festgestellt wird, dass IOPS andere Ressourcen oder Arbeitslasten im gemeinsam genutzten Speicherpool beeinträchtigen.

Anspruchsvolle Arbeitslasten

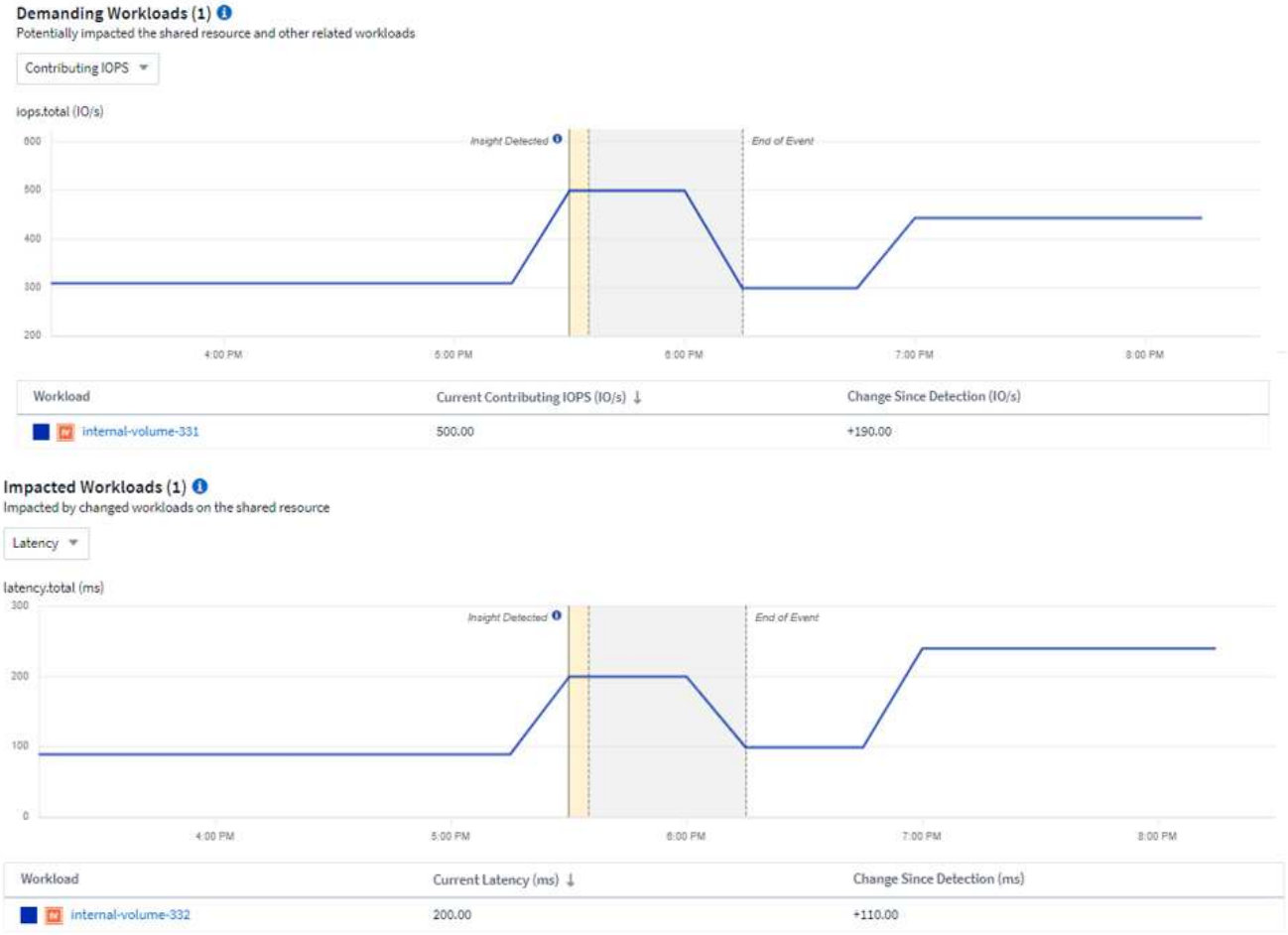
Um anspruchsvolle und beeinträchtigte Arbeitslasten in Ihren gemeinsam genutzten Ressourcen zu untersuchen, klicken Sie auf **Dashboards > Einblicke** und wählen Sie den Einblick **Gemeinsam genutzte Ressourcen unter Stress** aus.



Data Infrastructure Insights zeigt eine Liste aller Workloads an, bei denen eine Sättigung erkannt wurde. Beachten Sie, dass Data Infrastructure Insights Workloads anzeigt, bei denen mindestens eine *anspruchsvolle Ressource* **oder** *beeinträchtigte Ressource* erkannt wurde.

Klicken Sie auf eine Arbeitslast, um die Detailseite dazu anzuzeigen. Das obere Diagramm zeigt die Aktivität auf der gemeinsam genutzten Ressource (z. B. einem Speicherpool), auf der die Konflikte/Sättigungen auftreten.

Darunter befinden sich zwei Diagramme, die die *anspruchsvollen* Arbeitslasten und die Arbeitslasten zeigen, die von diesen anspruchsvollen Arbeitslasten *beeinflusst* werden.



Unter jeder Tabelle befindet sich eine Liste der Arbeitslasten und/oder Ressourcen, die den Konflikt beeinflussen oder davon betroffen sind. Wenn Sie auf eine Ressource (z. B. eine VM) klicken, wird eine Detailseite für diese Ressource geöffnet. Durch Klicken auf eine Arbeitslast wird eine Abfrageseite geöffnet, auf der die beteiligten Pods angezeigt werden. Beachten Sie: Wenn der Link eine leere Abfrage öffnet, kann dies daran liegen, dass der betroffene Pod nicht mehr Teil der aktiven Konkurrenz ist. Sie können den Zeitbereich der Abfrage ändern, um die Pod-Liste in einem größeren oder fokussierteren Zeitbereich anzuzeigen.

Was kann ich tun, um die Sättigung zu beheben?

Sie können eine Reihe von Schritten unternehmen, um die Gefahr einer Überlastung Ihres Mieters zu verringern oder auszuschließen. Diese werden durch Erweitern des Links **+Empfehlungen anzeigen** auf der Seite angezeigt. Hier sind ein paar Dinge, die Sie ausprobieren können.

- Verschieben von Verbrauchern mit hohem IOPS-Aufkommen

  Verschieben Sie die „gierigen“ Workloads in weniger gesättigte Speicherpools. Es wird empfohlen, die Ebene und Kapazität dieser Pools zu bewerten, bevor Sie die Workloads verschieben, um unnötige Kosten oder zusätzliche Konflikte zu vermeiden.

- Implementieren Sie eine Quality of Service (QoS)-Richtlinie

  Durch die Implementierung einer QoS-Richtlinie pro Arbeitslast, um sicherzustellen, dass genügend freie Ressourcen verfügbar sind, wird die Sättigung des Speicherpools verringert. Dies ist eine langfristige Lösung.

- Hinzufügen zusätzlicher Ressourcen

  Wenn die gemeinsam genutzte Ressource (z. B. der Speicherpool) den IOPS-Sättigungspunkt erreicht hat, können Sie durch Hinzufügen weiterer oder schnellerer Festplatten zum Pool sicherstellen, dass genügend freie Ressourcen zur Verfügung stehen, um die Sättigung zu verringern.

Abschließend können Sie auf **Insight-Link kopieren** klicken, um die Seiten-URL in die Zwischenablage zu kopieren und sie einfacher mit Kollegen zu teilen.

Einblicke: Kubernetes-Namespaces haben nicht mehr genügend Speicherplatz

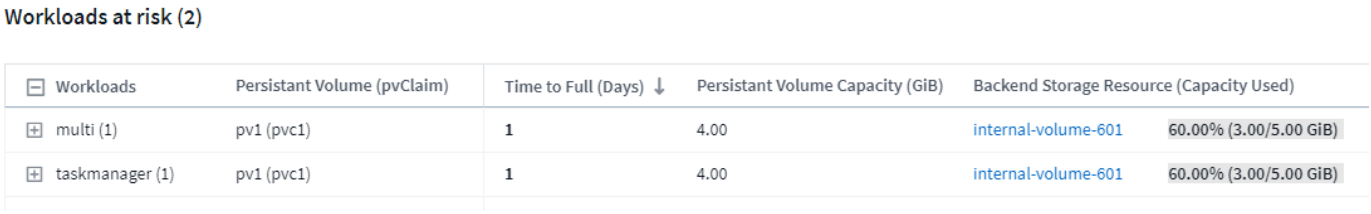
Es ist nie eine gute Situation, wenn auf Ihrem Mandanten der Speicherplatz ausgeht. Mithilfe von Data Infrastructure Insights können Sie vorhersagen, wie viel Zeit Ihnen bleibt, bevor die persistenten Kubernetes-Volumes voll sind.

Der Einblick „Kubernetes-Namespaces laufen Gefahr, nicht mehr genügend Speicherplatz zu haben“ bietet Ihnen einen Überblick über die Workloads in Ihren Kubernetes-Namespaces, bei denen das Risiko besteht, dass der Speicherplatz knapp wird, und enthält eine Schätzung der verbleibenden Tage, bis jedes persistente Volume voll ist.

Sie können diesen Insight anzeigen, indem Sie zu **Dashboards > Insights** navigieren.

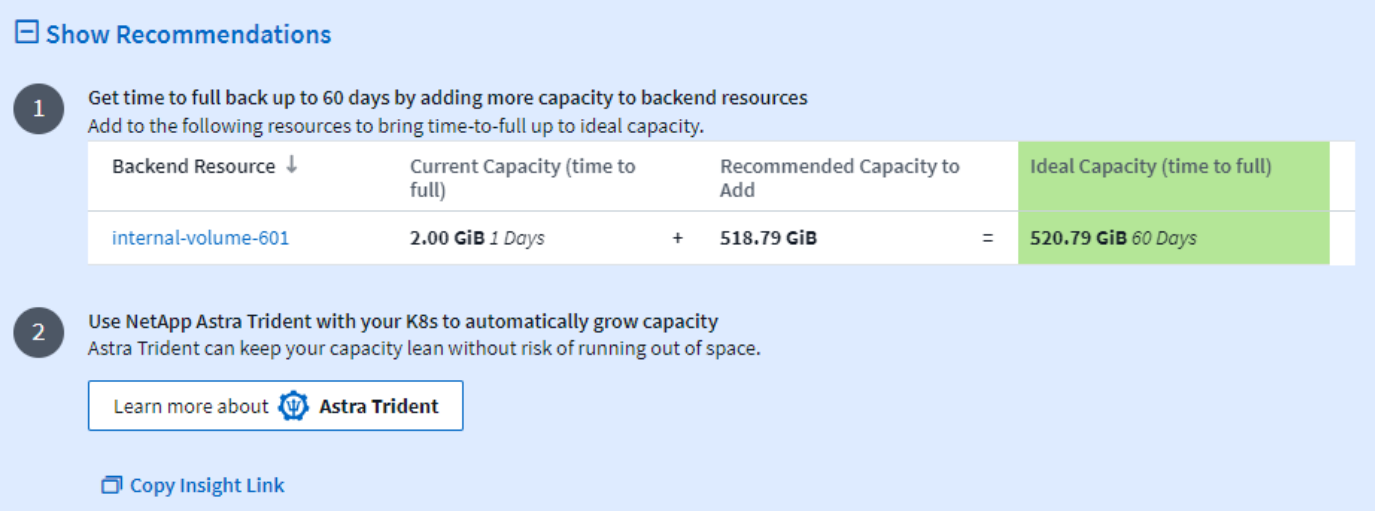
Klicken Sie auf eine Arbeitslast, um eine Detailseite für den Insight zu öffnen. Auf dieser Seite sehen Sie ein Diagramm mit den Trends der Arbeitslastkapazität sowie eine Tabelle mit den folgenden Informationen:

- Name der Arbeitslast
- Betroffen ist das dauerhafte Volume
- Voraussichtliche Zeit bis zur Fertigstellung in Tagen
- Persistente Volume-Kapazität
- Betroffen ist die Back-End-Speicherressource, wobei die aktuelle Kapazität im Vergleich zur Gesamtkapazität genutzt wird. Durch Klicken auf diesen Link wird die detaillierte Zielseite für das Backend-Volume geöffnet.



Was kann ich tun, wenn mir der Speicherplatz ausgeht?

Klicken Sie auf der Insight-Seite auf **+Empfehlungen anzeigen**, um mögliche Lösungen anzuzeigen. Die einfachste Option bei Speicherplatzmangel besteht immer darin, mehr Kapazität hinzuzufügen. Data Infrastructure Insights zeigt Ihnen die optimale Kapazität an, die Sie hinzufügen müssen, um die Zeit bis zur vollständigen Belegung auf eine Zielvorgabe von 60 Tagen zu erhöhen. Darüber hinaus werden auch andere Empfehlungen angezeigt.



Hier können Sie auch bequem einen Link zu diesem Insight kopieren, die Seite mit einem Lesezeichen versehen oder sie einfach mit Ihrem Team teilen.

Einblicke: ONTAP Cold Storage zurückgewinnen

Der *Reclaim ONTAP Cold Storage* Insight bietet Daten zur Kaltkapazität, zu potenziellen Kosten-/Stromeinsparungen und empfohlenen Aktionselementen für Volumes auf ONTAP Systemen.

Um diese Insights anzuzeigen, navigieren Sie zu **Dashboards > Insights** und werfen Sie einen Blick auf den Insight „Reclaim ONTAP Cold Storage“. Beachten Sie, dass dieser Insight betroffene Speicher nur auflistet, wenn Data Infrastructure Insights Cold Storage erkannt hat. Andernfalls wird die Meldung „Entwarnung“

angezeigt.

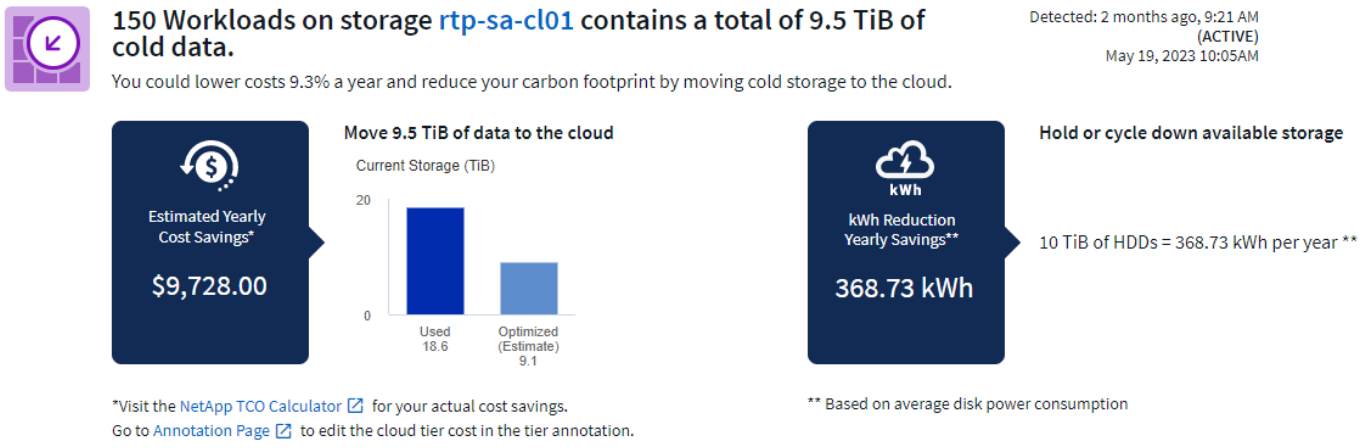
Beachten Sie, dass Kältedaten, die jünger als 30 Tage sind, nicht angezeigt werden.

Reclaim ONTAP Cold Storage (3)

Description	Cold data storage(TiB)	Workloads with cold data	Detected ↓
0.30 TiB of cold data on storage rtp-sa-cl04	0.30	45	an hour ago
1.22 TiB of cold data on storage umeng-aff300-01-02	1.22	84	16 days ago
11.62 TiB of cold data on storage rtp-sa-cl01	11.62	171	16 days ago

Die Insight-Beschreibung gibt einen schnellen Hinweis auf die Menge der als „kalt“ erkannten Daten und auf welchem Speicher sich diese Daten befinden. Die Tabelle enthält außerdem eine Zählung der Workloads mit kalten Daten.

Wenn Sie einen Insight aus der Liste auswählen, wird eine Seite mit weiteren Details geöffnet, darunter Empfehlungen zum Verschieben von Daten in die Cloud oder zum Herunterfahren unisierter Datenträger sowie geschätzte Kosten- und Energieeinsparungen, die Sie möglicherweise durch die Umsetzung dieser Empfehlungen erzielen könnten. Die Seite bietet sogar einen praktischen Link zu"TCO-Rechner von NetApp" Sie können also mit den Zahlen experimentieren.



Empfehlungen

Erweitern Sie auf der Insight-Seite die **Empfehlungen**, um die folgenden Optionen zu erkunden:

- Verschieben Sie ungenutzte Workloads (Zombies) auf eine kostengünstigere Speicherebene (HDD).

  Suchen Sie mithilfe der Zombie-Flagge, des Cold Storage und der Anzahl der Tage die kälteste und größte Datenmenge und verschieben Sie die Arbeitslast auf eine kostengünstigere Speicherebene (z. B. einen Speicherpool mit Festplattenspeicher). Eine Arbeitslast wird als „Zombie“ betrachtet, wenn sie 30 Tage oder länger keine nennenswerten E/A-Anfragen erhalten hat.

- Löschen Sie nicht verwendete Workloads

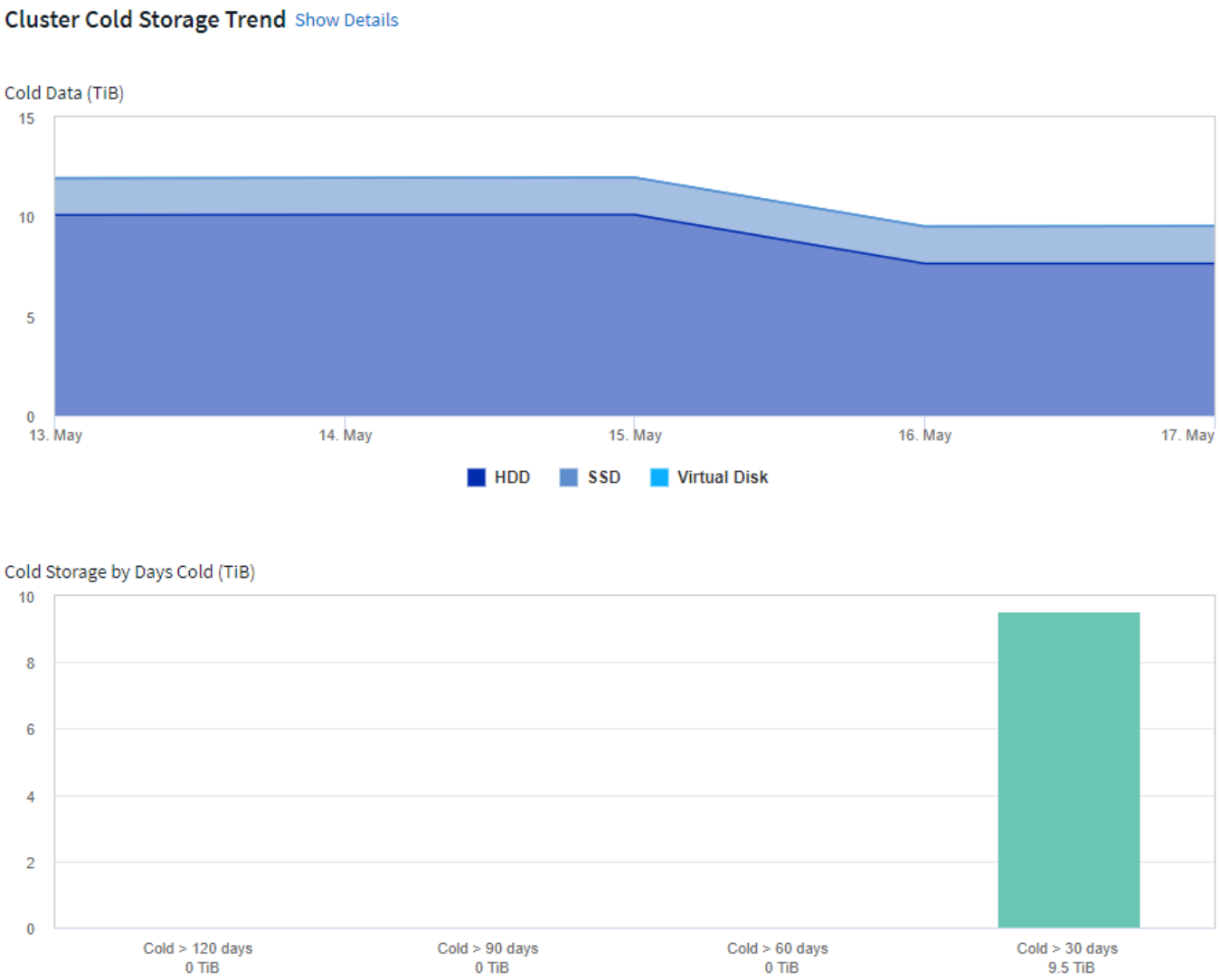
  Überprüfen Sie, welche Workloads nicht verwendet werden, und ziehen Sie in Erwägung, sie zu archivieren oder aus dem Speichersystem zu entfernen.

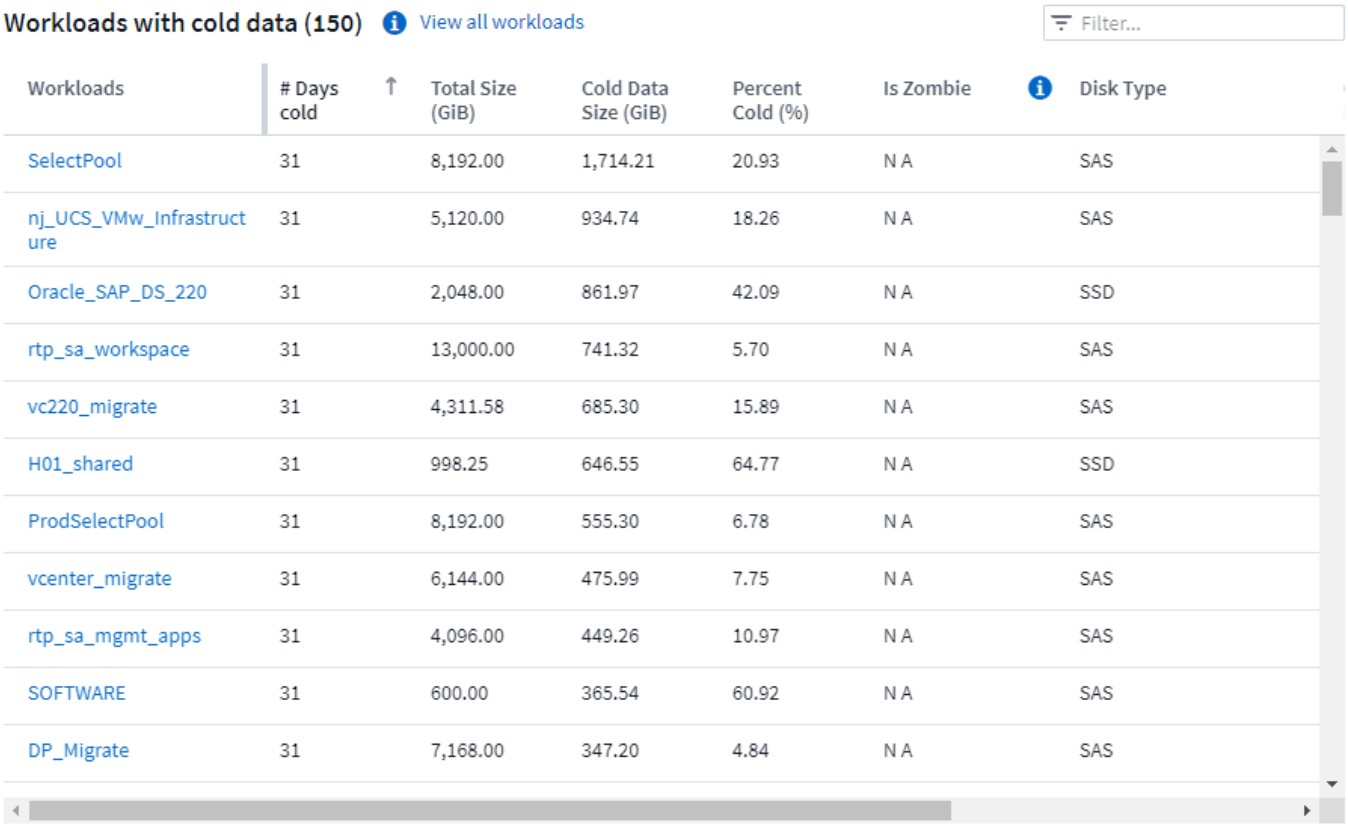
- Ziehen Sie die Fabric Pool-Lösung von NetApp in Betracht

NetApps"Fabric Pool-Lösung" verteilt kalte Daten automatisch auf kostengünstigen Cloud-Speicher und erhöht so die Effizienz Ihrer Leistungsebene und bietet Remote-Datenschutz.

Visualisieren und erkunden

Die Diagramme und Tabellen liefern zusätzliche Trendinformationen und ermöglichen Ihnen, die einzelnen Arbeitslasten genauer zu untersuchen.





Workloads with cold data (150) View all workloads

Filter...

Workloads	# Days cold	Total Size (GiB)	Cold Data Size (GiB)	Percent Cold (%)	Is Zombie	Disk Type
SelectPool	31	8,192.00	1,714.21	20.93	N A	SAS
nj_UCS_VMw_Infrastructure	31	5,120.00	934.74	18.26	N A	SAS
Oracle_SAP_DS_220	31	2,048.00	861.97	42.09	N A	SSD
rtp_sa_workspace	31	13,000.00	741.32	5.70	N A	SAS
vc220_migrate	31	4,311.58	685.30	15.89	N A	SAS
H01_shared	31	998.25	646.55	64.77	N A	SSD
ProdSelectPool	31	8,192.00	555.30	6.78	N A	SAS
vcenter_migrate	31	6,144.00	475.99	7.75	N A	SAS
rtp_sa_mgmt_apps	31	4,096.00	449.26	10.97	N A	SAS
SOFTWARE	31	600.00	365.54	60.92	N A	SAS
DP_Migrate	31	7,168.00	347.20	4.84	N A	SAS

Monitore und Warnungen

Alarmierung mit Monitoren

Konfigurieren Sie Monitore, um Leistungsschwellenwerte, Protokollereignisse und Anomalien in Ihren Infrastrukturressourcen zu verfolgen. Erstellen Sie benutzerdefinierte Warnungen für Kennzahlen wie Schreiblatenz des Knotens, Speicherkapazität oder Anwendungsleistung und erhalten Sie Benachrichtigungen, wenn diese Bedingungen erfüllt sind.

Mithilfe von Monitoren können Sie Schwellenwerte für Metriken festlegen, die von „Infrastruktur“-Objekten wie Speicher, VM, EC2 und Ports generiert werden, sowie für „Integration“-Daten, wie sie beispielsweise für Kubernetes, erweiterte ONTAP -Metriken und Telegraf-Plugins erfasst werden. Diese *metrischen* Monitore warnen Sie, wenn Warnschwellen oder kritische Schwellenwerte überschritten werden.

Sie können auch Monitore erstellen, um Warnungen auf Warn-, kritischer oder informativer Ebene auszulösen, wenn bestimmte *Protokollereignisse* erkannt werden.

Data Infrastructure Insights bietet eine Reihe von"Systemdefinierte Monitore" auch basierend auf Ihrer Umgebung.

Best Practice für die Sicherheit

Die Warnmeldungen von Data Infrastructure Insights sollen Datenpunkte und Trends zu Ihrem Mandanten hervorheben. Außerdem können Sie mit Data Infrastructure Insights eine beliebige gültige E-Mail-Adresse als Warnmeldungsempfänger eingeben. Wenn Sie in einer sicheren Umgebung arbeiten, achten Sie besonders

darauf, wer die Benachrichtigung erhält oder anderweitig Zugriff auf die Warnung hat.

Metrik- oder Protokollmonitor?

1. Klicken Sie im Menü „Data Infrastructure Insights“ auf **Warnungen > Monitore verwalten**

   Die Seite mit der Monitorliste wird angezeigt und zeigt die aktuell konfigurierten Monitore.

2. Um einen vorhandenen Monitor zu ändern, klicken Sie in der Liste auf den Monitornamen.
3. Um einen Monitor hinzuzufügen, klicken Sie auf **+ Monitor**.

   Wenn Sie einen neuen Monitor hinzufügen, werden Sie aufgefordert, einen Metrikmonitor oder einen Protokollmonitor zu erstellen.

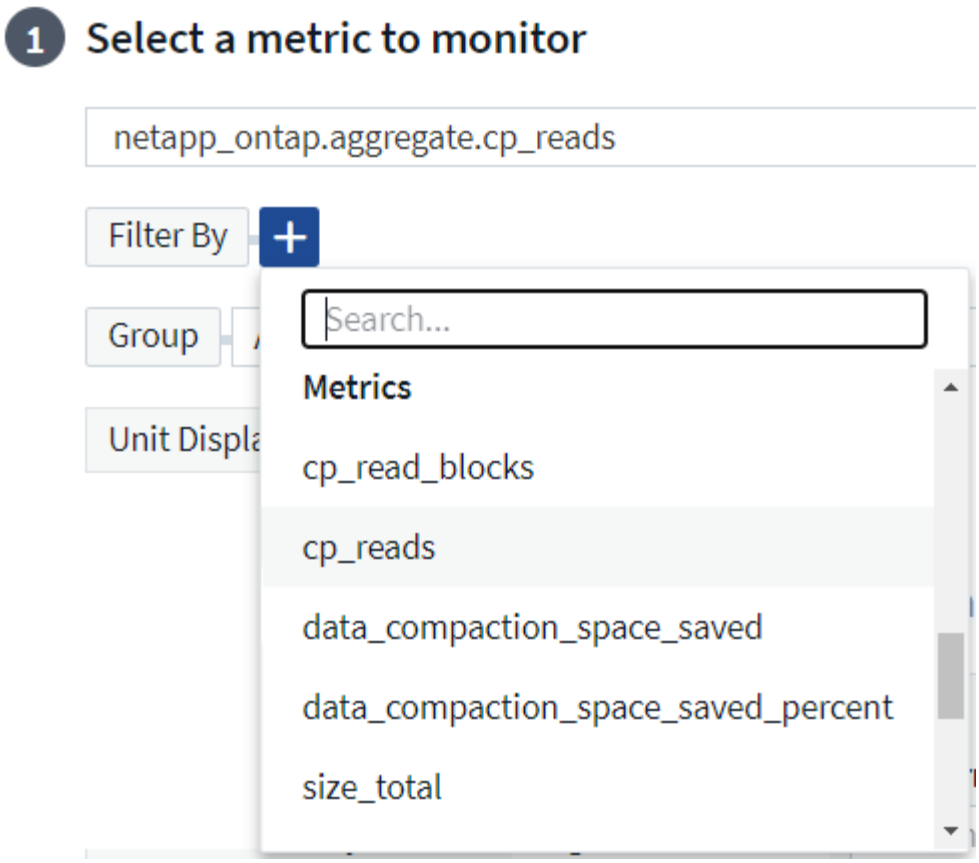
   - *Metric* überwacht Warnungen bei infrastruktur- oder leistungsbezogenen Auslösern
   - *Log* überwacht Warnungen bei protokollbezogenen Aktivitäten

   Nachdem Sie Ihren Monitortyp ausgewählt haben, wird das Dialogfeld „Monitorkonfiguration“ angezeigt. Die Konfiguration variiert je nach dem von Ihnen erstellten Monitortyp.

Metrikmonitor

1. Suchen Sie in der Dropdown-Liste nach einem zu überwachenden Objekttyp und einer Metrik und wählen Sie diese aus.

Sie können Filter festlegen, um einzugrenzen, welche Objektattribute oder Metriken überwacht werden sollen.



Beim Arbeiten mit Integrationsdaten (Kubernetes, ONTAP Advanced Data usw.) entfernt die Metrikfilterung die einzelnen/nicht übereinstimmenden Datenpunkte aus der dargestellten Datenreihe. Bei Infrastrukturdaten (Speicher, VM, Ports usw.) hingegen arbeiten Filter mit dem aggregierten Wert der Datenreihe und entfernen möglicherweise das gesamte Objekt aus dem Diagramm.

Um einen Monitor mit mehreren Bedingungen zu erstellen (z. B. IOPS > X und Latenz > Y), definieren Sie die erste Bedingung als Schwellenwert und die zweite Bedingung als Filter.

Definieren Sie die Bedingungen des Monitors.

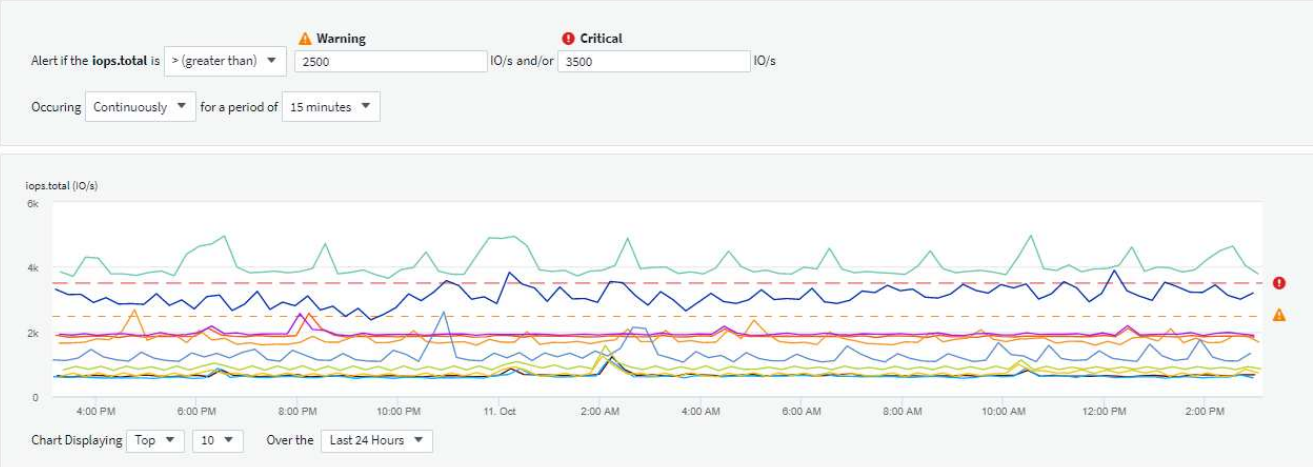
1. Nachdem Sie das zu überwachende Objekt und die Metrik ausgewählt haben, legen Sie die Schwellenwerte für die Warnstufe und/oder die kritische Stufe fest.
2. Geben Sie für die Warnstufe in unserem Beispiel 200 ein. Die gestrichelte Linie, die diese Warnstufe anzeigt, wird im Beispieldiagramm angezeigt.
3. Geben Sie für die Stufe *Kritisch* den Wert 400 ein. Die gestrichelte Linie, die diesen kritischen Pegel anzeigt, wird im Beispieldiagramm angezeigt.

   Das Diagramm zeigt historische Daten. Die Warn- und Kritisch-Level-Linien im Diagramm sind eine visuelle Darstellung des Monitors, sodass Sie leicht erkennen können, wann der Monitor in jedem Fall eine Warnung auslösen könnte.

4. Wählen Sie für das Auftretensintervall *Kontinuierlich* für einen Zeitraum von *15 Minuten*.

   Sie können wählen, ob Sie einen Alarm auslösen möchten, sobald ein Schwellenwert überschritten wird, oder ob Sie warten möchten, bis der Schwellenwert über einen bestimmten Zeitraum hinweg kontinuierlich überschritten wurde. In unserem Beispiel möchten wir nicht jedes Mal benachrichtigt werden, wenn die Gesamt-IOPS den Warn- oder kritischen Wert überschreiten, sondern nur, wenn ein überwachtes Objekt

mindestens 15 Minuten lang kontinuierlich einen dieser Werte überschreitet.



Definieren des Alarmauflösungsverhaltens

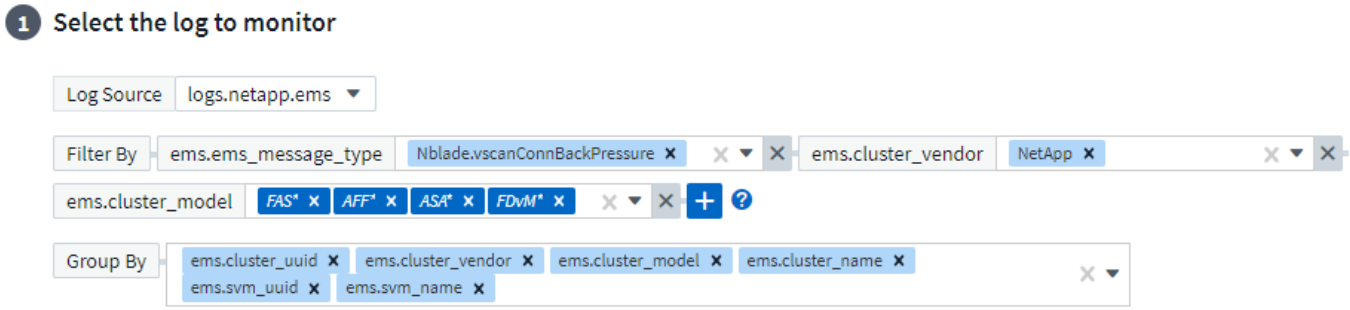
Sie können auswählen, wie eine Metriküberwachungswarnung aufgelöst wird. Ihnen stehen zwei Möglichkeiten zur Verfügung:

- Lösen Sie das Problem, wenn die Metrik wieder in den akzeptablen Bereich zurückkehrt.
- Lösen Sie das Problem, wenn die Metrik für einen bestimmten Zeitraum (von 1 Minute bis 7 Tagen) im akzeptablen Bereich liegt.

Protokollmonitor

Wählen Sie beim Erstellen eines **Protokollmonitors** zunächst aus der verfügbaren Protokollliste aus, welches Protokoll überwacht werden soll. Anschließend können Sie wie oben beschrieben anhand der verfügbaren Attribute filtern. Sie können auch ein oder mehrere „Gruppieren nach“-Attribute auswählen.

Der Log-Monitor-Filter darf nicht leer sein.



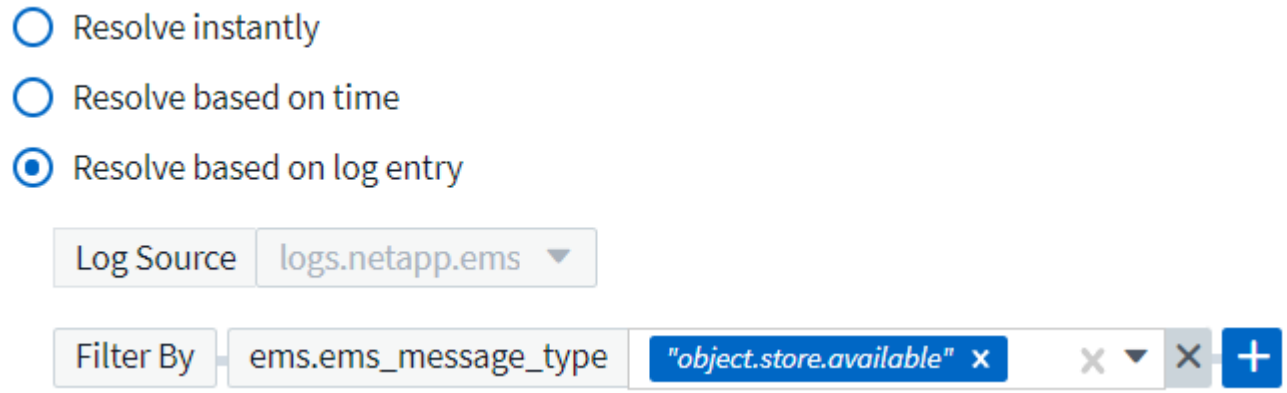
Definieren Sie das Alarmverhalten

Sie können den Monitor so erstellen, dass er mit dem Schweregrad *Kritisch*, *Warnung* oder *Informativ* warnt, wenn die oben definierten Bedingungen einmal (also sofort) eintreten, oder mit der Warnung warten, bis die Bedingungen zweimal oder öfter eintreten.

Definieren des Alarmauflösungsverhaltens

Sie können auswählen, wie eine Warnung des Protokollmonitors aufgelöst wird. Ihnen stehen drei Auswahlmöglichkeiten zur Verfügung:

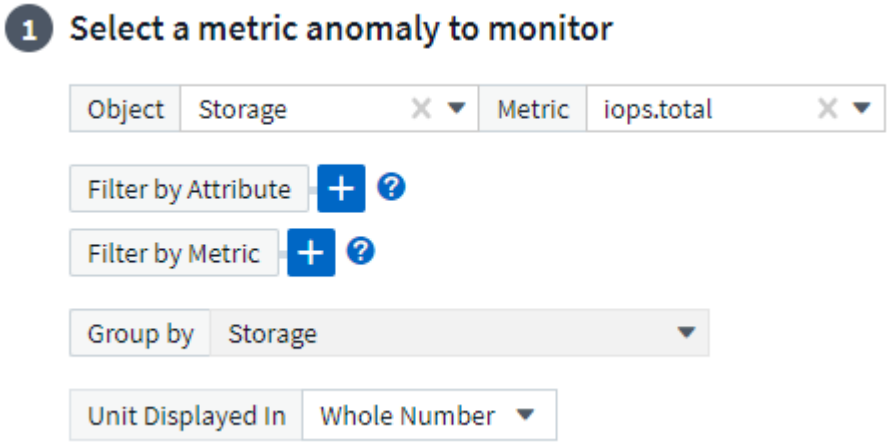
- **Sofort lösen**: Der Alarm wird sofort gelöst, es sind keine weiteren Maßnahmen erforderlich
- **Auflösung basierend auf Zeit**: Der Alarm wird nach Ablauf der angegebenen Zeit aufgelöst
- **Auflösung basierend auf Protokolleintrag**: Der Alarm wird aufgelöst, wenn eine nachfolgende Protokollaktivität aufgetreten ist. Beispielsweise wenn ein Objekt als „verfügbar“ protokolliert wird.



Anomalieerkennungsmonitor

1. Suchen Sie in der Dropdown-Liste nach einem zu überwachenden Objekttyp und einer Metrik und wählen Sie diese aus.

Sie können Filter festlegen, um einzugrenzen, welche Objektattribute oder Metriken überwacht werden sollen.

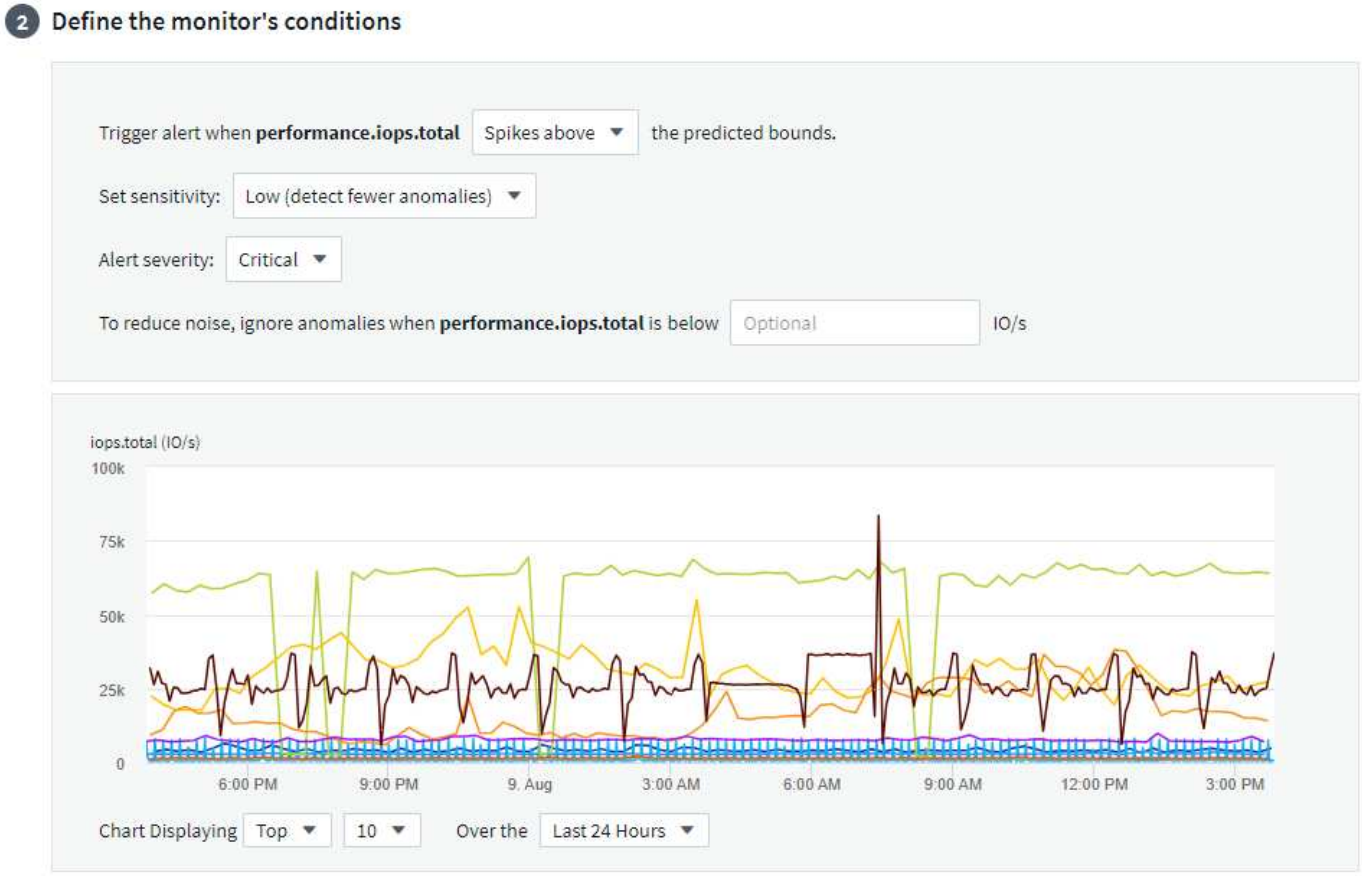


Definieren Sie die Bedingungen des Monitors.

1. Nachdem Sie das zu überwachende Objekt und die Metrik ausgewählt haben, legen Sie die Bedingungen fest, unter denen eine Anomalie erkannt wird.
    - Wählen Sie, ob eine Anomalie erkannt werden soll, wenn die gewählte Metrik die vorhergesagten Grenzen **überschreitet**, **unterschreitet** oder **über oder unterschreitet**.
    - Stellen Sie die **Empfindlichkeit** der Erkennung ein. **Niedrig** (weniger Anomalien werden erkannt),

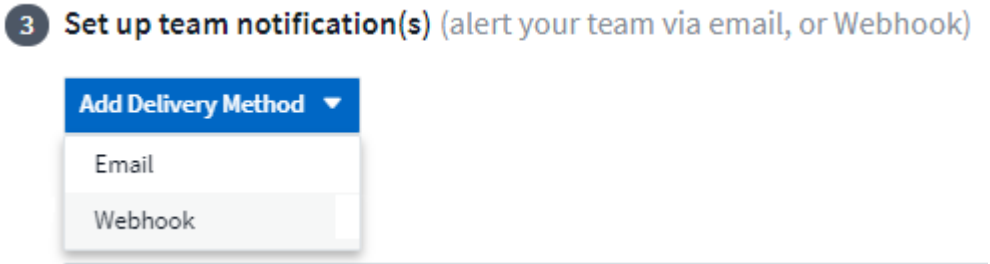
Mittel oder **Hoch** (mehr Anomalien werden erkannt).

- Stellen Sie die Warnungen auf **Warnung** oder **Kritisch** ein.
- Bei Bedarf können Sie das Rauschen reduzieren und Anomalien ignorieren, wenn die gewählte Metrik unter einem von Ihnen festgelegten Schwellenwert liegt.



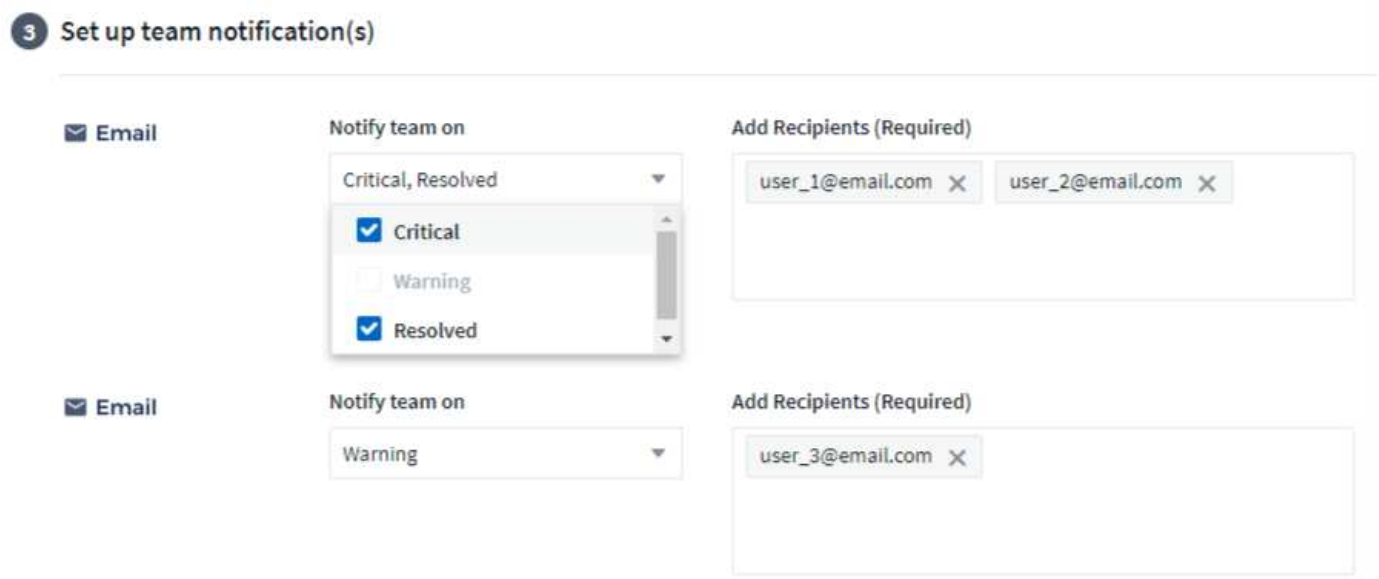
Benachrichtigungstyp und Empfänger auswählen

Im Abschnitt „Teambenachrichtigung(en) einrichten“ können Sie auswählen, ob Ihr Team per E-Mail oder Webhook benachrichtigt werden soll.



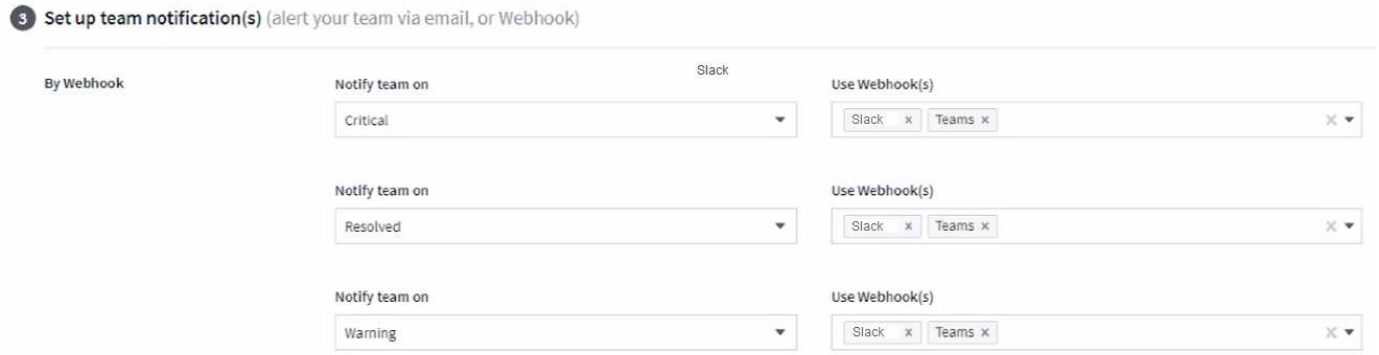
Benachrichtigung per E-Mail:

Geben Sie die E-Mail-Empfänger für Warnbenachrichtigungen an. Bei Bedarf können Sie für Warnungen oder kritische Alarme unterschiedliche Empfänger auswählen.



Alarmierung per Webhook:

Geben Sie den/die Webhook(s) für Warnbenachrichtigungen an. Bei Bedarf können Sie verschiedene Webhooks für Warnungen oder kritische Alarme auswählen.



ONTAP Data Collector-Benachrichtigungen haben Vorrang vor allen spezifischen Monitor-Benachrichtigungen, die für den Cluster/Data Collector relevant sind. Die Empfängerliste, die Sie für den Datensammler selbst festlegen, erhält die Warnungen des Datensammlers. Wenn keine aktiven Datensammlerwarnungen vorliegen, werden vom Monitor generierte Warnungen an bestimmte Monitorempfänger gesendet.

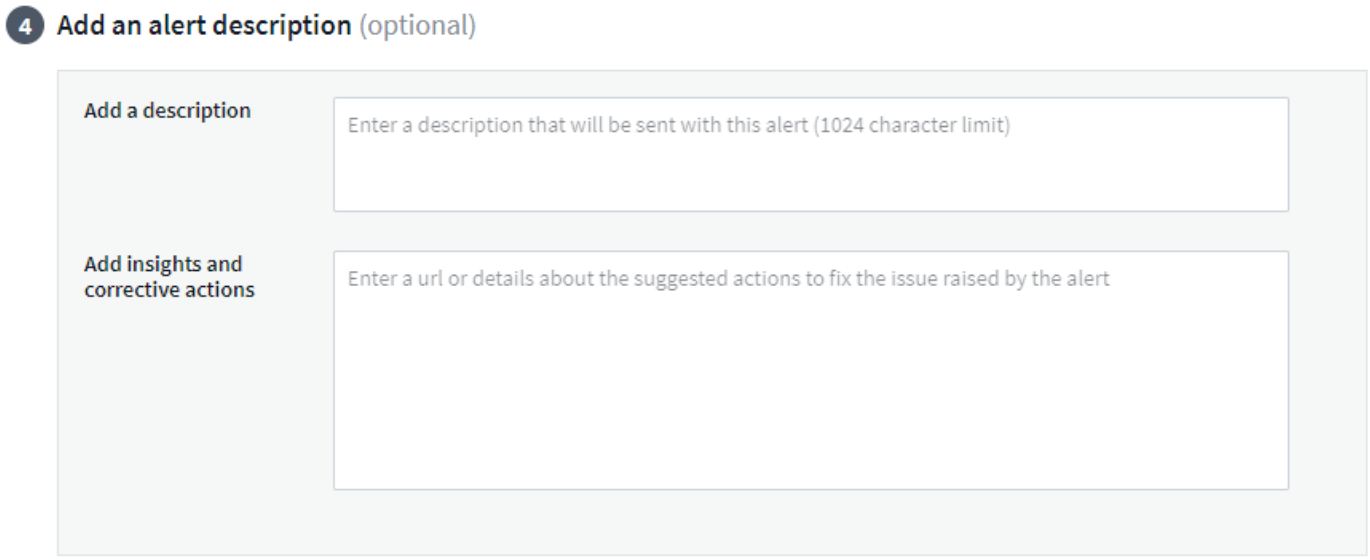
Festlegen von Korrekturmaßnahmen oder zusätzlichen Informationen

Sie können eine optionale Beschreibung sowie zusätzliche Erkenntnisse und/oder Korrekturmaßnahmen hinzufügen, indem Sie den Abschnitt **Warnungsbeschreibung hinzufügen** ausfüllen. Die Beschreibung kann bis zu 1024 Zeichen lang sein und wird mit der Warnung gesendet. Das Feld „Erkenntnisse/Korrekturmaßnahmen“ kann bis zu 67.000 Zeichen umfassen und wird im Zusammenfassungsbereich der Zielseite der Warnung angezeigt.

In diesen Feldern können Sie Notizen, Links oder Schritte zur Korrektur oder anderweitigen Bearbeitung der Warnung angeben.

Sie können einer Alarmbeschreibung jedes beliebige Objektattribut (z. B. den Speichernamen) als Parameter hinzufügen. Sie können beispielsweise Parameter für den Volumenamen und den Speichernamen in einer

Beschreibung wie folgt festlegen: „Hohe Latenz für Volume: *%%relatedObject.volume.name%%*, Speicher: *%%relatedObject.storage.name%%*“.



Speichern Sie Ihren Monitor

1. Falls gewünscht, können Sie eine Beschreibung des Monitors hinzufügen.
2. Geben Sie dem Monitor einen aussagekräftigen Namen und klicken Sie auf **Speichern**.

   Ihr neuer Monitor wird der Liste der aktiven Monitore hinzugefügt.

Monitorliste

Auf der Seite „Monitor“ werden die aktuell konfigurierten Monitore aufgelistet und Folgendes angezeigt:

- Monitorname
- Status
- Überwachtes Objekt/Metrik
- Bedingungen des Monitors

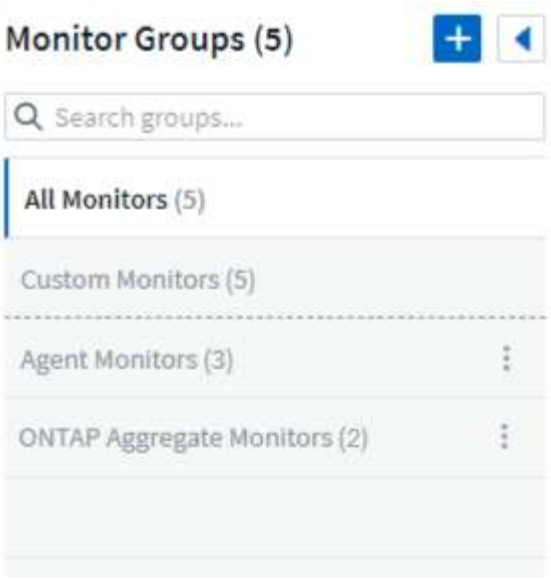
Sie können die Überwachung eines Objekttyps vorübergehend anhalten, indem Sie auf das Menü rechts neben dem Monitor klicken und **Pause** auswählen. Wenn Sie bereit sind, die Überwachung fortzusetzen, klicken Sie auf **Fortsetzen**.

Sie können einen Monitor kopieren, indem Sie im Menü **Duplizieren** auswählen. Anschließend können Sie den neuen Monitor modifizieren und Objekt/Metrik, Filter, Bedingungen, E-Mail-Empfänger usw. ändern.

Wenn ein Monitor nicht mehr benötigt wird, können Sie ihn löschen, indem Sie im Menü **Löschen** auswählen.

Monitorgruppen

Durch Gruppieren können Sie zusammengehörige Monitore anzeigen und verwalten. Sie können beispielsweise eine Monitorgruppe speziell für den Speicher Ihres Mandanten einrichten oder Monitore, die für eine bestimmte Empfängerliste relevant sind.



Die folgenden Monitorgruppen werden angezeigt. Die Anzahl der in einer Gruppe enthaltenen Monitore wird neben dem Gruppennamen angezeigt.

- **Alle Monitore** listet alle Monitore auf.
- **Benutzerdefinierte Monitore** listet alle vom Benutzer erstellten Monitore auf.
- **Angehaltene Monitore** listet alle Systemmonitore auf, die von Data Infrastructure Insights angehalten wurden.
- Data Infrastructure Insights zeigt auch eine Reihe von **System Monitor Groups** an, die eine oder mehrere Gruppen von"systemdefinierte Monitore" , einschließlich ONTAP -Infrastruktur- und Workload-Monitoren.

Benutzerdefinierte Monitore können angehalten, fortgesetzt, gelöscht oder in eine andere Gruppe verschoben werden. Systemdefinierte Monitore können angehalten und fortgesetzt, aber nicht gelöscht oder verschoben werden.

Hängende Monitore

Diese Gruppe wird nur angezeigt, wenn Data Infrastructure Insights einen oder mehrere Monitore angehalten hat. Ein Monitor kann ausgesetzt werden, wenn er übermäßig viele oder kontinuierliche Warnungen generiert. Wenn es sich bei dem Monitor um einen benutzerdefinierten Monitor handelt, ändern Sie die Bedingungen, um die kontinuierliche Alarmierung zu verhindern, und setzen Sie den Monitor dann fort. Der Monitor wird aus der Gruppe „Angehaltene Monitore“ entfernt, wenn das Problem, das zur Anhaltung geführt hat, behoben ist.

Systemdefinierte Monitore

Diese Gruppen zeigen die von Data Infrastructure Insights bereitgestellten Monitore an, sofern Ihre Umgebung die von den Monitoren benötigten Geräte und/oder Protokollverfügbarkeit enthält.

Systemdefinierte Monitore können nicht geändert, in eine andere Gruppe verschoben oder gelöscht werden. Sie können jedoch einen Systemmonitor duplizieren und das Duplikat ändern oder verschieben.

Systemmonitore können Monitore für die ONTAP Infrastruktur (Speicher, Volume usw.) oder Workloads (d. h. Protokollmonitore) oder andere Gruppen umfassen. NetApp wertet ständig die Kundenbedürfnisse und Produktfunktionen aus und aktualisiert oder ergänzt Systemmonitore und -gruppen nach Bedarf.

Benutzerdefinierte Monitorgruppen

Sie können Ihre eigenen Gruppen erstellen, um Monitore entsprechend Ihren Anforderungen zu enthalten. Beispielsweise möchten Sie möglicherweise eine Gruppe für alle Ihre speicherbezogenen Monitore.

Um eine neue benutzerdefinierte Monitorgruppe zu erstellen, klicken Sie auf die Schaltfläche **"+" Neue Monitorgruppe erstellen**. Geben Sie einen Namen für die Gruppe ein und klicken Sie auf **Gruppe erstellen**. Es wird eine leere Gruppe mit diesem Namen erstellt.

Um Monitore zur Gruppe hinzuzufügen, gehen Sie zur Gruppe „Alle Monitore“ (empfohlen) und führen Sie einen der folgenden Schritte aus:

- Um einen einzelnen Monitor hinzuzufügen, klicken Sie auf das Menü rechts neben dem Monitor und wählen Sie *Zur Gruppe hinzufügen*. Wählen Sie die Gruppe aus, zu der der Monitor hinzugefügt werden soll.
- Klicken Sie auf den Monitornamen, um die Bearbeitungsansicht des Monitors zu öffnen, und wählen Sie im Abschnitt *Mit einer Monitorgruppe verknüpfen* eine Gruppe aus.

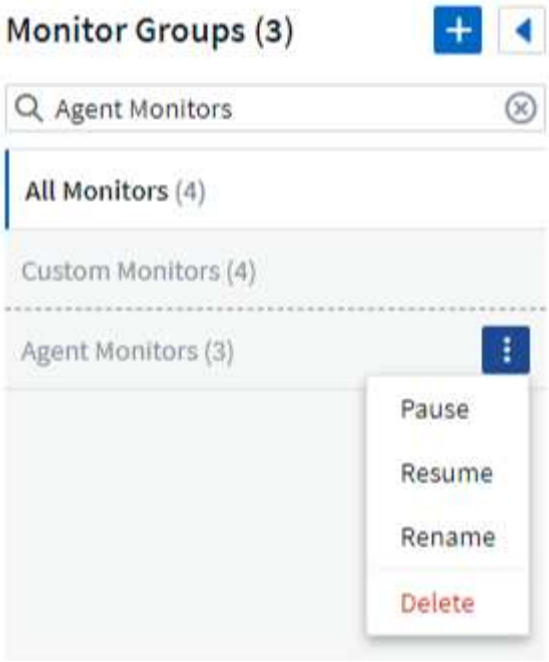
Entfernen Sie Monitore, indem Sie auf eine Gruppe klicken und im Menü „Aus Gruppe entfernen“ auswählen. Sie können keine Monitore aus der Gruppe „Alle Monitore“ oder „Benutzerdefinierte Monitore“ entfernen. Um einen Monitor aus diesen Gruppen zu löschen, müssen Sie den Monitor selbst löschen.

Durch das Entfernen eines Monitors aus einer Gruppe wird der Monitor nicht aus Data Infrastructure Insights gelöscht. Um einen Monitor vollständig zu entfernen, wählen Sie den Monitor aus und klicken Sie auf *Löschen*. Dadurch wird es auch aus der Gruppe entfernt, zu der es gehörte, und steht keinem Benutzer mehr zur Verfügung.

Sie können einen Monitor auf die gleiche Weise auch in eine andere Gruppe verschieben, indem Sie *In Gruppe verschieben* auswählen.

Um alle Monitore einer Gruppe gleichzeitig anzuhalten oder fortzusetzen, wählen Sie das Menü für die Gruppe aus und klicken Sie auf *Pause* oder *Fortsetzen*.

Verwenden Sie dasselbe Menü, um eine Gruppe umzubenennen oder zu löschen. Durch das Löschen einer Gruppe werden die Monitore nicht aus Data Infrastructure Insights gelöscht. Sie sind weiterhin unter „Alle Monitore“ verfügbar.



Systemdefinierte Monitore

Data Infrastructure Insights umfasst eine Reihe systemdefinierter Monitore für Metriken und Protokolle. Die verfügbaren Systemmonitore hängen von den auf Ihrem Mandanten vorhandenen Datensammlern ab. Aus diesem Grund können sich die in Data Infrastructure Insights verfügbaren Monitore ändern, wenn Datensammler hinzugefügt oder ihre Konfigurationen geändert werden.

Sehen Sie sich die"Systemdefinierte Monitore" Seite mit Beschreibungen der in Data Infrastructure Insights enthaltenen Monitore.

Weitere Informationen

- "Anzeigen und Verwerfen von Warnungen"

Anzeigen und Verwalten von Warnungen von Monitoren

Data Infrastructure Insights zeigt Warnungen an, wenn"überwachte Schwellenwerte" überschritten werden.

Monitore und Warnungen sind in der Data Infrastructure Insights Standard Edition und höher verfügbar.

Anzeigen und Verwalten von Warnungen

Gehen Sie wie folgt vor, um Warnungen anzuzeigen und zu verwalten.

1. Navigieren Sie zur Seite **Warnungen > Alle Warnungen**.
2. Es wird eine Liste mit bis zu 1.000 der letzten Warnungen angezeigt. Sie können diese Liste nach jedem Feld sortieren, indem Sie auf die Spaltenüberschrift des Felds klicken. Die Liste zeigt die folgenden Informationen an. Beachten Sie, dass nicht alle dieser Spalten standardmäßig angezeigt werden. Sie können die anzuzeigenden Spalten auswählen, indem Sie auf das Zahnradsymbol klicken:
   - **Alarm-ID**: Vom System generierte eindeutige Alarm-ID

- **Auslösezeit**: Der Zeitpunkt, zu dem der entsprechende Monitor den Alarm ausgelöst hat
- **Aktueller Schweregrad** (Registerkarte „Aktive Warnungen“): Der aktuelle Schweregrad der aktiven Warnung
- **Höchster Schweregrad** (Registerkarte „Behobene Warnungen“): Der maximale Schweregrad der Warnung, bevor sie behoben wurde.
- **Monitor**: Der Monitor, der zum Auslösen des Alarms konfiguriert ist
- **Ausgelöst am**: Das Objekt, bei dem der überwachte Schwellenwert überschritten wurde
- **Status**: Aktueller Alarmstatus, *Neu* oder *In Bearbeitung*
- **Aktivstatus**: *Aktiv* oder *Gelöst*
- **Bedingung**: Die Schwellenwertbedingung, die den Alarm ausgelöst hat
- **Metrik**: Die Metrik des Objekts, bei der der überwachte Schwellenwert überschritten wurde
- **Monitorstatus**: Aktueller Status des Monitors, der den Alarm ausgelöst hat
- **Hat Korrekturmaßnahmen**: Die Warnung hat Korrekturmaßnahmen vorgeschlagen. Öffnen Sie die Warnseite, um diese anzuzeigen.

Sie können eine Warnung verwalten, indem Sie auf das Menü rechts neben der Warnung klicken und eine der folgenden Optionen auswählen:

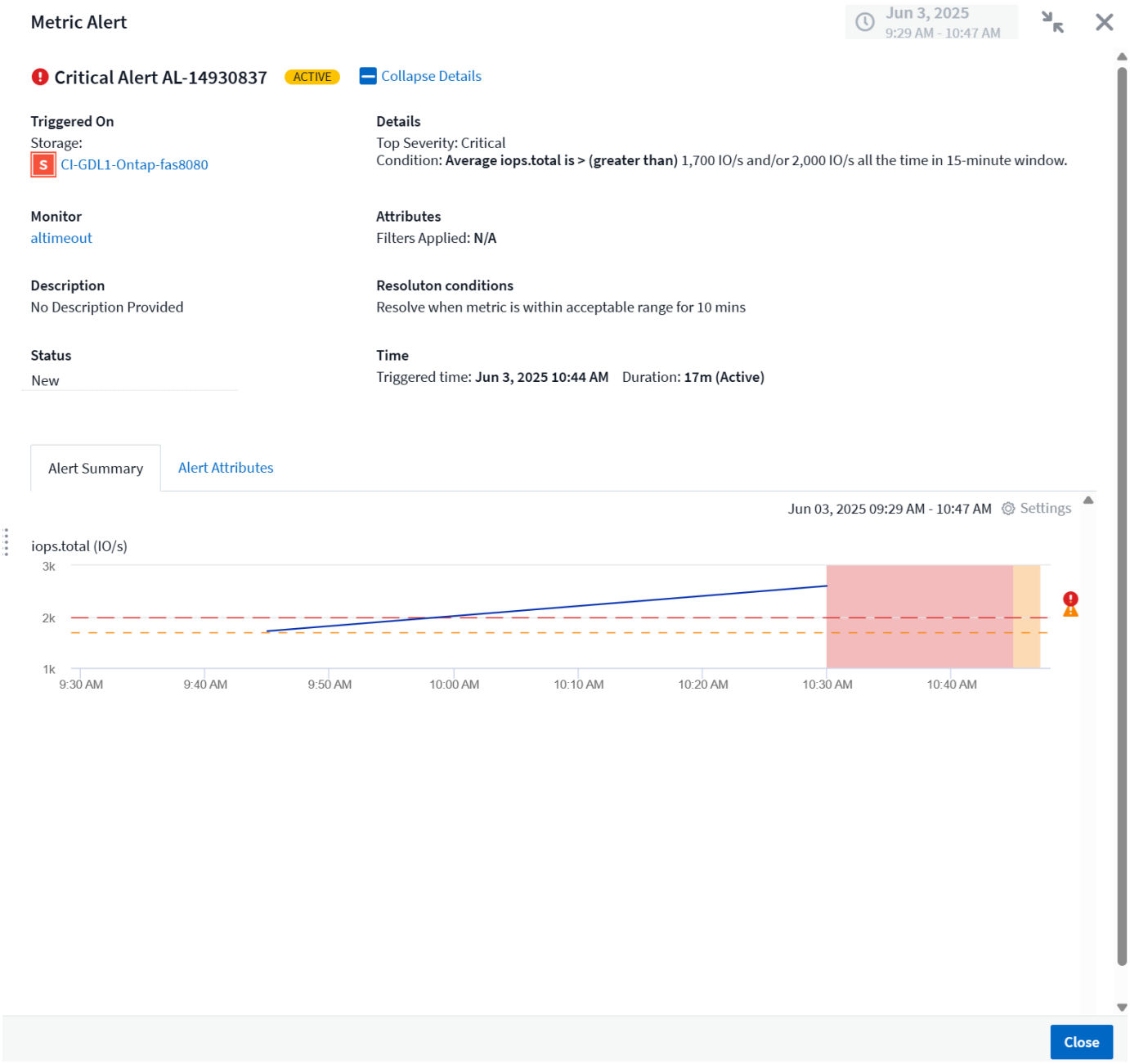
- **In Bearbeitung**, um anzuzeigen, dass die Warnung untersucht wird oder aus anderen Gründen offen gehalten werden muss
- **Ablehnen**, um die Warnung aus der Liste der aktiven Warnungen zu entfernen.

Sie können mehrere Warnungen verwalten, indem Sie das Kontrollkästchen links neben jeder Warnung aktivieren und auf „Status ausgewählter Warnungen ändern“ klicken.

Durch Klicken auf eine Alarm-ID wird die Alarmdetailseite geöffnet.

Alarmdetailbereich

Wählen Sie eine beliebige Alarmzeile aus, um das Detailfenster des Alarms zu öffnen. Das Alarmdetailfenster bietet zusätzliche Einzelheiten zum Alarm, darunter eine *Zusammenfassung*, einen Abschnitt *Leistung* mit Diagrammen zu den Daten des Objekts, alle *zugehörigen Assets* und *Kommentare*, die von den Alarmermittlern eingegeben wurden.



Warnmeldungen bei fehlenden Daten

Um in einem Echtzeitsystem wie Data Infrastructure Insights die Analyse eines Monitors auszulösen und zu entscheiden, ob eine Warnung generiert werden soll, verlassen wir uns auf eines von zwei Dingen:

- der nächste ankommende Datenpunkt
- ein Timer, der ausgelöst wird, wenn kein Datenpunkt vorhanden ist und Sie lange genug gewartet haben

Wie bei langsamem Dateneingang – oder keinem Dateneingang – muss der Zeitgebermechanismus eingreifen, da die Dateneingangsrate nicht ausreicht, um Warnungen in „Echtzeit“ auszulösen. Daher lautet die Frage normalerweise: „Wie lange muss ich warten, bevor ich das Analysefenster schließe und mir ansehe, was ich habe?“ Wenn Sie zu lange warten, generieren Sie die Warnungen nicht schnell genug, um nützlich zu sein.

Wenn Sie einen Monitor mit einem 30-Minuten-Fenster haben, der erkennt, dass eine Bedingung durch den

letzten Datenpunkt vor einem langfristigen Datenverlust verletzt wurde, wird eine Warnung generiert, da der Monitor keine anderen Informationen erhalten hat, um eine Wiederherstellung der Metrik zu bestätigen oder festzustellen, dass die Bedingung weiterhin besteht.

„Dauerhaft aktive“ Warnungen

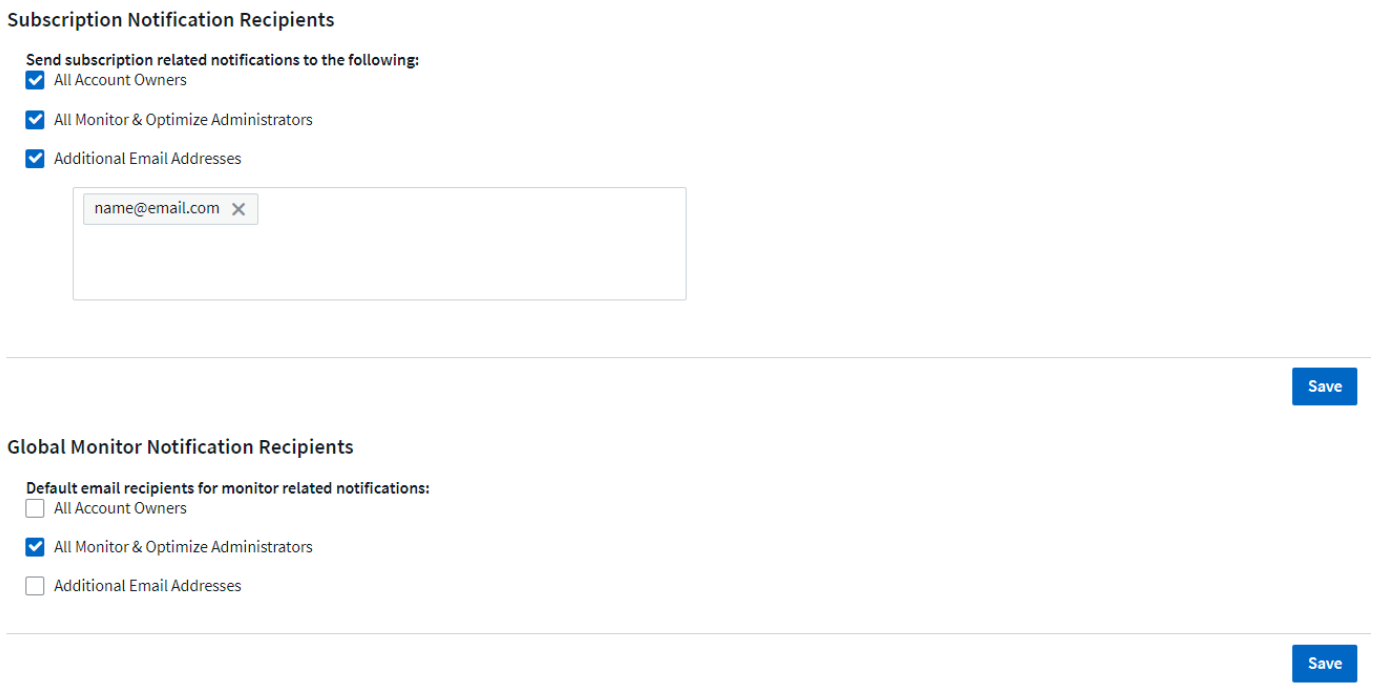
Es ist möglich, einen Monitor so zu konfigurieren, dass die Bedingung für das überwachte Objekt **immer** erfüllt ist – beispielsweise IOPS > 1 oder Latenz > 0. Diese werden oft als „Test“-Monitore erstellt und dann vergessen. Solche Monitore erstellen Warnungen, die für die einzelnen Objekte dauerhaft offen bleiben, was mit der Zeit zu Systembelastungen und Stabilitätsproblemen führen kann.

Um dies zu verhindern, schließt Data Infrastructure Insights alle „dauerhaft aktiven“ Warnungen nach 7 Tagen automatisch. Beachten Sie, dass die zugrunde liegenden Überwachungsbedingungen möglicherweise (wahrscheinlich) weiterhin bestehen bleiben, sodass fast sofort eine neue Warnung ausgegeben wird. Durch das Schließen der „immer aktiven“ Warnungen wird jedoch ein Teil der Systembelastung gemildert, die andernfalls auftreten kann.

Konfigurieren von E-Mail-Benachrichtigungen

Sie können eine E-Mail-Liste für abonnementbezogene Benachrichtigungen sowie eine globale E-Mail-Liste mit Empfängern für Benachrichtigungen über Verstöße gegen Schwellenwerte der Leistungsrichtlinie konfigurieren.

Um die Einstellungen für den Empfänger von Benachrichtigungs-E-Mails zu konfigurieren, gehen Sie zur Seite **Admin > Benachrichtigungen** und wählen Sie die Registerkarte *E-Mail*.



Empfänger von Abonnementbenachrichtigungen

Um Empfänger für abonnementbezogene Ereignisbenachrichtigungen zu konfigurieren, gehen Sie zum Abschnitt „Empfänger von Abonnementbenachrichtigungen“. Sie können festlegen, dass E-Mail-Benachrichtigungen zu abonnementbezogenen Ereignissen an einen oder alle der folgenden Empfänger gesendet werden:

- Alle Kontoinhaber
- Alle *Monitor & Optimize*-Administratoren
- Zusätzliche E-Mail-Adressen, die Sie angeben

Im Folgenden finden Sie Beispiele für die Arten von Benachrichtigungen, die gesendet werden können, und für Benutzeraktionen, die Sie ausführen können.

Benachrichtigung:	**Benutzeraktion:**
Testversion oder Abonnement wurde aktualisiert	Überprüfen Sie die Abonnementdetails auf der"Abonnement" Seite
Das Abonnement läuft in 90 Tagen ab. Das Abonnement läuft in 30 Tagen ab.	Wenn „Automatische Verlängerung“ aktiviert ist, sind keine Maßnahmen erforderlich. Wenden Sie sich an den NetApp -Vertrieb, um das Abonnement zu verlängern.
Testversion endet in 2 Tagen	Testversion erneuern von"Abonnement" Seite. Sie können eine Testversion einmal verlängern. Kontaktieren Sie den NetApp -Vertrieb, um ein Abonnement zu erwerben
Testversion oder Abonnement ist abgelaufen. Das Konto wird in 48 Stunden keine Daten mehr sammeln. Das Konto wird nach 48 Stunden gelöscht.	Kontaktieren Sie den NetApp -Vertrieb, um ein Abonnement zu erwerben

Um sicherzustellen, dass Ihre Empfänger Benachrichtigungen von Data Infrastructure Insights erhalten, fügen Sie die folgenden E-Mail-Adressen zu allen Zulassungslisten hinzu:

- accounts@service.cloudinsights.netapp.com
- DoNotReply@cloudinsights.netapp.com

Globale Empfängerliste für Warnmeldungen

Für jede Aktion im Zusammenhang mit der Warnung werden E-Mail-Benachrichtigungen zu Warnungen an die Warnungsempfängerliste gesendet. Sie können Warnbenachrichtigungen an eine globale Empfängerliste senden.

Um globale Alarmempfänger zu konfigurieren, wählen Sie die gewünschten Empfänger im Abschnitt **Globale Monitor-Benachrichtigungsempfänger** aus.

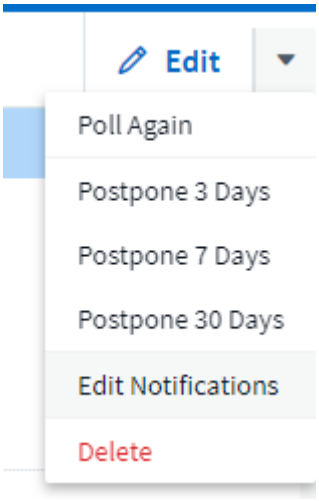
Sie können die globale Empfängerliste für einen einzelnen Monitor jederzeit überschreiben, wenn Sie den Monitor erstellen oder ändern.

ONTAP Data Collector-Benachrichtigungen haben Vorrang vor allen spezifischen Monitor-Benachrichtigungen, die für den Cluster/Data Collector relevant sind. Die Empfängerliste, die Sie für den Datensammler selbst festlegen, erhält die Warnungen des Datensammlers. Wenn keine aktiven Datensammlerwarnungen vorliegen, werden vom Monitor generierte Warnungen an bestimmte Monitorempfänger gesendet.

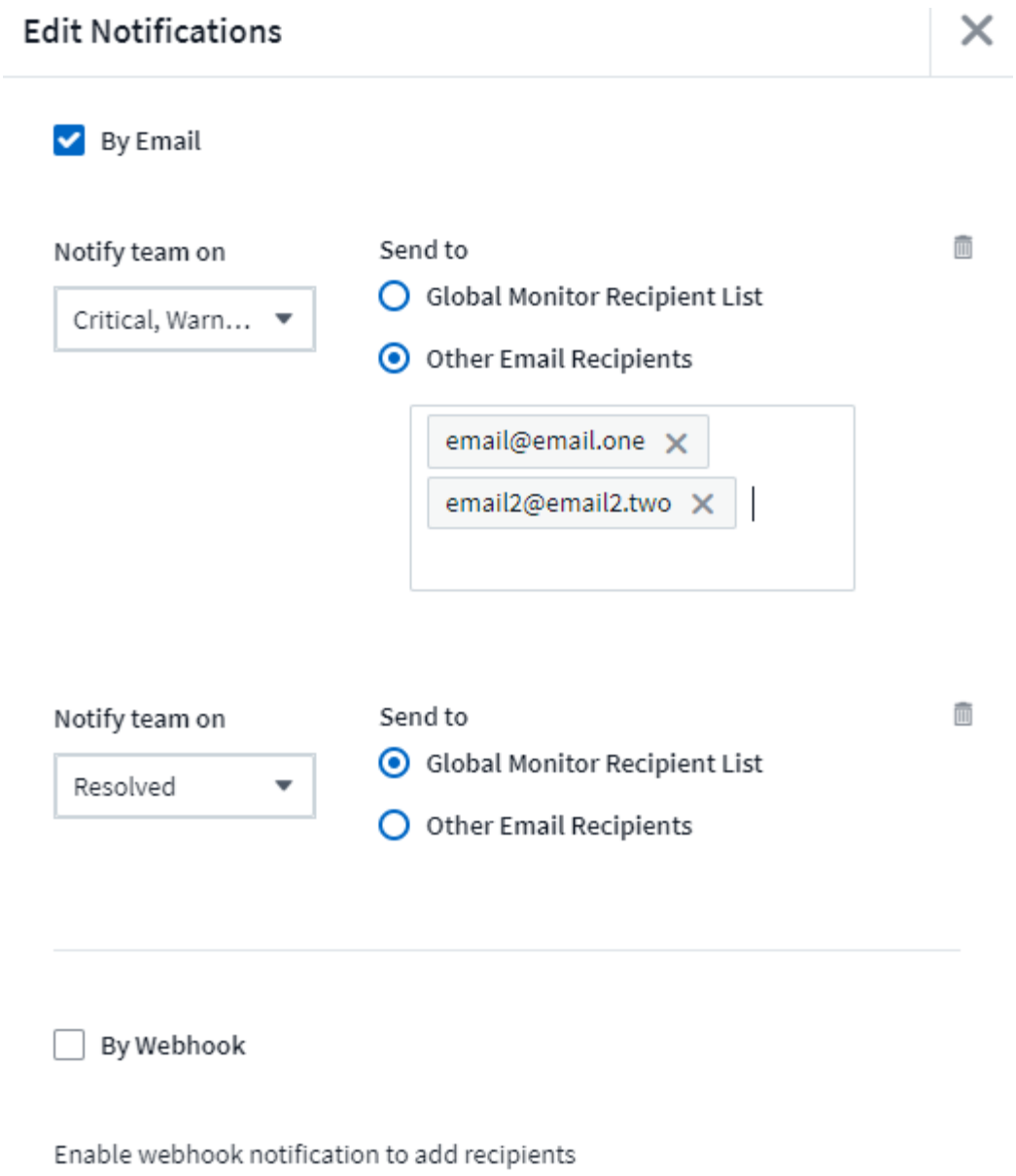
Bearbeiten von Benachrichtigungen für ONTAP

Sie können Benachrichtigungen für ONTAP Cluster ändern, indem Sie auf einer Speicher-Landingpage im

Dropdown-Menü oben rechts „Benachrichtigungen bearbeiten“ auswählen.



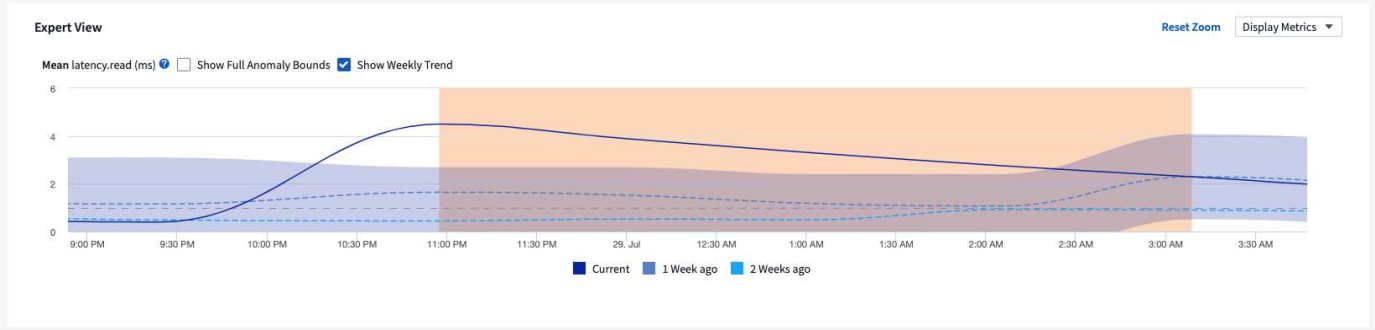
Von hier aus können Sie Benachrichtigungen für kritische, Warn-, Informations- und/oder behobene Alarme festlegen. Jedes Szenario kann die globale Empfängerliste oder andere von Ihnen ausgewählte Empfänger benachrichtigen.



Anomalieerkennungsmonitore

Die Anomalieerkennung bietet Einblick in unerwartete Änderungen in den Datenmustern Ihres Mandanten. Eine Anomalie tritt auf, wenn sich das Verhaltensmuster eines Objekts ändert. Wenn beispielsweise ein Objekt mittwochs zu einer bestimmten Uhrzeit eine bestimmte Latenz aufweist, die Latenz am darauffolgenden Mittwoch jedoch zu dieser Uhrzeit über diesen Wert ansteigt, wird dieser Anstieg als Anomalie betrachtet. Data Infrastructure Insights ermöglicht die Erstellung von Monitoren, die beim Auftreten solcher Anomalien eine Warnung ausgeben.

Die Anomalieerkennung eignet sich für Objektmetriken, die ein wiederkehrendes, vorhersehbares Muster aufweisen. Wenn diese Objektmetriken über oder unter die erwarteten Werte steigen, kann Data Infrastructure Insights eine Warnung generieren, um eine Untersuchung einzuleiten.



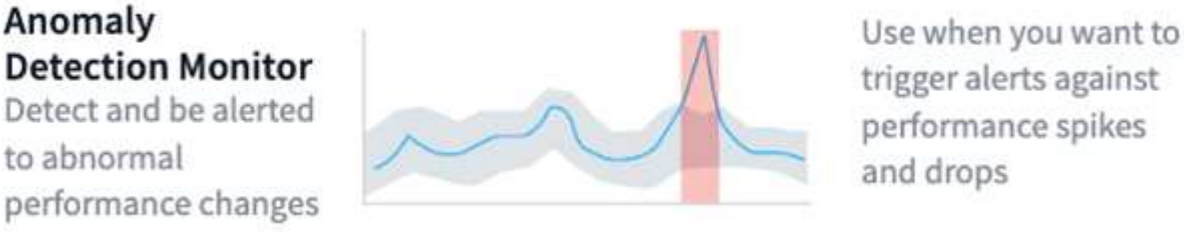
Was ist Anomalieerkennung?

Eine Anomalie tritt auf, wenn der Mittelwert einer Metrik um eine bestimmte Anzahl von Standardabweichungen vom gewichteten Mittelwert dieser Metrik der letzten Wochen abweicht, wobei die letzten Wochen stärker gewichtet werden als die vorherigen Wochen. Data Infrastructure Insights bietet die Möglichkeit, Daten zu überwachen und bei erkannten Anomalien eine Warnung auszugeben. Sie haben die Möglichkeit, die Empfindlichkeitsstufen der Erkennung einzustellen. Eine höhere Empfindlichkeit liegt beispielsweise vor, wenn der Mittelwert weniger Standardabweichungen vom Mittelwert aufweist und somit mehr Warnungen generiert werden. Umgekehrt gilt: geringere Empfindlichkeit = mehr Standardabweichungen vom Mittelwert = weniger Warnungen.

Die Überwachung der Anomalieerkennung unterscheidet sich von der Schwellenwertüberwachung.

- **Schwellenwertbasierte Überwachung** funktioniert, wenn Sie vordefinierte Schwellenwerte für bestimmte Metriken haben. Mit anderen Worten, wenn Sie ein klares Verständnis davon haben, was erwartet wird (d. h. innerhalb eines normalen Bereichs).

- Bei der **Überwachung der Anomalieerkennung** werden Algorithmen des maschinellen Lernens verwendet, um Ausreißer zu identifizieren, die von der Norm abweichen, wenn die Definition von „normal“ nicht klar ist.



Wann benötige ich eine Anomalieerkennung?

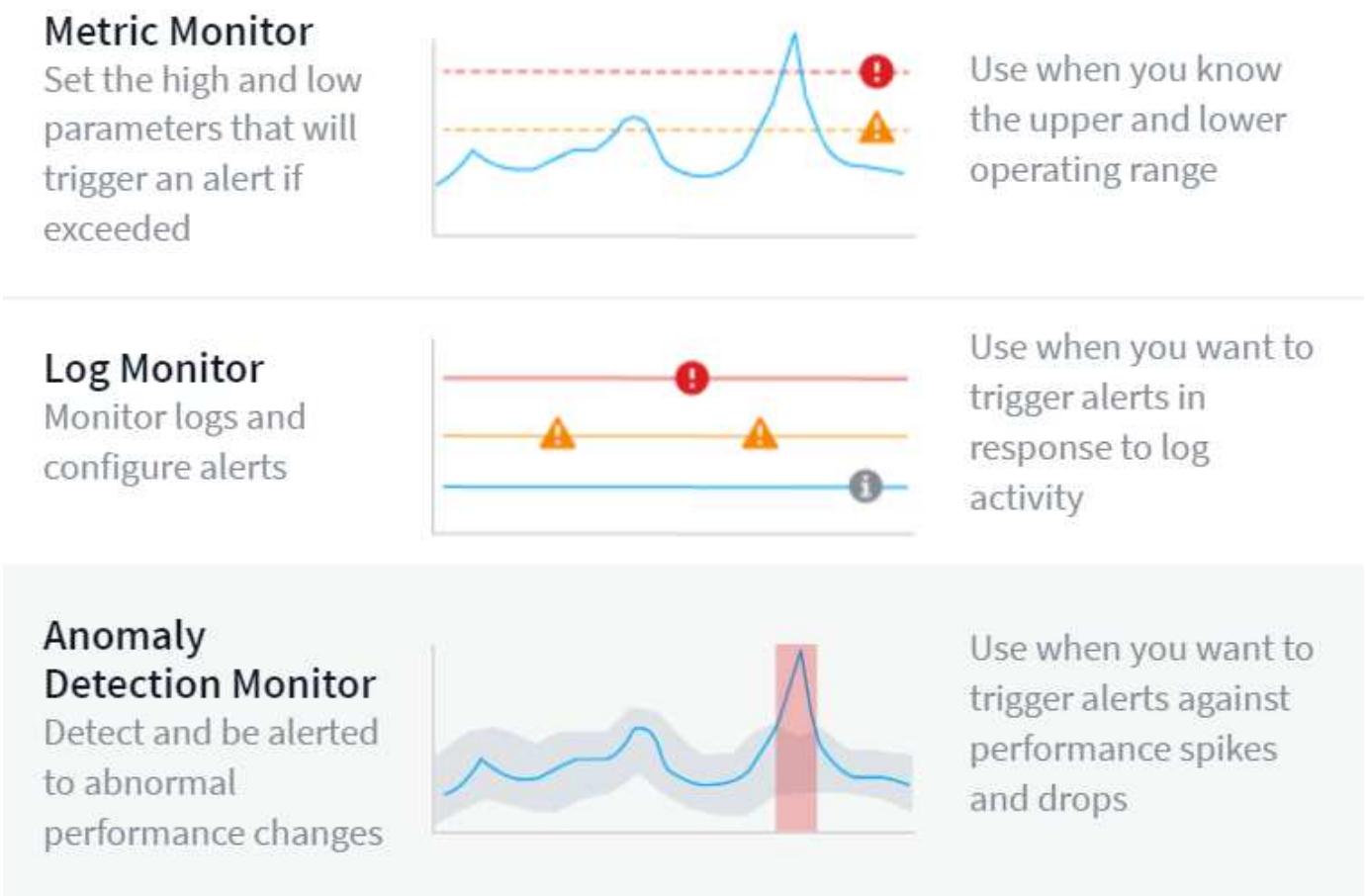
Die Überwachung der Anomalieerkennung kann in vielen Situationen hilfreiche Warnungen liefern, darunter in

den folgenden:

- Wenn die Definition von *normal* unklar ist. Beispielsweise kann es je nach Port zu unterschiedlich hohen SAN-Fehlerraten kommen. Eine Warnung bei einem einzelnen Fehler ist unnötig und unauffällig, ein plötzlicher oder deutlicher Anstieg kann jedoch auf ein weitverbreitetes Problem hinweisen.
- Wo es im Laufe der Zeit zu Veränderungen kommt. Arbeitslasten, die Saisonalität aufweisen (d. h. zu bestimmten Zeiten sind sie ausgelastet oder ruhig). Hierzu können unerwartete Ruhephasen gehören, die auf einen Batch-Stillstand hindeuten können.
- Arbeiten mit großen Datenmengen, bei denen das manuelle Definieren und Anpassen von Schwellenwerten unpraktisch ist. Beispielsweise ein Mandant mit einer großen Anzahl von Hosts und/oder Volumes mit unterschiedlichen Arbeitslasten. Jeder hat möglicherweise andere SLAs, daher ist es wichtig zu verstehen, welche die Norm überschreiten.

Erstellen eines Anomalieerkennungsmonitors

Um bei Anomalien Warnungen auszugeben, erstellen Sie einen Monitor, indem Sie zu **Beobachtbarkeit > Warnungen > +Monitor** navigieren. Wählen Sie *Anomaly Detection Monitor* als Monitortyp aus.

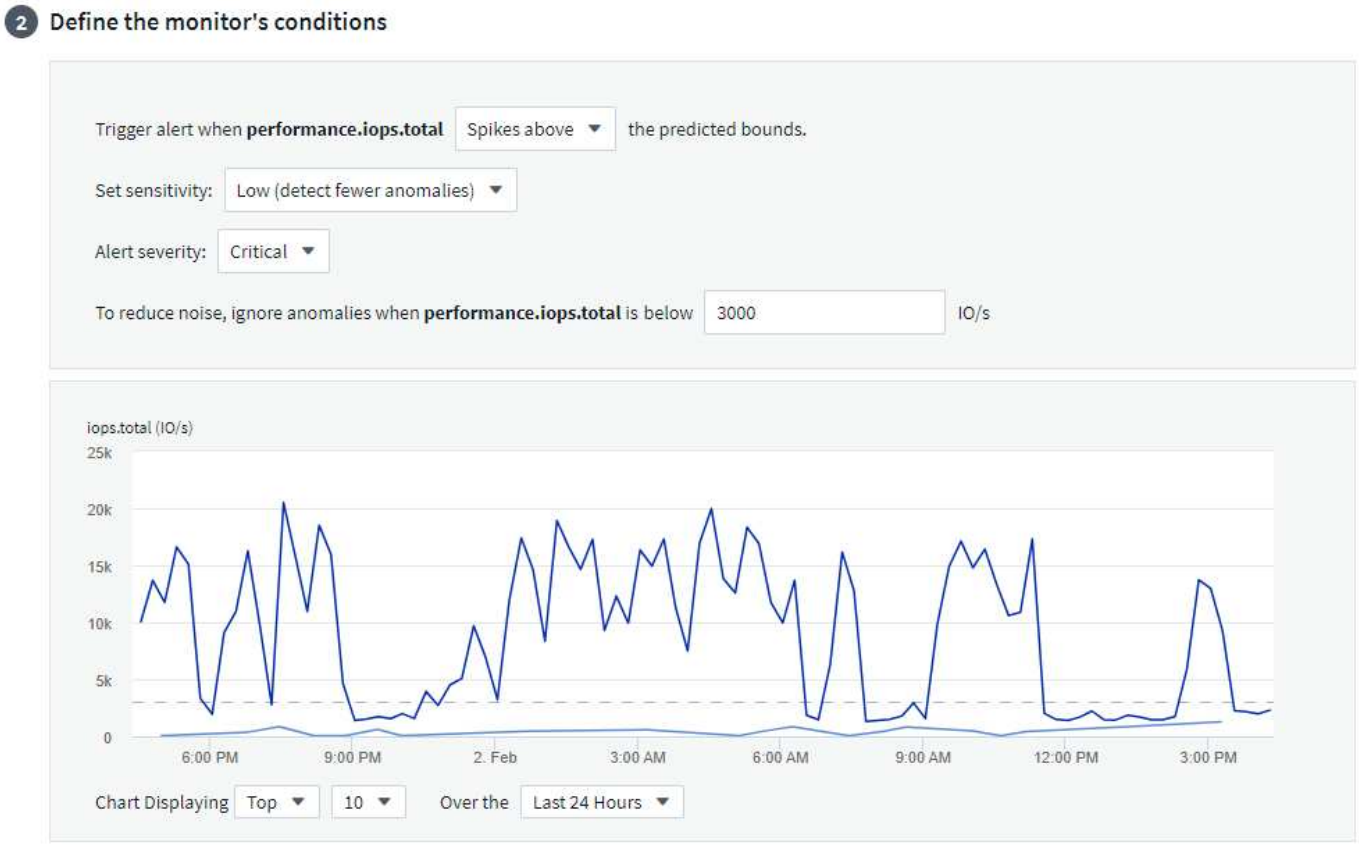


Wählen Sie das Objekt und die Metrik aus, die Sie überwachen möchten. Sie können Filter und Gruppierungen wie bei anderen Monitortypen festlegen.

Legen Sie als Nächstes die Bedingungen für den Monitor fest.

- Lösen Sie eine Warnung aus, wenn die ausgewählte Metrik entweder über die vorhergesagten Grenzen *steigt*, *unter diese Grenzen fällt* oder beides.

- Stellen Sie die Empfindlichkeit auf *Mittel*, *Niedrig* (es werden weniger Anomalien erkannt) oder *Hoch* (es werden mehr Anomalien erkannt) ein.
- Bestimmen Sie, ob die Warnstufe *Kritisch* oder *Warnung* ist.
- Legen Sie optional einen Wert fest, unterhalb dessen Anomalien *ignoriert* werden. Dies kann zur Lärmreduzierung beitragen. Dieser Wert wird im Beispieldiagramm als gestrichelte Linie angezeigt.



Abschließend können Sie eine Übermittlungsmethode für die Warnungen konfigurieren (E-Mail, Webhook oder beides), dem Monitor eine optionale Beschreibung oder Korrekturmaßnahmen zuweisen und den Monitor bei Bedarf einer benutzerdefinierten Gruppe hinzufügen.

Speichern Sie den Monitor unter einem aussagekräftigen Namen und fertig.

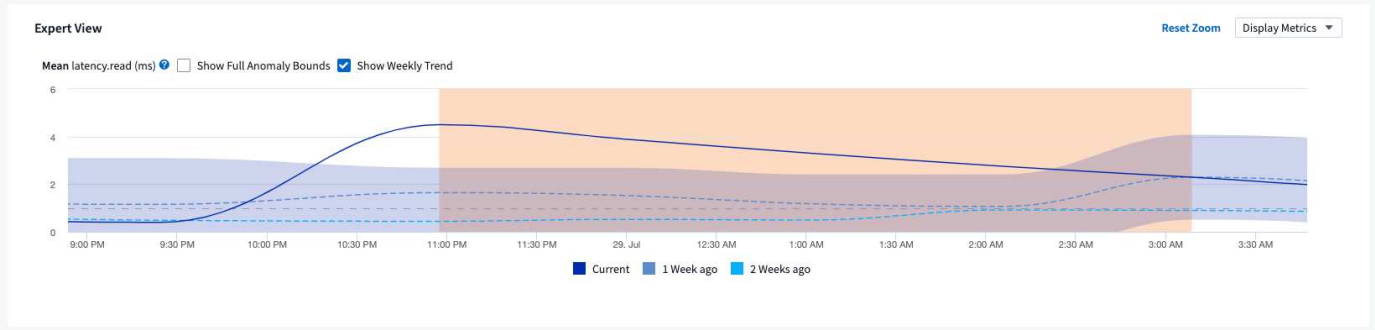
Nach der Erstellung analysiert der Monitor die Daten der vorherigen Woche, um eine erste Basislinie festzulegen. Die Anomalieerkennung wird mit der Zeit und mit zunehmender Historie genauer.

> Wenn ein Monitor erstellt wird, prüft DII alle vorhandenen Daten der vorherigen Woche auf signifikante Datenspitzen oder -abfälle. Diese werden als Anomalien betrachtet. Während der ersten Woche nach der Monitorerstellung (der „Lernphase“) besteht die Möglichkeit, dass es bei den Warnungen zu verstärktem „Rauschen“ kommt. Um dieses Rauschen zu mildern, werden nur Spitzen oder Einbrüche, die länger als 30 Minuten andauern, als Anomalien betrachtet und lösen Warnungen aus. Wenn in der darauffolgenden Woche weitere Daten analysiert werden, nimmt das Rauschen normalerweise ab und ein signifikanter Anstieg oder Abfall, der länger anhält, wird als Anomalie betrachtet.

Anzeigen der Anomalien

Auf einer Warnmeldungs-Landingpage werden Warnmeldungen, die bei der Erkennung von Anomalien

ausgelöst werden, im Diagramm durch ein hervorgehobenes Band angezeigt, und zwar von dem Zeitpunkt an, als die Metrik die vorhergesagten Grenzen überschritt, bis zu dem Zeitpunkt, als sie wieder innerhalb dieser Grenzen lag.



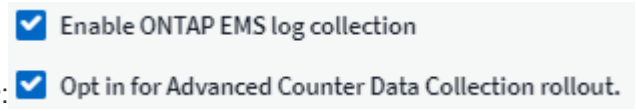
Beim Anzeigen eines Anomaliediagramms auf einer Warnmeldungs-Zielseite können Sie die folgenden Optionen auswählen:

- Wöchentlicher Trend: Vergleichen Sie Werte mit der gleichen Uhrzeit und dem gleichen Tag der vorherigen Wochen für bis zu 5 vorherige Wochen.
- Vollständige Anomaliegrenzen: Standardmäßig konzentriert sich das Diagramm auf den Metrikwert, damit Sie das Metrikverhalten besser analysieren können. Wählen Sie diese Option aus, um die vollständigen Anomaliegrenzen (Maximalwert usw.) anzuzeigen.

Sie können auch Objekte anzeigen, die zur Anomalie beigetragen haben, indem Sie diese im Leistungsbereich der Zielseite auswählen. Das Diagramm zeigt das Verhalten der ausgewählten Objekte.

Systemmonitore

Data Infrastructure Insights umfasst eine Reihe systemdefinierter Monitore für Metriken und Protokolle. Die verfügbaren Systemmonitore hängen von den auf Ihrem Mandanten vorhandenen Datensammlern ab. Aus diesem Grund können sich die in Data Infrastructure Insights verfügbaren Monitore ändern, wenn Datensammler hinzugefügt oder ihre Konfigurationen geändert werden.

Viele Systemmonitore befinden sich standardmäßig im Status *Pausiert*. Sie können einen Systemmonitor aktivieren, indem Sie die Option *Fortsetzen* für den Monitor auswählen. Stellen Sie sicher, dass „Erweiterte Zählerdatenerfassung“ und „ONTAP EMS-Protokollerfassung aktivieren“ im Datensammler aktiviert sind. Diese Optionen finden Sie im ONTAP Data Collector unter *Erweiterte Konfiguration*: 

Inhaltsverzeichnis:[]

Monitorbeschreibungen

Systemdefinierte Monitore bestehen aus vordefinierten Metriken und Bedingungen sowie Standardbeschreibungen und Korrekturmaßnahmen, die nicht geändert werden können. Sie *können* die Benachrichtigungsempfängerliste für systemdefinierte Monitore ändern. Um die Kennzahlen, Bedingungen, Beschreibungen und Korrekturmaßnahmen anzuzeigen oder die Empfängerliste zu ändern, öffnen Sie eine systemdefinierte Monitorgruppe und klicken Sie in der Liste auf den Monitornamen.

Systemdefinierte Monitorgruppen können nicht geändert oder entfernt werden.

Die folgenden systemdefinierten Monitore sind in den angegebenen Gruppen verfügbar.

- * ONTAP -Infrastruktur* umfasst Monitore für infrastrukturbezogene Probleme in ONTAP Clustern.
- * ONTAP Workload-Beispiele* umfassen Monitore für Workload-bezogene Probleme.
- Monitore in beiden Gruppen befinden sich standardmäßig im Status „Angehalten“.

Nachfolgend sind die Systemmonitore aufgeführt, die derzeit in Data Infrastructure Insights enthalten sind:

Metrische Monitore

Monitorname	Schwere	Monitorbeschreibung	Korrekturmaßnahme

Hohe Auslastung der Fiber Channel-Ports	KRITISCH	Fiber Channel Protocol-Ports werden zum Empfangen und Übertragen des SAN-Verkehrs zwischen dem Kundenhostsystem und den ONTAP LUNs verwendet. Eine hohe Portauslastung führt zu einem Engpass und beeinträchtigt letztendlich die Leistung sensibler Fiber Channel Protocol-Workloads. … Eine Warnmeldung weist darauf hin, dass geplante Maßnahmen zum Ausgleich des Netzwerkverkehrs ergriffen werden sollten. … Eine kritische Meldung weist darauf hin, dass eine Dienstunterbrechung unmittelbar bevorsteht und Notfallmaßnahmen zum Ausgleich des Netzwerkverkehrs ergriffen werden sollten, um die Dienstkontinuität sicherzustellen.	Wenn ein kritischer Schwellenwert überschritten wird, sollten Sie sofortige Maßnahmen ergreifen, um die Dienstunterbrechung zu minimieren: 1. Verschieben Sie Workloads auf einen anderen FCP-Port mit geringerer Auslastung. 2. Beschränken Sie den Datenverkehr bestimmter LUNs auf unbedingt erforderliche Aufgaben, entweder über QoS-Richtlinien in ONTAP oder über die Konfiguration auf Hostseite, um die Auslastung der FCP-Ports zu verringern. … Wenn der Warnschwellenwert überschritten wird, planen Sie die folgenden Maßnahmen: 1. Konfigurieren Sie mehrere FCP-Ports zur Abwicklung des Datenverkehrs, sodass die Portauslastung auf mehrere Ports verteilt wird. 2. Verschieben Sie Workloads auf einen anderen FCP-Port mit geringerer Auslastung. 3. Beschränken Sie den Datenverkehr bestimmter LUNs auf unbedingt erforderliche Aufgaben, entweder über QoS-Richtlinien in ONTAP oder über die Konfiguration auf Hostseite, um die Auslastung der FCP-Ports zu verringern.

Lun-Latenz hoch	KRITISCH	LUNs sind Objekte, die den E/A-Verkehr bedienen, der häufig von leistungsempfindlichen Anwendungen wie Datenbanken verursacht wird. Hohe LUN-Latenzen bedeuten, dass die Anwendungen selbst darunter leiden und ihre Aufgaben nicht erfüllen können. … Eine Warnmeldung weist darauf hin, dass geplante Maßnahmen ergriffen werden sollten, um die LUN auf den entsprechenden Knoten oder das entsprechende Aggregat zu verschieben. … Eine kritische Meldung weist darauf hin, dass eine Dienstunterbrechung unmittelbar bevorsteht und Notfallmaßnahmen ergriffen werden sollten, um die Dienstkontinuität sicherzustellen. Die erwarteten Latenzen basieren auf dem Medientyp: SSD bis zu 1–2 Millisekunden, SAS bis zu 8–10 Millisekunden und SATA HDD 17–20 Millisekunden	Wenn ein kritischer Schwellenwert überschritten wird, sollten Sie die folgenden Maßnahmen in Betracht ziehen, um Dienstunterbrechungen zu minimieren: Wenn mit der LUN oder ihrem Volume eine QoS-Richtlinie verknüpft ist, bewerten Sie deren Schwellenwerte und überprüfen Sie, ob diese zu einer Drosselung der LUN-Arbeitslast führen. … Wenn der Warnschwellenwert überschritten wird, planen Sie die folgenden Maßnahmen: 1. Wenn das Aggregat ebenfalls eine hohe Auslastung aufweist, verschieben Sie die LUN in ein anderes Aggregat. 2. Wenn der Knoten ebenfalls stark ausgelastet ist, verschieben Sie das Volume auf einen anderen Knoten oder reduzieren Sie die Gesamtarbeitslast des Knotens. 3. Wenn der LUN oder ihrem Volume eine QoS-Richtlinie zugeordnet ist, bewerten Sie deren Schwellenwerte und überprüfen Sie, ob diese zu einer Drosselung der LUN-Arbeitslast führen.

Hohe Netzwerk-Port-Auslastung	KRITISCH	Netzwerkports werden zum Empfangen und Übertragen des NFS-, CIFS- und iSCSI-Protokollverkehrs zwischen den Hostsystemen des Kunden und den ONTAP -Volumes verwendet. Wenn die Portauslastung hoch ist, wird dies zu einem Engpass und beeinträchtigt letztendlich die Leistung von NFS-, CIFS- und iSCSI-Workloads. … Eine Warnmeldung weist darauf hin, dass geplante Maßnahmen zum Ausgleich des Netzwerkverkehrs ergriffen werden sollten. … Eine kritische Meldung weist darauf hin, dass eine Dienstunterbrechung unmittelbar bevorsteht und Notfallmaßnahmen ergriffen werden sollten, um den Netzwerkverkehr auszugleichen und so die Dienstkontinuität sicherzustellen.	Wenn ein kritischer Schwellenwert überschritten wird, sollten Sie die folgenden Sofortmaßnahmen ergreifen, um die Dienstunterbrechung zu minimieren: 1. Beschränken Sie den Datenverkehr bestimmter Volumes auf die unbedingt erforderlichen Aufgaben, entweder über QoS-Richtlinien in ONTAP oder über eine hostseitige Analyse, um die Auslastung der Netzwerkports zu verringern. 2. Konfigurieren Sie ein oder mehrere Volumes so, dass sie einen anderen, weniger ausgelasteten Netzwerkport verwenden. … Wenn der Warnschwellenwert überschritten wird, sollten Sie die folgenden Sofortmaßnahmen in Betracht ziehen: 1. Konfigurieren Sie mehrere Netzwerkports zur Abwicklung des Datenverkehrs, sodass die Portauslastung auf mehrere Ports verteilt wird. 2. Konfigurieren Sie ein oder mehrere Volumes so, dass sie einen anderen, weniger ausgelasteten Netzwerkport verwenden.

NVMe-Namespace-Latenz hoch	KRITISCH	NVMe-Namespaces sind Objekte, die den E/A-Verkehr bedienen, der von leistungsempfindlichen Anwendungen wie Datenbanken gesteuert wird. Eine hohe Latenz der NVMe-Namespaces bedeutet, dass die Anwendungen selbst darunter leiden und ihre Aufgaben nicht erfüllen können. … Eine Warnmeldung weist darauf hin, dass geplante Maßnahmen ergriffen werden sollten, um die LUN auf den entsprechenden Knoten oder das entsprechende Aggregat zu verschieben. … Eine kritische Meldung weist darauf hin, dass eine Dienstunterbrechung unmittelbar bevorsteht und Notfallmaßnahmen ergriffen werden sollten, um die Dienstkontinuität sicherzustellen.	Wenn ein kritischer Schwellenwert überschritten wird, sollten Sie sofortige Maßnahmen in Betracht ziehen, um Dienstunterbrechungen zu minimieren: Wenn dem NVMe-Namespace oder seinem Volume eine QoS-Richtlinie zugewiesen ist, prüfen Sie dessen Grenzwerte, falls diese zu einer Drosselung der NVMe-Namespace-Workload führen. … Wenn der Warnschwellenwert überschritten wird, sollten Sie die folgenden Maßnahmen in Erwägung ziehen: 1. Wenn das Aggregat ebenfalls eine hohe Auslastung aufweist, verschieben Sie die LUN in ein anderes Aggregat. 2. Wenn der Knoten ebenfalls stark ausgelastet ist, verschieben Sie das Volume auf einen anderen Knoten oder reduzieren Sie die Gesamtarbeitslast des Knotens. 3. Wenn dem NVMe-Namespace oder seinem Volume eine QoS-Richtlinie zugewiesen ist, prüfen Sie die Grenzwerte, falls diese zu einer Drosselung der NVMe-Namespace-Workload führen.

QTree-Kapazität voll	KRITISCH	Ein Qtree ist ein logisch definiertes Dateisystem, das als spezielles Unterverzeichnis des Stammverzeichnisses innerhalb eines Volumes existieren kann. Jeder Qtree verfügt über ein Standardspeicherkontingent oder ein durch eine Kontingentrichtlinie definiertes Kontingent, um die im Baum gespeicherte Datenmenge innerhalb der Volumekapazität zu begrenzen. … Eine Warnmeldung weist darauf hin, dass geplante Maßnahmen zur Vergrößerung des Speicherplatzes ergriffen werden sollten. … Eine kritische Meldung weist darauf hin, dass eine Dienstunterbrechung unmittelbar bevorsteht und Notfallmaßnahmen ergriffen werden sollten, um Speicherplatz freizugeben und die Dienstkontinuität sicherzustellen.	Wenn ein kritischer Schwellenwert überschritten wird, sollten Sie sofortige Maßnahmen ergreifen, um die Dienstunterbrechung zu minimieren: 1. Erhöhen Sie den Platz des Qtree, um dem Wachstum gerecht zu werden. 2. Löschen Sie nicht benötigte Daten, um Speicherplatz freizugeben. … Wenn der Warnschwellenwert überschritten wird, planen Sie die folgenden Sofortmaßnahmen: 1. Erhöhen Sie den Platz des Qtree, um dem Wachstum gerecht zu werden. 2. Löschen Sie nicht benötigte Daten, um Speicherplatz freizugeben.

QTree-Kapazitätsgrenze	KRITISCH	Ein Qtree ist ein logisch definiertes Dateisystem, das als spezielles Unterverzeichnis des Stammverzeichnisses innerhalb eines Volumes existieren kann. Jeder Qtree verfügt über ein in KBytes gemessenes Speicherplatzkontingent, das zum Speichern von Daten verwendet wird, um das Wachstum des Benutzerdatenvolumens zu kontrollieren und seine Gesamtkapazität nicht zu überschreiten. … Ein Qtree verwaltet ein weiches Speicherkapazitätskontingent, das den Benutzer proaktiv warnt, bevor das Gesamtkapazitätskontingentlimit im Qtree erreicht wird und keine Daten mehr gespeichert werden können. Durch die Überwachung der in einem Qtree gespeicherten Datenmenge wird sichergestellt, dass der Benutzer einen unterbrechungsfreien Datendienst erhält.	Wenn ein kritischer Schwellenwert überschritten wird, sollten Sie die folgenden Sofortmaßnahmen ergreifen, um die Dienstunterbrechung zu minimieren: 1. Erhöhen Sie das Baumflächenkontingent, um dem Wachstum Rechnung zu tragen 2. Weisen Sie den Benutzer an, unerwünschte Daten im Baum zu löschen, um Speicherplatz freizugeben

QTree-Kapazitäts-Softlimit	WARNING (Warnung)	Ein Qtree ist ein logisch definiertes Dateisystem, das als spezielles Unterverzeichnis des Stammverzeichnisses innerhalb eines Volumes existieren kann. Jeder Qtree verfügt über ein in KBytes gemessenes Speicherplatzkontingent, das er zum Speichern von Daten verwenden kann, um das Wachstum des Benutzerdatenvolumens zu kontrollieren und seine Gesamtkapazität nicht zu überschreiten. … Ein Qtree verwaltet ein weiches Speicherkapazitätskontingent, das den Benutzer proaktiv warnt, bevor das Gesamtkapazitätskontingentlimit im Qtree erreicht wird und keine Daten mehr gespeichert werden können. Durch die Überwachung der in einem Qtree gespeicherten Datenmenge wird sichergestellt, dass der Benutzer einen unterbrechungsfreien Datendienst erhält.	Wenn der Warnschwellenwert überschritten wird, sollten Sie die folgenden Sofortmaßnahmen in Betracht ziehen: 1. Erhöhen Sie das Baumplatzkontingent, um dem Wachstum Rechnung zu tragen. 2. Weisen Sie den Benutzer an, nicht benötigte Daten im Baum zu löschen, um Speicherplatz freizugeben.

QTree-Dateien – hartes Limit	KRITISCH	Ein Qtree ist ein logisch definiertes Dateisystem, das als spezielles Unterverzeichnis des Stammverzeichnisses innerhalb eines Volumes existieren kann. Jeder Qtree verfügt über ein Kontingent für die Anzahl der Dateien, die er enthalten kann, um eine verwaltbare Dateisystemgröße innerhalb des Datenträgers aufrechtzuerhalten. … Ein Qtree verwaltet ein festes Dateianzahlkontingent, über dem neue Dateien im Baum abgelehnt werden. Durch die Überwachung der Anzahl der Dateien innerhalb eines Qtree wird sichergestellt, dass der Benutzer einen unterbrechungsfreien Datendienst erhält.	Wenn ein kritischer Schwellenwert überschritten wird, sollten Sie sofortige Maßnahmen ergreifen, um die Dienstunterbrechung zu minimieren: 1. Erhöhen Sie das Dateianzahlkontingent für den Qtree. 2. Löschen Sie unerwünschte Dateien aus dem Qtree-Dateisystem.

QTree-Dateien Soft Limit	WARNING (Warnung)	Ein Qtree ist ein logisch definiertes Dateisystem, das als spezielles Unterverzeichnis des Stammverzeichnisses innerhalb eines Volumes existieren kann. Jeder Qtree verfügt über ein Kontingent für die Anzahl der Dateien, die er enthalten kann, um eine verwaltbare Dateisystemgröße innerhalb des Datenträgers aufrechtzuerhalten. … Ein Qtree verwaltet ein weiches Dateianzahlkontingent, um den Benutzer proaktiv zu warnen, bevor das Dateilimit im Qtree erreicht wird und keine weiteren Dateien mehr gespeichert werden können. Durch die Überwachung der Anzahl der Dateien innerhalb eines Qtree wird sichergestellt, dass der Benutzer einen unterbrechungsfreien Datendienst erhält.	Wenn der Warnschwellenwert überschritten wird, planen Sie die folgenden Sofortmaßnahmen: 1. Erhöhen Sie das Dateianzahlkontingent für den Qtree. 2. Löschen Sie unerwünschte Dateien aus dem Qtree-Dateisystem.

Snapshot-Reservespeicherplatz voll	KRITISCH	Die Speicherkapazität eines Datenträgers ist zum Speichern von Anwendungs- und Kundendaten erforderlich. Ein Teil dieses Speicherplatzes, der sogenannte reservierte Snapshot-Speicherplatz, wird zum Speichern von Snapshots verwendet, die einen lokalen Schutz der Daten ermöglichen. Je mehr neue und aktualisierte Daten im ONTAP Volume gespeichert werden, desto mehr Snapshot-Kapazität wird verwendet und desto weniger Snapshot-Speicherkapazität steht für zukünftige neue oder aktualisierte Daten zur Verfügung. Wenn die Snapshot-Datenkapazität innerhalb eines Volumes den gesamten Snapshot-Reservespeicherplatz erreicht, kann dies dazu führen, dass der Kunde keine neuen Snapshot-Daten speichern kann und der Schutzgrad der Daten im Volume verringert wird. Durch die Überwachung der Snapshot-Kapazität des verwendeten Volumes wird die Kontinuität der Datendienste sichergestellt.	Wenn ein kritischer Schwellenwert überschritten wird, sollten Sie sofortige Maßnahmen ergreifen, um die Dienstunterbrechung zu minimieren: 1. Konfigurieren Sie Snapshots, um den Datenspeicherplatz im Volume zu nutzen, wenn die Snapshot-Reserve voll ist. 2. Löschen Sie einige ältere, nicht mehr benötigte Snapshots, um Speicherplatz freizugeben. … Wenn der Warnschwellenwert überschritten wird, planen Sie die folgenden Sofortmaßnahmen: 1. Erhöhen Sie den Snapshot-Reservespeicherplatz innerhalb des Volumes, um dem Wachstum Rechnung zu tragen. 2. Konfigurieren Sie Snapshots, um den Datenspeicherplatz im Volume zu nutzen, wenn die Snapshot-Reserve voll ist.

Speicherkapazitätsgrenze	KRITISCH	Wenn sich ein Speicherpool (Aggregat) füllt, verlangsamen sich die E/A-Vorgänge und werden schließlich gestoppt, was zu einem Speicherausfall führt. Eine Warnmeldung weist darauf hin, dass bald eine geplante Aktion durchgeführt werden sollte, um den minimalen freien Speicherplatz wiederherzustellen. Eine kritische Warnung weist darauf hin, dass eine Dienstunterbrechung unmittelbar bevorsteht und Notfallmaßnahmen ergriffen werden sollten, um Speicherplatz freizugeben und die Dienstkontinuität sicherzustellen.	Wenn ein kritischer Schwellenwert überschritten wird, sollten Sie sofort die folgenden Maßnahmen in Betracht ziehen, um die Dienstunterbrechung zu minimieren: 1. Löschen Sie Snapshots auf nicht kritischen Volumes. 2. Löschen Sie Volumes oder LUNs, die keine wesentlichen Arbeitslasten darstellen und die möglicherweise aus externen Speicherkopien wiederhergestellt werden können.……Wenn der Warnschwellenwert überschritten wird, planen Sie die folgenden Sofortmaßnahmen: 1. Verschieben Sie ein oder mehrere Volumes an einen anderen Speicherort. 2. Fügen Sie mehr Speicherkapazität hinzu. 3. Ändern Sie die Einstellungen für die Speichereffizienz oder verschieben Sie inaktive Daten in den Cloud-Speicher.

Speicherleistungsgrenze	KRITISCH	Wenn ein Speichersystem seine Leistungsgrenze erreicht, verlangsamen sich die Vorgänge, die Latenz steigt und es kann zu Ausfällen bei Arbeitslasten und Anwendungen kommen. ONTAP wertet die Speicherpoolauslastung für Workloads aus und schätzt, wie viel Prozent der Leistung verbraucht wurden. … Eine Warnmeldung weist darauf hin, dass geplante Maßnahmen zur Reduzierung der Speicherpoolauslastung ergriffen werden sollten, um sicherzustellen, dass genügend Speicherpoolleistung übrig bleibt, um Workloadspitzen zu bewältigen. … Eine kritische Meldung weist darauf hin, dass ein Leistungsabfall unmittelbar bevorsteht und Notfallmaßnahmen ergriffen werden sollten, um die Speicherpoolauslastung zu reduzieren und so die Servicekontinuität sicherzustellen.	Wenn ein kritischer Schwellenwert überschritten wird, sollten Sie die folgenden Sofortmaßnahmen ergreifen, um die Dienstunterbrechung zu minimieren: 1. Unterbrechen Sie geplante Aufgaben wie Snapshots oder SnapMirror -Replikation. 2. Leerlauf, nicht unbedingt erforderliche Arbeitslasten. … Wenn der Warnschwellenwert überschritten wird, ergreifen Sie sofort die folgenden Maßnahmen: 1. Verschieben Sie eine oder mehrere Workloads an einen anderen Speicherort. 2. Fügen Sie weitere Speicherknoten (AFF) oder Festplattenregale (FAS) hinzu und verteilen Sie die Arbeitslasten neu 3. Ändern Sie die Arbeitslasteigenschaften (Blockgröße, Anwendungs-Caching).

Hartes Limit für die Benutzerkontingentkapazität	KRITISCH	ONTAP erkennt die Benutzer von Unix- oder Windows-Systemen, die über die Rechte zum Zugriff auf Volumes, Dateien oder Verzeichnisse innerhalb eines Volumes verfügen. Daher ermöglicht ONTAP den Kunden, die Speicherkapazität für ihre Benutzer oder Benutzergruppen ihrer Linux- oder Windows-Systeme zu konfigurieren. Das Benutzer- oder Gruppenrichtlinienkontingent begrenzt den Speicherplatz, den der Benutzer für seine eigenen Daten nutzen kann. … Eine harte Begrenzung dieses Kontingents ermöglicht die Benachrichtigung des Benutzers, wenn die innerhalb des Volumes genutzte Kapazität kurz vor dem Erreichen des Gesamtkapazitätskontingents liegt. Durch die Überwachung der innerhalb eines Benutzer- oder Gruppenkontingents gespeicherten Datenmenge wird sichergestellt, dass der Benutzer einen unterbrechungsfreien Datendienst erhält.	Wenn ein kritischer Schwellenwert überschritten wird, sollten Sie die folgenden Sofortmaßnahmen ergreifen, um die Dienstunterbrechung zu minimieren: 1. Erhöhen Sie den Speicherplatz des Benutzer- oder Gruppenkontingents, um dem Wachstum Rechnung zu tragen. 2. Weisen Sie den Benutzer oder die Gruppe an, nicht benötigte Daten zu löschen, um Speicherplatz freizugeben.

Soft-Limit für Benutzerkontingentkapazität	WARNING (Warnung)	ONTAP erkennt die Benutzer von Unix- oder Windows-Systemen, die über die Rechte zum Zugriff auf Volumes, Dateien oder Verzeichnisse innerhalb eines Volumes verfügen. Daher ermöglicht ONTAP den Kunden, die Speicherkapazität für ihre Benutzer oder Benutzergruppen ihrer Linux- oder Windows-Systeme zu konfigurieren. Das Benutzer- oder Gruppenrichtlinienkontingent begrenzt den Speicherplatz, den der Benutzer für seine eigenen Daten nutzen kann. … Eine weiche Begrenzung dieses Kontingents ermöglicht eine proaktive Benachrichtigung des Benutzers, wenn die innerhalb des Volumes genutzte Kapazität das Gesamtkapazitätskontingent erreicht. Durch die Überwachung der innerhalb eines Benutzer- oder Gruppenkontingents gespeicherten Datenmenge wird sichergestellt, dass der Benutzer einen unterbrechungsfreien Datendienst erhält.	Wenn der Warnschwellenwert überschritten wird, planen Sie die folgenden Sofortmaßnahmen: 1. Erhöhen Sie den Speicherplatz des Benutzer- oder Gruppenkontingents, um dem Wachstum Rechnung zu tragen. 2. Löschen Sie nicht benötigte Daten, um Speicherplatz freizugeben.

Volumenkapazität Voll	KRITISCH	Die Speicherkapazität eines Datenträgers ist zum Speichern von Anwendungs- und Kundendaten erforderlich. Je mehr Daten im ONTAP -Volume gespeichert werden, desto geringer ist die Speicherverfügbarkeit für zukünftige Daten. Wenn die Datenspeicherkapazität innerhalb eines Volumes die Gesamtspeicherkapazität erreicht, kann dies dazu führen, dass der Kunde aufgrund fehlender Speicherkapazität keine Daten speichern kann. Durch die Überwachung der genutzten Speicherkapazität wird die Kontinuität der Datendienste gewährleistet.	Wenn ein kritischer Schwellenwert überschritten wird, sollten Sie die folgenden Sofortmaßnahmen ergreifen, um die Dienstunterbrechung zu minimieren: 1. Erhöhen Sie den Speicherplatz des Volumens, um dem Wachstum gerecht zu werden. 2. Löschen Sie nicht benötigte Daten, um Speicherplatz freizugeben. 3. Wenn Snapshot-Kopien mehr Speicherplatz belegen als die Snapshot-Reserve, löschen Sie alte Snapshots oder aktivieren Sie die automatische Löschung von Volume-Snapshots. … Wenn der Warnschwellenwert überschritten wird, planen Sie die folgenden sofortigen Maßnahmen: 1. Erhöhen Sie den Platz im Volumen, um dem Wachstum gerecht zu werden 2. Wenn Snapshot-Kopien mehr Speicherplatz belegen als die Snapshot-Reserve, löschen Sie alte Snapshots oder aktivieren Sie die automatische Löschung von Volume-Snapshots.……

Volume-Inodes-Limit	KRITISCH	Volumes, die Dateien speichern, verwenden Indexknoten (Inode) zum Speichern von Dateimetadaten. Wenn ein Volume seine Inode-Zuweisung erschöpft, können keine weiteren Dateien hinzugefügt werden. … Eine Warnmeldung weist darauf hin, dass geplante Maßnahmen ergriffen werden sollten, um die Anzahl der verfügbaren Inodes zu erhöhen. … Eine kritische Meldung weist darauf hin, dass die Erschöpfung des Dateilimits unmittelbar bevorsteht und Notfallmaßnahmen ergriffen werden sollten, um Inodes freizugeben und so die Dienstkontinuität sicherzustellen.	Wenn ein kritischer Schwellenwert überschritten wird, sollten Sie die folgenden Sofortmaßnahmen ergreifen, um die Dienstunterbrechung zu minimieren: 1. Erhöhen Sie den Inodes-Wert für das Volume. Wenn der Inodes-Wert bereits den Maximalwert erreicht hat, teilen Sie das Volume in zwei oder mehr Volumes auf, da das Dateisystem über die maximale Größe hinausgewachsen ist. 2. Verwenden Sie FlexGroup , da es bei der Unterbringung großer Dateisysteme hilft. … Wenn der Warnschwellenwert überschritten wird, planen Sie die folgenden Sofortmaßnahmen: 1. Erhöhen Sie den Inodes-Wert für das Volume. Wenn der Inodes-Wert bereits das Maximum erreicht hat, teilen Sie das Volume in zwei oder mehr Volumes auf, da das Dateisystem über die maximale Größe hinausgewachsen ist. 2. Verwenden Sie FlexGroup , da es bei der Unterbringung großer Dateisysteme hilft

Lautstärkelatenz hoch	KRITISCH	Volumes sind Objekte, die den E/A-Verkehr bedienen, der häufig von leistungsempfindlichen Anwendungen wie DevOps-Anwendungen, Home-Verzeichnissen und Datenbanken gesteuert wird. Hohe Volumenlatenzen können dazu führen, dass die Anwendungen selbst darunter leiden und ihre Aufgaben nicht erfüllen können. Die Überwachung der Volume-Latenzen ist entscheidend, um eine konsistente Anwendungsleistung aufrechtzuerhalten. Je nach Medientyp sind folgende Latenzen zu erwarten: SSD bis zu 1–2 Millisekunden, SAS bis zu 8–10 Millisekunden und SATA-HDD 17–20 Millisekunden.	Wenn ein kritischer Schwellenwert überschritten wird, sollten Sie die folgenden Sofortmaßnahmen ergreifen, um die Dienstunterbrechung zu minimieren: Wenn dem Volume eine QoS-Richtlinie zugewiesen ist, prüfen Sie dessen Grenzwerte, falls diese zu einer Drosselung der Volume-Arbeitslast führen. … Wenn der Warnschwellenwert überschritten wird, sollten Sie die folgenden Sofortmaßnahmen in Betracht ziehen: 1. Wenn das Aggregat ebenfalls eine hohe Auslastung aufweist, verschieben Sie das Volume auf ein anderes Aggregat. 2. Wenn dem Volume eine QoS-Richtlinie zugewiesen ist, prüfen Sie dessen Grenzwerte, um zu prüfen, ob diese zu einer Drosselung der Volume-Arbeitslast führen. 3. Wenn der Knoten ebenfalls stark ausgelastet ist, verschieben Sie das Volume auf einen anderen Knoten oder reduzieren Sie die Gesamtarbeitslast des Knotens.
Monitorname	Schwere	Monitorbeschreibung	Korrekturmaßnahme

Knoten mit hoher Latenz	WARNUNG / KRITISCH	Die Knotenlatenz hat ein Niveau erreicht, bei dem sie die Leistung der Anwendungen auf dem Knoten beeinträchtigen könnte. Eine geringere Knotenlatenz gewährleistet eine konsistente Leistung der Anwendungen. Die erwarteten Latenzen je nach Medientyp sind: SSD bis zu 1–2 Millisekunden, SAS bis zu 8–10 Millisekunden und SATA HDD 17–20 Millisekunden.	Wenn ein kritischer Schwellenwert überschritten wird, sollten sofort Maßnahmen ergriffen werden, um die Dienstunterbrechung zu minimieren: 1. Unterbrechen Sie geplante Aufgaben, Snapshots oder die SnapMirror -Replikation 2. Reduzieren Sie die Nachfrage nach Workloads mit niedrigerer Priorität über QoS-Grenzen 3. Deaktivieren Sie nicht unbedingt erforderliche Workloads. Erwägen Sie sofortige Maßnahmen, wenn der Warnschwellenwert überschritten wird: 1. Verschieben Sie einen oder mehrere Workloads an einen anderen Speicherort 2. Reduzieren Sie die Nachfrage nach Workloads mit niedrigerer Priorität über QoS-Grenzen 3. Fügen Sie weitere Speicherknoten (AFF) oder Festplattenregale (FAS) hinzu und verteilen Sie die Arbeitslasten neu 4. Ändern Sie die Arbeitslasteigenschaften (Blockgröße, Anwendungs-Caching usw.)

Knotenleistungsgrenze	WARNUNG / KRITISCH	Die Leistungsauslastung des Knotens hat ein Niveau erreicht, bei dem sie die Leistung der E/As und der vom Knoten unterstützten Anwendungen beeinträchtigen könnte. Eine geringe Knotenleistungsauslastung gewährleistet eine gleichbleibende Leistung der Anwendungen.	Um die Serviceunterbrechung bei einer Überschreitung eines kritischen Schwellenwerts zu minimieren, sollten umgehend Maßnahmen ergriffen werden: 1. Unterbrechen Sie geplante Aufgaben, Snapshots oder die SnapMirror -Replikation 2. Reduzieren Sie die Nachfrage nach Workloads mit niedrigerer Priorität über QoS-Grenzen 3. Deaktivieren Sie nicht unbedingt erforderliche Workloads. Erwägen Sie die folgenden Maßnahmen, wenn der Warnschwellenwert überschritten wird: 1. Verschieben Sie einen oder mehrere Workloads an einen anderen Speicherort 2. Reduzieren Sie die Nachfrage nach Workloads mit niedrigerer Priorität über QoS-Grenzen 3. Fügen Sie weitere Speicherknoten (AFF) oder Festplattenregale (FAS) hinzu und verteilen Sie die Arbeitslasten neu 4. Ändern Sie die Arbeitslasteigenschaften (Blockgröße, Anwendungs-Caching usw.)

Hohe Latenz der Speicher-VM	WARNUNG / KRITISCH	Die Latenz der Storage-VM (SVM) hat ein Niveau erreicht, bei dem sie die Leistung der Anwendungen auf der Storage-VM beeinträchtigen könnte. Eine geringere Speicher-VM-Latenz gewährleistet eine konsistente Leistung der Anwendungen. Die erwarteten Latenzen je nach Medientyp sind: SSD bis zu 1–2 Millisekunden, SAS bis zu 8–10 Millisekunden und SATA HDD 17–20 Millisekunden.	Wenn ein kritischer Schwellenwert überschritten wird, bewerten Sie sofort die Schwellenwerte für Volumes der Speicher-VM mit einer zugewiesenen QoS-Richtlinie, um zu überprüfen, ob sie eine Drosselung der Volume-Workloads verursachen. Erwägen Sie die folgenden Sofortmaßnahmen, wenn der Warnschwellenwert überschritten wird: 1. Wenn das Aggregat ebenfalls eine hohe Auslastung aufweist, verschieben Sie einige Volumes der Speicher-VM in ein anderes Aggregat. 2. Bewerten Sie für Volumes der Speicher-VM mit zugewiesener QoS-Richtlinie die Schwellenwerte, wenn diese zu einer Drosselung der Volume-Workloads führen 3. Wenn der Knoten eine hohe Auslastung aufweist, verschieben Sie einige Volumes der Speicher-VM auf einen anderen Knoten oder reduzieren Sie die Gesamtarbeitslast des Knotens

Hartes Limit für Benutzerkontingentdateien	KRITISCH	Die Anzahl der im Volume erstellten Dateien hat die kritische Grenze erreicht und es können keine weiteren Dateien erstellt werden. Durch die Überwachung der Anzahl der gespeicherten Dateien wird sichergestellt, dass der Benutzer einen unterbrechungsfreien Datendienst erhält.	Um Serviceunterbrechungen zu minimieren, wenn ein kritischer Schwellenwert überschritten wird, sind sofortige Maßnahmen erforderlich. … Erwägen Sie die Durchführung der folgenden Maßnahmen: 1. Erhöhen Sie das Dateianzahlkontingent für den jeweiligen Benutzer 2. Löschen Sie nicht benötigte Dateien, um den Druck auf das Dateikontingent für den jeweiligen Benutzer zu verringern
Soft-Limit für Benutzerkontingentdateien	WARNING (Warnung)	Die Anzahl der im Volume erstellten Dateien hat den Schwellenwert des Kontingents erreicht und liegt nahe der kritischen Grenze. Sie können keine weiteren Dateien erstellen, wenn das Kontingent die kritische Grenze erreicht. Durch die Überwachung der Anzahl der von einem Benutzer gespeicherten Dateien wird sichergestellt, dass der Benutzer einen unterbrechungsfreien Datendienst erhält.	Erwägen Sie sofortige Maßnahmen, wenn die Warnschwelle überschritten wird: 1. Erhöhen Sie das Dateianzahlkontingent für das spezifische Benutzerkontingent 2. Löschen Sie nicht benötigte Dateien, um den Druck auf das Dateikontingent für den jeweiligen Benutzer zu verringern

Volume-Cache-Fehlerquote	WARNUNG / KRITISCH	Die Volume Cache Miss Ratio ist der Prozentsatz der Leseanforderungen der Clientanwendungen, die von der Festplatte und nicht vom Cache zurückgegeben werden. Dies bedeutet, dass die Lautstärke den eingestellten Schwellenwert erreicht hat.	Wenn ein kritischer Schwellenwert überschritten wird, sollten sofort Maßnahmen ergriffen werden, um die Dienstunterbrechung zu minimieren: 1. Verschieben Sie einige Workloads vom Knoten des Volumes, um die E/A-Last 2 zu reduzieren. Falls er sich noch nicht auf dem Knoten des Volumes befindet, erhöhen Sie den WAFL Cache, indem Sie einen Flash Cache 3 kaufen und hinzufügen. Reduzieren Sie die Nachfrage nach Workloads mit niedrigerer Priorität auf demselben Knoten über QoS-Grenzwerte. Erwägen Sie sofortige Maßnahmen, wenn der Warnschwellenwert überschritten wird: 1. Verschieben Sie einige Workloads vom Knoten des Volumes, um die E/A-Last 2 zu reduzieren. Falls er sich noch nicht auf dem Knoten des Volumes befindet, erhöhen Sie den WAFL Cache, indem Sie einen Flash Cache 3 kaufen und hinzufügen. Verringern Sie die Nachfrage nach Workloads mit niedrigerer Priorität auf demselben Knoten über QoS-Grenzwerte 4. Ändern Sie die Arbeitslasteigenschaften (Blockgröße, Anwendungs-Caching usw.)

Volume Qtree-Kontingentüberbelegung	WARNUNG / KRITISCH	Volume Qtree Quota Overcommit gibt den Prozentsatz an, ab dem ein Volume als durch die Qtree-Kontingente überbelegt gilt. Der festgelegte Schwellenwert für das Qtree-Kontingent ist für das Volume erreicht. Durch die Überwachung der Überbelegung des Volume-Qtree-Kontingents wird sichergestellt, dass der Benutzer einen unterbrechungsfreien Datendienst erhält.	Wenn ein kritischer Schwellenwert überschritten wird, sollten sofort Maßnahmen ergriffen werden, um die Dienstunterbrechung zu minimieren: 1. Erhöhen Sie den Speicherplatz des Bandes 2. Löschen Sie nicht benötigte Daten. Wenn der Warnschwellenwert überschritten wird, sollten Sie den Speicherplatz des Datenträgers vergrößern.

Zurück nach oben

Protokollmonitore

Monitorname	Schwere	Beschreibung	Korrekturmaßnahme
AWS-Anmeldeinformationen nicht initialisiert	INFO	Dieses Ereignis tritt auf, wenn ein Modul versucht, auf rollenbasierte Anmeldeinformationen von Amazon Web Services (AWS) Identity and Access Management (IAM) aus dem Cloud-Anmeldeinformations-Thread zuzugreifen, bevor diese initialisiert werden.	Warten Sie, bis der Thread mit den Cloud-Anmeldeinformationen und das System die Initialisierung abgeschlossen haben.

Cloud-Ebene nicht erreichbar	KRITISCH	Ein Speicherknoten kann keine Verbindung zur Cloud Tier-Objektspeicher-API herstellen. Auf einige Daten kann nicht zugegriffen werden.	Wenn Sie lokale Produkte verwenden, führen Sie die folgenden Korrekturmaßnahmen durch: … Stellen Sie mithilfe des Befehls „network interface show“ sicher, dass Ihr Intercluster-LIF online und funktionsfähig ist. … Überprüfen Sie die Netzwerkkonnektivität zum Objektspeicherserver, indem Sie den Befehl „ping“ über das Intercluster-LIF des Zielknotens ausführen. … Stellen Sie Folgendes sicher: … Die Konfiguration Ihres Objektspeichers hat sich nicht geändert. … Die Anmelde- und Konnektivitätsinformationen sind weiterhin gültig. … Wenden Sie sich an den technischen Support von NetApp , wenn das Problem weiterhin besteht. Wenn Sie Cloud Volumes ONTAP verwenden, führen Sie die folgenden Korrekturmaßnahmen durch: …Stellen Sie sicher, dass sich die Konfiguration Ihres Objektspeichers nicht geändert hat.… Stellen Sie sicher, dass die Anmelde- und Verbindungsinformationen noch gültig sind. … Wenden Sie sich an den technischen Support von NetApp, wenn das Problem weiterhin besteht.

Festplatte außer Betrieb	INFO	Dieses Ereignis tritt ein, wenn eine Festplatte außer Betrieb genommen wird, weil sie als fehlerhaft markiert wurde, bereinigt wird oder in das Wartungscenter gelangt ist.	Keiner.
FlexGroup -Bestandteil Voll	KRITISCH	Ein Bestandteil eines FlexGroup -Volumes ist voll, was zu einer möglichen Dienstunterbrechung führen kann. Sie können weiterhin Dateien auf dem FlexGroup -Volume erstellen oder erweitern. Allerdings können keine der auf der Komponente gespeicherten Dateien geändert werden. Daher treten möglicherweise zufällige Fehlermeldungen wegen unzureichendem Speicherplatz auf, wenn Sie versuchen, Schreibvorgänge auf dem FlexGroup -Volume durchzuführen.	Es wird empfohlen, die Kapazität des FlexGroup -Volumes mit dem Befehl „volume modify -files +X“ zu erhöhen. …Alternativ können Sie Dateien aus dem FlexGroup -Volume löschen. Allerdings ist es schwierig festzustellen, welche Dateien beim Wähler gelandet sind.
Flexgroup-Bestandteil fast voll	WARNING (Warnung)	Ein Bestandteil eines FlexGroup -Volumes hat fast keinen Speicherplatz mehr, was zu einer möglichen Dienstunterbrechung führen kann. Dateien können erstellt und erweitert werden. Wenn jedoch der Speicherplatz der Komponente ausgeht, können Sie die Dateien auf der Komponente möglicherweise nicht anhängen oder ändern.	Es wird empfohlen, die Kapazität des FlexGroup -Volumes mit dem Befehl „volume modify -files +X“ zu erhöhen. …Alternativ können Sie Dateien aus dem FlexGroup -Volume löschen. Allerdings ist es schwierig festzustellen, welche Dateien beim Wähler gelandet sind.

FlexGroup -Bestandteil hat fast keine Inodes mehr	WARNING (Warnung)	Ein Bestandteil eines FlexGroup -Volumes hat fast keine Inodes mehr, was zu einer möglichen Dienstunterbrechung führen kann. Der Bestandteil erhält weniger Erstellungsanfragen als der Durchschnitt. Dies kann die Gesamtleistung des FlexGroup -Volumes beeinträchtigen, da die Anforderungen an Bestandteile mit mehr Inodes weitergeleitet werden.	Es wird empfohlen, die Kapazität des FlexGroup -Volumes mit dem Befehl „volume modify -files +X“ zu erhöhen. …Alternativ können Sie Dateien aus dem FlexGroup -Volume löschen. Allerdings ist es schwierig festzustellen, welche Dateien beim Wähler gelandet sind.
FlexGroup -Bestandteil außerhalb der Inodes	KRITISCH	Einem Bestandteil eines FlexGroup -Volumes sind die Inodes ausgegangen, was zu einer möglichen Dienstunterbrechung führen kann. Sie können für diesen Bestandteil keine neuen Dateien erstellen. Dies kann zu einer insgesamt unausgewogenen Verteilung der Inhalte über das FlexGroup -Volumen führen.	Es wird empfohlen, die Kapazität des FlexGroup -Volumes mit dem Befehl „volume modify -files +X“ zu erhöhen. …Alternativ können Sie Dateien aus dem FlexGroup -Volume löschen. Allerdings ist es schwierig festzustellen, welche Dateien beim Wähler gelandet sind.
LUN offline	INFO	Dieses Ereignis tritt auf, wenn eine LUN manuell offline geschaltet wird.	Bringen Sie die LUN wieder online.
Lüfter der Haupteinheit ausgefallen	WARNING (Warnung)	Ein oder mehrere Lüfter der Haupteinheit sind ausgefallen. Das System bleibt betriebsbereit. …Wenn der Zustand jedoch zu lange anhält, kann die Übertemperatur eine automatische Abschaltung auslösen.	Setzen Sie die ausgefallenen Lüfter neu ein. Wenn der Fehler weiterhin besteht, ersetzen Sie sie.
Lüfter der Haupteinheit im Warnzustand	INFO	Dieses Ereignis tritt auf, wenn sich ein oder mehrere Lüfter der Haupteinheit in einem Warnzustand befinden.	Ersetzen Sie die angegebenen Lüfter, um eine Überhitzung zu vermeiden.

NVRAM -Batterie schwach	WARNING (Warnung)	Die NVRAM Batteriekapazität ist kritisch niedrig. Wenn der Akku leer ist, kann es zu einem Datenverlust kommen. … Ihr System generiert und überträgt eine AutoSupport oder „Call Home“-Nachricht an den technischen Support von NetApp und die konfigurierten Ziele, sofern es entsprechend konfiguriert ist. Die erfolgreiche Zustellung einer AutoSupport -Nachricht verbessert die Problembestimmung und -lösung erheblich.	Führen Sie die folgenden Korrekturmaßnahmen durch: … Zeigen Sie den aktuellen Status, die Kapazität und den Ladezustand der Batterie mit dem Befehl „Systemknoten-Umgebungssensoren anzeigen“ an. … Wenn die Batterie vor Kurzem ausgetauscht wurde oder das System längere Zeit nicht betriebsbereit war, überwachen Sie die Batterie, um sicherzustellen, dass sie ordnungsgemäß geladen wird. … Wenden Sie sich an den technischen Support von NetApp , wenn die Batterielaufzeit weiterhin unter kritische Werte sinkt und das Speichersystem automatisch herunterfährt.
Serviceprozessor nicht konfiguriert	WARNING (Warnung)	Dieses Ereignis tritt wöchentlich auf, um Sie daran zu erinnern, den Serviceprozessor (SP) zu konfigurieren. Der SP ist ein physisches Gerät, das in Ihr System integriert wird, um Fernzugriff und Fernverwaltungsfunktionen bereitzustellen. Sie sollten den SP so konfigurieren, dass er seine volle Funktionalität nutzt.	Führen Sie die folgenden Korrekturmaßnahmen durch: … Konfigurieren Sie den SP mit dem Befehl „system service-processor network modify“. … Ermitteln Sie optional die MAC-Adresse des SP mit dem Befehl „system service-processor network show“. … Überprüfen Sie die SP Netzwerkkonfiguration mit dem Befehl „system service-processor network show“. … Überprüfen Sie mit dem Befehl „system service-processor autosupport invoke“, ob der SP eine AutoSupport E-Mail senden kann. HINWEIS: AutoSupport E-Mail-Hosts und -Empfänger sollten in ONTAP konfiguriert werden, bevor Sie diesen Befehl ausführen.

Serviceprozessor offline	KRITISCH	ONTAP empfängt keine Heartbeats mehr vom Serviceprozessor (SP), obwohl alle SP Wiederherstellungsmaßnahmen durchgeführt wurden. ONTAP kann den Zustand der Hardware ohne den SP nicht überwachen. … Das System wird heruntergefahren, um Hardwareschäden und Datenverlust zu verhindern. Richten Sie einen Panikalarm ein, um sofort benachrichtigt zu werden, wenn der SP offline geht.	Führen Sie einen Neustart des Systems durch, indem Sie die folgenden Aktionen ausführen: … Ziehen Sie den Controller aus dem Gehäuse. … Schieben Sie den Controller wieder hinein. … Schalten Sie den Controller wieder ein. … Wenn das Problem weiterhin besteht, ersetzen Sie das Controllermodul.
Regallüfter ausgefallen	KRITISCH	Der angegebene Kühllüfter oder das Lüftermodul des Regals ist ausgefallen. Die Festplatten im Regal erhalten möglicherweise nicht genügend Kühlluftstrom, was zu einem Festplattenausfall führen kann.	Führen Sie die folgenden Korrekturmaßnahmen durch: … Stellen Sie sicher, dass das Lüftermodul vollständig sitzt und gesichert ist. HINWEIS: Bei einigen Festplatten-Shelves ist der Lüfter in das Stromversorgungsmodul integriert. …Wenn das Problem weiterhin besteht, ersetzen Sie das Lüftermodul. …Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support von NetApp , um Hilfe zu erhalten.
Das System kann aufgrund eines Lüfterfehlers der Haupteinheit nicht betrieben werden	KRITISCH	Ein oder mehrere Lüfter der Haupteinheit sind ausgefallen, wodurch der Systembetrieb unterbrochen wird. Dies kann zu einem möglichen Datenverlust führen.	Ersetzen Sie die ausgefallenen Lüfter.

Nicht zugewiesene Datenträger	INFO	Dem System sind keine Festplatten zugewiesen – Kapazität wird verschwendet und Ihr System weist möglicherweise eine Fehlkonfiguration auf oder es wurden teilweise Konfigurationsänderungen vorgenommen.	Führen Sie die folgenden Korrekturmaßnahmen durch: … Ermitteln Sie mit dem Befehl „disk show -n“, welche Datenträger nicht zugewiesen sind. … Weisen Sie die Datenträger mit dem Befehl „disk assign“ einem System zu.
Antivirus-Server ausgelastet	WARNING (Warnung)	Der Antivirenserver ist zu ausgelastet, um neue Scananforderungen anzunehmen.	Wenn diese Meldung häufig auftritt, stellen Sie sicher, dass genügend Antivirenserver vorhanden sind, um die von der SVM generierte Virenscanlast zu bewältigen.
AWS-Anmeldeinformationen für IAM-Rolle abgelaufen	KRITISCH	Auf Cloud Volume ONTAP kann nicht mehr zugegriffen werden. Die rollenbasierten Anmeldeinformationen für Identity and Access Management (IAM) sind abgelaufen. Die Anmeldeinformationen werden mithilfe der IAM-Rolle vom Metadatenserver von Amazon Web Services (AWS) abgerufen und zum Signieren von API-Anfragen an Amazon Simple Storage Service (Amazon S3) verwendet.	Führen Sie Folgendes aus: … Melden Sie sich bei der AWS EC2-Verwaltungskonsole an. … Navigieren Sie zur Seite „Instanzen“. … Suchen Sie die Instanz für die Cloud Volumes ONTAP Bereitstellung und überprüfen Sie ihren Zustand. … Stellen Sie sicher, dass die mit der Instanz verknüpfte AWS IAM-Rolle gültig ist und ihr die entsprechenden Berechtigungen für die Instanz erteilt wurden.
AWS-Anmeldeinformationen für IAM-Rolle nicht gefunden	KRITISCH	Der Thread für Cloud-Anmeldeinformationen kann die rollenbasierten Anmeldeinformationen für das Identity and Access Management (IAM) von Amazon Web Services (AWS) nicht vom AWS-Metadatenserver abrufen. Die Anmeldeinformationen werden zum Signieren von API-Anfragen an Amazon Simple Storage Service (Amazon S3) verwendet. Cloud Volume ONTAP ist nicht mehr zugänglich. …	Führen Sie Folgendes aus: … Melden Sie sich bei der AWS EC2-Verwaltungskonsole an. … Navigieren Sie zur Seite „Instanzen“. … Suchen Sie die Instanz für die Cloud Volumes ONTAP Bereitstellung und überprüfen Sie ihren Zustand. … Stellen Sie sicher, dass die mit der Instanz verknüpfte AWS IAM-Rolle gültig ist und ihr die entsprechenden Berechtigungen für die Instanz erteilt wurden.

AWS-Anmeldeinformationen für IAM-Rolle ungültig	KRITISCH	Die rollenbasierten Anmeldeinformationen für Identity and Access Management (IAM) sind ungültig. Die Anmeldeinformationen werden mithilfe der IAM-Rolle vom Metadatenserver von Amazon Web Services (AWS) abgerufen und zum Signieren von API-Anfragen an Amazon Simple Storage Service (Amazon S3) verwendet. Auf Cloud Volume ONTAP kann nicht mehr zugegriffen werden.	Führen Sie Folgendes aus: … Melden Sie sich bei der AWS EC2-Verwaltungskonsole an. … Navigieren Sie zur Seite „Instanzen“. … Suchen Sie die Instanz für die Cloud Volumes ONTAP Bereitstellung und überprüfen Sie ihren Zustand. … Stellen Sie sicher, dass die mit der Instanz verknüpfte AWS IAM-Rolle gültig ist und ihr die entsprechenden Berechtigungen für die Instanz erteilt wurden.
AWS IAM-Rolle nicht gefunden	KRITISCH	Der Thread für Identity and Access Management (IAM)-Rollen kann auf dem AWS-Metadatenserver keine Amazon Web Services (AWS)-IAM-Rolle finden. Die IAM-Rolle ist erforderlich, um rollenbasierte Anmeldeinformationen zu erhalten, die zum Signieren von API-Anfragen an Amazon Simple Storage Service (Amazon S3) verwendet werden. Cloud Volume ONTAP ist nicht mehr zugänglich. …	Führen Sie Folgendes aus: … Melden Sie sich bei der AWS EC2-Verwaltungskonsole an. … Navigieren Sie zur Seite „Instanzen“. … Suchen Sie die Instanz für die Cloud Volumes ONTAP Bereitstellung und überprüfen Sie ihren Zustand. … Stellen Sie sicher, dass die mit der Instanz verknüpfte AWS IAM-Rolle gültig ist.

AWS IAM-Rolle ungültig	KRITISCH	Die Amazon Web Services (AWS) Identity and Access Management (IAM)-Rolle auf dem AWS-Metadatenserver ist ungültig. Auf Cloud Volume ONTAP kann nicht mehr zugegriffen werden. …	Führen Sie Folgendes aus: … Melden Sie sich bei der AWS EC2-Verwaltungskonsole an. … Navigieren Sie zur Seite „Instanzen“. … Suchen Sie die Instanz für die Cloud Volumes ONTAP Bereitstellung und überprüfen Sie ihren Zustand. … Stellen Sie sicher, dass die mit der Instanz verknüpfte AWS IAM-Rolle gültig ist und ihr die entsprechenden Berechtigungen für die Instanz erteilt wurden.
AWS-Metadatenserver-Verbindung fehlgeschlagen	KRITISCH	Der Rollenthread für Identity and Access Management (IAM) kann keine Kommunikationsverbindung mit dem Metadatenserver von Amazon Web Services (AWS) herstellen. Es sollte eine Kommunikation hergestellt werden, um die erforderlichen rollenbasierten AWS IAM-Anmeldeinformationen zu erhalten, die zum Signieren von API-Anfragen an Amazon Simple Storage Service (Amazon S3) verwendet werden. Cloud Volume ONTAP ist nicht mehr zugänglich. …	Führen Sie Folgendes aus: … Melden Sie sich bei der AWS EC2-Verwaltungskonsole an. … Navigieren Sie zur Seite „Instanzen“. … Suchen Sie die Instanz für die Cloud Volumes ONTAP -Bereitstellung und überprüfen Sie ihren Zustand. …

FabricPool Speicherplatznutzungslimit fast erreicht	WARNING (Warnung)	Die gesamte clusterweite FabricPool Speicherplatznutzung von Objektspeichern von Anbietern mit Kapazitätslizenz hat fast das lizenzierte Limit erreicht.	Führen Sie die folgenden Korrekturmaßnahmen durch: … Überprüfen Sie den Prozentsatz der lizenzierten Kapazität, die von jeder FabricPool Speicherebene verwendet wird, indem Sie den Befehl „storage aggregate object-store show-space“ verwenden. … Löschen Sie Snapshot-Kopien von Volumes mit der Tiering-Richtlinie „Snapshot“ oder „Backup“, indem Sie den Befehl „volume snapshot delete“ verwenden, um Speicherplatz freizugeben. … Installieren Sie eine neue Lizenz auf dem Cluster, um die lizenzierte Kapazität zu erhöhen.
FabricPool Speicherplatznutzungslimit erreicht	KRITISCH	Die gesamte clusterweite FabricPool Speicherplatznutzung von Objektspeichern von Anbietern mit Kapazitätslizenz hat das Lizenzlimit erreicht.	Führen Sie die folgenden Korrekturmaßnahmen durch: … Überprüfen Sie den Prozentsatz der lizenzierten Kapazität, die von jeder FabricPool Speicherebene verwendet wird, indem Sie den Befehl „storage aggregate object-store show-space“ verwenden. … Löschen Sie Snapshot-Kopien von Volumes mit der Tiering-Richtlinie „Snapshot“ oder „Backup“, indem Sie den Befehl „volume snapshot delete“ verwenden, um Speicherplatz freizugeben. … Installieren Sie eine neue Lizenz auf dem Cluster, um die lizenzierte Kapazität zu erhöhen.

Rückgabe des Aggregats fehlgeschlagen	KRITISCH	Dieses Ereignis tritt während der Migration eines Aggregats im Rahmen einer Speicher-Failover-(SFO)-Rückgabe auf, wenn der Zielknoten die Objektspeicher nicht erreichen kann.	Führen Sie die folgenden Korrekturmaßnahmen durch: … Stellen Sie mithilfe des Befehls „network interface show“ sicher, dass Ihr Intercluster-LIF online und funktionsfähig ist. … Überprüfen Sie die Netzwerkkonnektivität zum Objektspeicherserver, indem Sie den Befehl „ping“ über das Intercluster-LIF des Zielknotens ausführen. …Überprüfen Sie mit dem Befehl „aggregate object-store config show“, dass sich die Konfiguration Ihres Objektspeichers nicht geändert hat und dass die Anmelde- und Verbindungsinformationen noch immer korrekt sind. …Alternativ können Sie den Fehler überschreiben, indem Sie für den Parameter „require-partner-waiting“ des Giveback-Befehls „false“ angeben. …Wenden Sie sich an den technischen Support von NetApp , um weitere Informationen oder Unterstützung zu erhalten.

HA-Verbindung ausgefallen	WARNING (Warnung)	Die Hochverfügbarkeitsverbindung (HA) ist ausgefallen. Risiko eines Dienstausfalls, wenn kein Failover verfügbar ist.	Korrekturmaßnahmen hängen von der Anzahl und Art der von der Plattform unterstützten HA-Verbindungslinks sowie vom Grund für den Verbindungsausfall ab. …Wenn die Links ausgefallen sind: …Überprüfen Sie, ob beide Controller im HA-Paar betriebsbereit sind. …Stellen Sie bei extern verbundenen Links sicher, dass die Verbindungskabel richtig angeschlossen sind und dass die Small Form-Factor Pluggables (SFPs), falls zutreffend, richtig auf beiden Controllern sitzen. …Deaktivieren und aktivieren Sie bei intern verbundenen Links die Links nacheinander mit den Befehlen „ic link off“ und „ic link on“. …Wenn Links deaktiviert sind, aktivieren Sie die Links mit dem Befehl „ic link on“. …Wenn kein Peer verbunden ist, deaktivieren und aktivieren Sie die Links nacheinander mit den Befehlen „ic link off“ und „ic link on“. …Wenden Sie sich an den technischen Support von NetApp, wenn das Problem weiterhin besteht.

Max. Sitzungen pro Benutzer überschritten	WARNING (Warnung)	Sie haben die maximal zulässige Anzahl von Sitzungen pro Benutzer über eine TCP-Verbindung überschritten. Jede Anfrage zum Herstellen einer Sitzung wird abgelehnt, bis einige Sitzungen freigegeben werden. …	Führen Sie die folgenden Korrekturmaßnahmen durch: …Überprüfen Sie alle Anwendungen, die auf dem Client ausgeführt werden, und beenden Sie alle, die nicht ordnungsgemäß funktionieren. …Starten Sie den Client neu. …Überprüfen Sie, ob das Problem durch eine neue oder vorhandene Anwendung verursacht wird: …Wenn die Anwendung neu ist, legen Sie mit dem Befehl „cifs option modify -max-opens -same-file-per-tree“ einen höheren Schwellenwert für den Client fest. In einigen Fällen funktionieren die Clients wie erwartet, erfordern jedoch eine höhere Schwelle. Sie sollten über erweiterte Berechtigungen verfügen, um einen höheren Schwellenwert für den Client festzulegen. …Wenn das Problem durch eine vorhandene Anwendung verursacht wird, liegt möglicherweise ein Problem mit dem Client vor. Wenden Sie sich an den technischen Support von NetApp , um weitere Informationen oder Unterstützung zu erhalten.

Maximale Anzahl der Öffnungen pro Datei überschritten	WARNING (Warnung)	Sie haben die maximale Anzahl überschritten, die Sie die Datei über eine TCP-Verbindung öffnen können. Jede Anfrage zum Öffnen dieser Datei wird abgelehnt, bis Sie einige geöffnete Instanzen der Datei schließen. Dies weist normalerweise auf ein abnormales Anwendungsverhalten hin.…	Führen Sie die folgenden Korrekturmaßnahmen durch: …Überprüfen Sie die Anwendungen, die auf dem Client über diese TCP-Verbindung ausgeführt werden. Der Client funktioniert möglicherweise aufgrund der darauf ausgeführten Anwendung nicht richtig. … Starten Sie den Client neu. … Prüfen Sie, ob das Problem durch eine neue oder vorhandene Anwendung verursacht wird: … Wenn die Anwendung neu ist, legen Sie mit dem Befehl „cifs option modify -max-opens -same-file-per-tree“ einen höheren Schwellenwert für den Client fest. In einigen Fällen funktionieren die Clients wie erwartet, erfordern jedoch eine höhere Schwelle. Sie sollten über erweiterte Berechtigungen verfügen, um einen höheren Schwellenwert für den Client festzulegen. …Wenn das Problem durch eine vorhandene Anwendung verursacht wird, liegt möglicherweise ein Problem mit dem Client vor. Wenden Sie sich an den technischen Support von NetApp , um weitere Informationen oder Unterstützung zu erhalten.

NetBIOS-Namenskonflikt	KRITISCH	Der NetBIOS-Namensdienst hat von einem Remotecomputer eine negative Antwort auf eine Namensregistrierungsanforderung erhalten. Dies wird normalerweise durch einen Konflikt im NetBIOS-Namen oder einem Alias verursacht. Dies hat zur Folge, dass Clients möglicherweise nicht auf Daten zugreifen oder keine Verbindung zum richtigen Datenbereitstellungsknoten im Cluster herstellen können.	Führen Sie eine der folgenden Korrekturmaßnahmen durch: …Wenn ein Konflikt im NetBIOS-Namen oder einem Alias vorliegt, führen Sie einen der folgenden Schritte aus: …Löschen Sie den doppelten NetBIOS-Alias mit dem Befehl „vserver cifs delete -aliases alias -vserver vserver“. …Benennen Sie einen NetBIOS-Alias um, indem Sie den doppelten Namen löschen und einen Alias mit einem neuen Namen hinzufügen, indem Sie den Befehl „vserver cifs create -aliases alias -vserver vserver“ verwenden. …Wenn keine Aliase konfiguriert sind und ein Konflikt im NetBIOS-Namen vorliegt, benennen Sie den CIFS-Server mit den Befehlen „vserver cifs delete -vserver vserver“ und „vserver cifs create -cifs -server netbiosname“ um. HINWEIS: Durch das Löschen eines CIFS-Servers kann der Zugriff auf die Daten unzugänglich werden. …Entfernen Sie den NetBIOS-Namen oder benennen Sie das NetBIOS auf dem Remotecomputer um.
NFSv4-Speicherpool erschöpft	KRITISCH	Ein NFSv4-Speicherpool ist erschöpft.	Wenn der NFS-Server nach diesem Ereignis länger als 10 Minuten nicht reagiert, wenden Sie sich an den technischen Support von NetApp .

Keine registrierte Scan-Engine	KRITISCH	Der Antivirus-Connector hat ONTAP benachrichtigt, dass er über keine registrierte Scan-Engine verfügt. Dies kann dazu führen, dass Daten nicht verfügbar sind, wenn die Option „Scan-obligatorisch“ aktiviert ist.	Führen Sie die folgenden Korrekturmaßnahmen durch: … Stellen Sie sicher, dass die auf dem Antivirenserver installierte Scan-Engine-Software mit ONTAP kompatibel ist. … Stellen Sie sicher, dass die Scan-Engine-Software ausgeführt wird und für die Verbindung mit dem Antiviren-Connector über lokales Loopback konfiguriert ist.
Keine Vscan-Verbindung	KRITISCH	ONTAP verfügt über keine Vscan-Verbindung, um Virenscan-Anfragen zu bedienen. Dies kann dazu führen, dass Daten nicht verfügbar sind, wenn die Option „Scan-obligatorisch“ aktiviert ist.	Stellen Sie sicher, dass der Scannerpool richtig konfiguriert ist und die Antivirenserver aktiv und mit ONTAP verbunden sind.
Knoten-Root-Volume-Speicherplatz niedrig	KRITISCH	Das System hat festgestellt, dass auf dem Stammvolume gefährlich wenig Speicherplatz vorhanden ist. Der Knoten ist nicht voll funktionsfähig. Möglicherweise ist innerhalb des Clusters ein Failover der Daten-LIFs aufgetreten, weshalb der NFS- und CIFS-Zugriff auf den Knoten eingeschränkt ist. Die Verwaltungsfunktionen sind auf lokale Wiederherstellungsverfahren für den Knoten beschränkt, um Speicherplatz auf dem Stammvolume freizugeben.	Führen Sie die folgenden Korrekturmaßnahmen durch: … Schaffen Sie Speicherplatz auf dem Stammvolume, indem Sie alte Snapshot-Kopien löschen, nicht mehr benötigte Dateien aus dem Verzeichnis /mroot löschen oder die Kapazität des Stammvolumes erweitern. … Starten Sie den Controller neu. … Wenden Sie sich an den technischen Support von NetApp , um weitere Informationen oder Unterstützung zu erhalten.
Nicht vorhandene Admin-Freigabe	KRITISCH	Vscan-Problem: Ein Client hat versucht, eine Verbindung zu einer nicht vorhandenen ONTAP_ADMIN$-Freigabe herzustellen.	Stellen Sie sicher, dass Vscan für die angegebene SVM-ID aktiviert ist. Durch die Aktivierung von Vscan auf einer SVM wird die ONTAP_ADMIN$-Freigabe automatisch für die SVM erstellt.

Nicht genügend Speicherplatz für den NVMe-Namespace	KRITISCH	Ein NVMe-Namespace wurde aufgrund eines Schreibfehlers aufgrund von Speicherplatzmangel offline geschaltet.	Fügen Sie dem Volume Speicherplatz hinzu und bringen Sie dann den NVMe-Namespace online, indem Sie den Befehl „vserver nvme namespace modify“ verwenden.
NVMe-oF-Gnadenfrist aktiv	WARNING (Warnung)	Dieses Ereignis tritt täglich auf, wenn das NVMe over Fabrics (NVMe-oF)-Protokoll verwendet wird und die Nachfrist der Lizenz aktiv ist. Für die NVMe-oF-Funktionalität ist nach Ablauf der Lizenzfrist eine Lizenz erforderlich. Die NVMe-oF-Funktionalität wird deaktiviert, wenn die Lizenzfrist abgelaufen ist.	Wenden Sie sich an Ihren Vertriebsmitarbeiter, um eine NVMe-oF-Lizenz zu erhalten und sie dem Cluster hinzuzufügen, oder entfernen Sie alle Instanzen der NVMe-oF-Konfiguration aus dem Cluster.
NVMe-oF-Karenzzeit abgelaufen	WARNING (Warnung)	Die Nachfrist für die NVMe over Fabrics (NVMe-oF)-Lizenz ist abgelaufen und die NVMe-oF-Funktionalität ist deaktiviert.	Wenden Sie sich an Ihren Vertriebsmitarbeiter, um eine NVMe-oF-Lizenz zu erhalten und sie dem Cluster hinzuzufügen.
NVMe-oF-Gnadenfrist beginnt	WARNING (Warnung)	Die NVMe over Fabrics (NVMe-oF)-Konfiguration wurde während des Upgrades auf die ONTAP 9.5-Software erkannt. Für die NVMe-oF-Funktionalität ist nach Ablauf der Lizenzfrist eine Lizenz erforderlich.	Wenden Sie sich an Ihren Vertriebsmitarbeiter, um eine NVMe-oF-Lizenz zu erhalten und sie dem Cluster hinzuzufügen.
Objektspeicher-Host nicht auflösbar	KRITISCH	Der Hostname des Objektspeicherservers kann nicht in eine IP-Adresse aufgelöst werden. Der Objektspeicherclient kann ohne Auflösung in eine IP-Adresse nicht mit dem Objektspeicherserver kommunizieren. Dies kann dazu führen, dass auf die Daten nicht zugegriffen werden kann.	Überprüfen Sie die DNS-Konfiguration, um sicherzustellen, dass der Hostname korrekt mit einer IP-Adresse konfiguriert ist.

Objektspeicher-Intercluster-LIF ausgefallen	KRITISCH	Der Objektspeicher-Client kann kein funktionsfähiges LIF für die Kommunikation mit dem Objektspeicher-Server finden. Der Knoten lässt keinen Objektspeicher-Clientverkehr zu, bis das Intercluster-LIF betriebsbereit ist. Dies kann dazu führen, dass auf die Daten nicht zugegriffen werden kann.	Führen Sie die folgenden Korrekturmaßnahmen durch: … Überprüfen Sie den Intercluster-LIF-Status mit dem Befehl „network interface show -role intercluster“. … Stellen Sie sicher, dass das Intercluster-LIF richtig konfiguriert und betriebsbereit ist. … Wenn kein Intercluster-LIF konfiguriert ist, fügen Sie es mit dem Befehl „network interface create -role intercluster“ hinzu.
Nichtübereinstimmung der Objektspeichersignatur	KRITISCH	Die an den Objektspeicherserver gesendete Anforderungssignatur stimmt nicht mit der vom Client berechneten Signatur überein. Dies kann dazu führen, dass auf die Daten nicht zugegriffen werden kann.	Überprüfen Sie, ob der geheime Zugriffsschlüssel richtig konfiguriert ist. Wenn es richtig konfiguriert ist, wenden Sie sich an den technischen Support von NetApp , um Hilfe zu erhalten.

READDIR-Zeitüberschreitung	KRITISCH	Ein READDIR-Dateivorgang hat das zulässige Zeitlimit für die Ausführung in WAFL überschritten. Dies kann an sehr großen oder spärlich gefüllten Verzeichnissen liegen. Es werden Korrekturmaßnahmen empfohlen.	Führen Sie die folgenden Korrekturmaßnahmen durch: … Suchen Sie nach spezifischen Informationen zu aktuellen Verzeichnissen, bei denen READDIR-Dateivorgänge abgelaufen sind, indem Sie den folgenden NodeShell-CLI-Befehl mit der Berechtigung „diag“ verwenden: wafl readdir notice show. … Überprüfen Sie, ob Verzeichnisse als spärlich gekennzeichnet sind oder nicht: … Wenn ein Verzeichnis als spärlich gekennzeichnet ist, wird empfohlen, den Inhalt des Verzeichnisses in ein neues Verzeichnis zu kopieren, um die Spärlichkeit der Verzeichnisdatei zu beheben. …Wenn ein Verzeichnis nicht als spärlich gekennzeichnet ist und das Verzeichnis groß ist, wird empfohlen, die Größe der Verzeichnisdatei zu reduzieren, indem Sie die Anzahl der Dateieinträge im Verzeichnis verringern.

Verlagerung des Aggregats fehlgeschlagen	KRITISCH	Dieses Ereignis tritt während der Verschiebung eines Aggregats auf, wenn der Zielknoten die Objektspeicher nicht erreichen kann.	Führen Sie die folgenden Korrekturmaßnahmen durch: … Stellen Sie mithilfe des Befehls „network interface show“ sicher, dass Ihr Intercluster-LIF online und funktionsfähig ist. … Überprüfen Sie die Netzwerkkonnektivität zum Objektspeicherserver, indem Sie den Befehl „ping“ über das Intercluster-LIF des Zielknotens ausführen. …Überprüfen Sie mit dem Befehl „aggregate object-store config show“, dass sich die Konfiguration Ihres Objektspeichers nicht geändert hat und dass die Anmelde- und Verbindungsinformationen noch immer korrekt sind. …Alternativ können Sie den Fehler mit dem Parameter „override-destination-checks“ des Umzugsbefehls überschreiben. …Wenden Sie sich an den technischen Support von NetApp, um weitere Informationen oder Unterstützung zu erhalten.

Schattenkopie fehlgeschlagen	KRITISCH	Ein Volume Shadow Copy Service (VSS), ein Sicherungs- und Wiederherstellungsdienstvorgang von Microsoft Server, ist fehlgeschlagen.	Überprüfen Sie anhand der in der Ereignismeldung bereitgestellten Informationen Folgendes: … Ist die Schattenkopiekonfiguration aktiviert? … Sind die entsprechenden Lizenzen installiert? …Auf welchen Freigaben wird der Schattenkopievorgang ausgeführt?…Ist der Freigabename korrekt?…Existiert der Freigabepfad?…Wie ist der Status des Schattenkopiesatzes und seiner Schattenkopien?
Ausfall der Stromversorgung des Speicherschalters	WARNING (Warnung)	Im Cluster-Switch fehlt eine Stromversorgung. Die Redundanz wird reduziert, das Risiko eines Stromausfalls bei weiteren Stromausfällen steigt.	Führen Sie die folgenden Korrekturmaßnahmen durch: … Stellen Sie sicher, dass das Netzteil, das den Cluster-Switch mit Strom versorgt, eingeschaltet ist. … Stellen Sie sicher, dass das Netzkabel an die Stromversorgung angeschlossen ist. … Wenden Sie sich an den technischen Support von NetApp , wenn das Problem weiterhin besteht.
Zu viele CIFS-Authentifizierungen	WARNING (Warnung)	Viele Authentifizierungsverhandlungen fanden gleichzeitig statt. Von diesem Client liegen 256 unvollständige neue Sitzungsanforderungen vor.	Untersuchen Sie, warum der Client 256 oder mehr neue Verbindungsanforderungen erstellt hat. Möglicherweise müssen Sie sich an den Anbieter des Clients oder der Anwendung wenden, um die Ursache des Fehlers zu ermitteln.

Unbefugter Benutzerzugriff auf die Administratorfreigabe	WARNING (Warnung)	Ein Client hat versucht, eine Verbindung zur privilegierten Freigabe ONTAP_ADMIN$ herzustellen, obwohl der angemeldete Benutzer kein zulässiger Benutzer ist.	Führen Sie die folgenden Korrekturmaßnahmen durch: … Stellen Sie sicher, dass der angegebene Benutzername und die IP-Adresse in einem der aktiven Vscan-Scannerpools konfiguriert sind. … Überprüfen Sie die aktuell aktive Scannerpoolkonfiguration mit dem Befehl „vserver vscan scanner pool show-active“.
Virus erkannt	WARNING (Warnung)	Ein Vscan-Server hat dem Speichersystem einen Fehler gemeldet. Dies weist normalerweise darauf hin, dass ein Virus gefunden wurde. Dieses Ereignis kann jedoch auch durch andere Fehler auf dem Vscan-Server verursacht werden. …Der Clientzugriff auf die Datei wird verweigert. Der Vscan-Server kann die Datei je nach seinen Einstellungen und seiner Konfiguration bereinigen, unter Quarantäne stellen oder löschen.	Überprüfen Sie das im „Syslog“-Ereignis gemeldete Protokoll des Vscan-Servers, um festzustellen, ob die infizierte Datei erfolgreich bereinigt, unter Quarantäne gestellt oder gelöscht werden konnte. Wenn dies nicht möglich ist, muss ein Systemadministrator die Datei möglicherweise manuell löschen.
Volume offline	INFO	Diese Meldung zeigt an, dass ein Volume offline geschaltet wurde.	Bringen Sie das Volume wieder online.
Volumenbeschränkt	INFO	Dieses Ereignis zeigt an, dass ein flexibles Volumen eingeschränkt wird.	Bringen Sie das Volume wieder online.
Speicher-VM erfolgreich beendet	INFO	Diese Meldung wird angezeigt, wenn ein „vServer-Stopp“-Vorgang erfolgreich ist.	Verwenden Sie den Befehl „vserver start“, um den Datenzugriff auf einer Speicher-VM zu starten.
Knotenpanik	WARNING (Warnung)	Dieses Ereignis wird ausgelöst, wenn eine Panik auftritt	Wenden Sie sich an den NetApp Kundensupport.

Zurück nach oben

Anti-Ransomware-Protokollmonitore

Monitorname	Schwere	Beschreibung	Korrekturmaßnahme
Storage VM Anti-Ransomware-Überwachung deaktiviert	WARNING (Warnung)	Die Anti-Ransomware-Überwachung für die Speicher-VM ist deaktiviert. Aktivieren Sie Anti-Ransomware, um die Speicher-VM zu schützen.	Keine
Storage VM Anti-Ransomware-Überwachung aktiviert (Lernmodus)	INFO	Die Anti-Ransomware-Überwachung für die Speicher-VM ist im Lernmodus aktiviert.	Keine
Volumen-Anti-Ransomware-Überwachung aktiviert	INFO	Die Anti-Ransomware-Überwachung für das Volume ist aktiviert.	Keine
Volumen-Anti-Ransomware-Überwachung deaktiviert	WARNING (Warnung)	Die Anti-Ransomware-Überwachung für das Volume ist deaktiviert. Aktivieren Sie Anti-Ransomware, um das Volume zu schützen.	Keine
Volumen-Anti-Ransomware-Überwachung aktiviert (Lernmodus)	INFO	Die Anti-Ransomware-Überwachung für das Volume ist im Lernmodus aktiviert.	Keine
Volumen-Anti-Ransomware-Überwachung angehalten (Lernmodus)	WARNING (Warnung)	Die Anti-Ransomware-Überwachung für das Volume wird im Lernmodus angehalten.	Keine
Volumen-Anti-Ransomware-Überwachung angehalten	WARNING (Warnung)	Die Anti-Ransomware-Überwachung für das Volume ist angehalten.	Keine
Deaktivieren der Volumen-Anti-Ransomware-Überwachung	WARNING (Warnung)	Die Anti-Ransomware-Überwachung für das Volume wird deaktiviert.	Keine

Ransomware-Aktivität erkannt	KRITISCH	Um die Daten vor der erkannten Ransomware zu schützen, wurde eine Snapshot-Kopie erstellt, mit der die Originaldaten wiederhergestellt werden können. Ihr System generiert und überträgt eine AutoSupport oder „Call Home“-Nachricht an den technischen Support von NetApp und alle konfigurierten Ziele. AutoSupport -Nachrichten verbessern die Problembestimmung und -lösung.	Informationen zum Ergreifen von Abhilfemaßnahmen gegen Ransomware-Aktivitäten finden Sie im „FINAL-DOCUMENT-NAME“.

Zurück nach oben

FSx für NetApp ONTAP -Monitore

Monitorname	Schwellenwerte	Monitorbeschreibung	Korrekturmaßnahme
Die FSx-Volumenkapazität ist voll	Warnung @ > 85 %…Kritisch @ > 95 %	Die Speicherkapazität eines Datenträgers ist zum Speichern von Anwendungs- und Kundendaten erforderlich. Je mehr Daten im ONTAP -Volume gespeichert werden, desto geringer ist die Speicherverfügbarkeit für zukünftige Daten. Wenn die Datenspeicherkapazität innerhalb eines Volumes die Gesamtspeicherkapazität erreicht, kann dies dazu führen, dass der Kunde aufgrund fehlender Speicherkapazität keine Daten speichern kann. Durch die Überwachung der genutzten Speicherkapazität wird die Kontinuität der Datendienste gewährleistet.	Um Serviceunterbrechungen zu minimieren, wenn ein kritischer Schwellenwert überschritten wird, sind sofortige Maßnahmen erforderlich: …1. Löschen Sie nicht mehr benötigte Daten, um Speicherplatz freizugeben.

FSx-Volumen, hohe Latenz	Warnung @ > 1000 µs…Kritisch @ > 2000 µs	Volumes sind Objekte, die den E/A-Verkehr bedienen, der häufig von leistungssensiblen Anwendungen wie DevOps-Anwendungen, Home-Verzeichnissen und Datenbanken gesteuert wird. Hohe Volumenlatenzen können dazu führen, dass die Anwendungen selbst darunter leiden und ihre Aufgaben nicht erfüllen können. Die Überwachung der Volume-Latenzen ist entscheidend, um eine konsistente Anwendungsleistung aufrechtzuerhalten.	Um Serviceunterbrechungen zu minimieren, wenn ein kritischer Schwellenwert überschritten wird, sind sofortige Maßnahmen erforderlich: …1. Wenn dem Volume eine QoS-Richtlinie zugewiesen ist, prüfen Sie dessen Grenzwerte, um zu prüfen, ob diese zu einer Drosselung der Volume-Arbeitslast führen. Planen Sie, bald die folgenden Maßnahmen zu ergreifen, wenn der Warnschwellenwert überschritten wird: …1. Wenn dem Volume eine QoS-Richtlinie zugewiesen ist, prüfen Sie dessen Grenzwerte, falls diese zu einer Drosselung der Volume-Arbeitslast führen. …2. Wenn der Knoten ebenfalls stark ausgelastet ist, verschieben Sie das Volume auf einen anderen Knoten oder reduzieren Sie die Gesamtarbeitslast des Knotens.

FSx-Volume-Inodes-Limit	Warnung @ > 85 %…Kritisch @ > 95 %	Volumes, die Dateien speichern, verwenden Indexknoten (Inode) zum Speichern von Dateimetadaten. Wenn ein Volume seine Inode-Zuweisung erschöpft, können ihm keine weiteren Dateien hinzugefügt werden. Eine Warnmeldung weist darauf hin, dass geplante Maßnahmen ergriffen werden sollten, um die Anzahl der verfügbaren Inodes zu erhöhen. Eine kritische Warnung weist darauf hin, dass die Erschöpfung des Dateilimits unmittelbar bevorsteht und Notfallmaßnahmen ergriffen werden sollten, um Inodes freizugeben und so die Servicekontinuität sicherzustellen.	Um Serviceunterbrechungen zu minimieren, wenn ein kritischer Schwellenwert überschritten wird, sind sofortige Maßnahmen erforderlich: …1. Erwägen Sie, den Inodes-Wert für das Volume zu erhöhen. Wenn der Inodes-Wert bereits das Maximum erreicht hat, sollten Sie das Volume in zwei oder mehr Volumes aufteilen, da das Dateisystem die maximale Größe überschritten hat. Planen Sie, bald die folgenden Maßnahmen zu ergreifen, wenn der Warnschwellenwert überschritten wird: …1. Erwägen Sie, den Inodes-Wert für das Volume zu erhöhen. Wenn der Inodes-Wert bereits das Maximum erreicht hat, sollten Sie das Volume in zwei oder mehr Volumes aufteilen, da das Dateisystem über die maximale Größe hinausgewachsen ist
FSx Volume Qtree-Kontingentüberbelegung	Warnung @ > 95 %…Kritisch @ > 100 %	Volume Qtree Quota Overcommit gibt den Prozentsatz an, ab dem ein Volume als durch die Qtree-Kontingente überbelegt gilt. Der festgelegte Schwellenwert für das Qtree-Kontingent ist für das Volume erreicht. Durch die Überwachung der Überbelegung des Volume-Qtree-Kontingents wird sichergestellt, dass der Benutzer einen unterbrechungsfreien Datendienst erhält.	Wenn ein kritischer Schwellenwert überschritten wird, sollten sofort Maßnahmen ergriffen werden, um die Dienstunterbrechung zu minimieren: 1. Löschen Sie nicht benötigte Daten. Wenn der Warnschwellenwert überschritten wird, sollten Sie den Speicherplatz des Datenträgers vergrößern.

Der reservierte Speicherplatz für FSx-Snapshots ist voll	Warnung @ > 90 %…Kritisch @ > 95 %	Die Speicherkapazität eines Datenträgers ist zum Speichern von Anwendungs- und Kundendaten erforderlich. Ein Teil dieses Speicherplatzes, der sogenannte reservierte Snapshot-Speicherplatz, wird zum Speichern von Snapshots verwendet, die einen lokalen Schutz der Daten ermöglichen. Je mehr neue und aktualisierte Daten im ONTAP Volume gespeichert werden, desto mehr Snapshot-Kapazität wird verwendet und desto weniger Snapshot-Speicherkapazität steht für zukünftige neue oder aktualisierte Daten zur Verfügung. Wenn die Snapshot-Datenkapazität innerhalb eines Volumes den gesamten Snapshot-Reservespeicherplatz erreicht, kann dies dazu führen, dass der Kunde keine neuen Snapshot-Daten speichern kann und der Schutzgrad der Daten im Volume verringert wird. Durch die Überwachung der Snapshot-Kapazität des verwendeten Volumes wird die Kontinuität der Datendienste sichergestellt.	Um Serviceunterbrechungen zu minimieren, wenn ein kritischer Schwellenwert überschritten wird, sind sofortige Maßnahmen erforderlich: …1. Erwägen Sie die Konfiguration von Snapshots, um den Datenspeicherplatz im Volume zu nutzen, wenn die Snapshot-Reserve voll ist … 2. Erwägen Sie, einige ältere Snapshots zu löschen, die möglicherweise nicht mehr benötigt werden, um Speicherplatz freizugeben. Planen Sie, bald die folgenden Maßnahmen zu ergreifen, wenn der Warnschwellenwert überschritten wird: …1. Erwägen Sie, den Snapshot-Reservespeicherplatz innerhalb des Volumes zu erhöhen, um dem Wachstum Rechnung zu tragen…2. Erwägen Sie die Konfiguration von Snapshots, um den Datenspeicherplatz im Volume zu nutzen, wenn die Snapshot-Reserve voll ist

FSx Volume Cache Miss Ratio	Warnung @ > 95 %…Kritisch @ > 100 %	Die Volume Cache Miss Ratio ist der Prozentsatz der Leseanforderungen der Clientanwendungen, die von der Festplatte und nicht vom Cache zurückgegeben werden. Dies bedeutet, dass die Lautstärke den eingestellten Schwellenwert erreicht hat.	Wenn ein kritischer Schwellenwert überschritten wird, sollten sofort Maßnahmen ergriffen werden, um die Dienstunterbrechung zu minimieren: 1. Verschieben Sie einige Workloads vom Knoten des Volumes, um die E/A-Last 2 zu reduzieren. Reduzieren Sie die Nachfrage nach Workloads mit niedrigerer Priorität auf demselben Knoten über QoS-Grenzwerte. Erwägen Sie sofortige Maßnahmen, wenn der Warnschwellenwert überschritten wird: 1. Verschieben Sie einige Workloads vom Knoten des Volumes, um die E/A-Last 2 zu reduzieren. Verringern Sie die Nachfrage nach Workloads mit niedrigerer Priorität auf demselben Knoten über QoS-Grenzwerte 3. Ändern Sie die Arbeitslasteigenschaften (Blockgröße, Anwendungs-Caching usw.)

Zurück nach oben

K8s-Monitore

Monitorname	Beschreibung	Korrekturmaßnahmen	Schweregrad/Schwellenwert

Hohe Latenz bei persistentem Volume	Hohe, anhaltende Volumenlatenzen können dazu führen, dass die Anwendungen selbst darunter leiden und ihre Aufgaben nicht erfüllen können. Die Überwachung dauerhafter Volume-Latenzen ist entscheidend, um eine konsistente Anwendungsleistung aufrechtzuerhalten. Je nach Medientyp sind folgende Latenzen zu erwarten: SSD bis zu 1–2 Millisekunden, SAS bis zu 8–10 Millisekunden und SATA-HDD 17–20 Millisekunden.	**Sofortmaßnahmen** Wenn ein kritischer Schwellenwert überschritten wird, sollten Sie sofortige Maßnahmen in Betracht ziehen, um Dienstunterbrechungen zu minimieren: Wenn dem Volume eine QoS-Richtlinie zugewiesen ist, prüfen Sie dessen Grenzwerte, falls diese zu einer Drosselung der Volume-Arbeitslast führen. **Bald zu ergreifende Maßnahmen** Wenn der Warnschwellenwert überschritten wird, planen Sie die folgenden Sofortmaßnahmen: 1. Wenn auch der Speicherpool stark ausgelastet ist, verschieben Sie das Volume in einen anderen Speicherpool. 2. Wenn dem Volume eine QoS-Richtlinie zugewiesen ist, prüfen Sie dessen Grenzwerte, um zu prüfen, ob diese zu einer Drosselung der Volume-Arbeitslast führen. 3. Wenn auch der Controller stark ausgelastet ist, verschieben Sie das Volume auf einen anderen Controller oder reduzieren Sie die Gesamtarbeitslast des Controllers.	Warnung @ > 6.000 µs Kritisch @ > 12.000 µs
Cluster-Speichersättigung hoch	Die Sättigung des dem Cluster zuweisbaren Speichers ist hoch. Die CPU-Sättigung des Clusters wird berechnet als Summe der Speichernutzung geteilt durch die Summe des zuweisbaren Speichers aller K8s-Knoten.	Knoten hinzufügen. Reparieren Sie alle nicht geplanten Knoten. Passen Sie die Größe der Pods an, um Speicher auf Knoten freizugeben.	Warnung @ > 80 % Kritisch @ > 90 %

POD-Anhängen fehlgeschlagen	Diese Warnung wird angezeigt, wenn ein Volume-Anhang mit POD fehlgeschlagen ist.		Warnung
Hohe Neuübertragungsrate	Hohe TCP-Neuübertragungsrate	Auf Netzwerküberlastung prüfen – Identifizieren Sie Arbeitslasten, die viel Netzwerkbandbreite verbrauchen. Überprüfen Sie, ob die CPU-Auslastung des Pods hoch ist. Überprüfen Sie die Hardware-Netzwerkleistung.	Warnung @ > 10 % Kritisch @ > 25 %
Knotendateisystemkapazität hoch	Knotendateisystemkapazität hoch	- Erhöhen Sie die Größe der Knotenfestplatten, um sicherzustellen, dass ausreichend Platz für die Anwendungsdateien vorhanden ist. - Reduzieren Sie die Verwendung von Anwendungsdateien.	Warnung @ > 80 % Kritisch @ > 90 %
Hoher Netzwerk-Jitter bei der Arbeitslast	Hoher TCP-Jitter (hohe Latenz-/Antwortzeitschwankungen)	Überprüfen Sie, ob das Netzwerk überlastet ist. Identifizieren Sie Workloads, die viel Netzwerkbandbreite verbrauchen. Überprüfen Sie, ob die CPU-Auslastung des Pods hoch ist. Überprüfen Sie die Leistung des Hardwarenetzwerks	Warnung @ > 30 ms Kritisch @ > 50 ms

Durchsatz persistenter Volumes	MBPS-Schwellenwerte für persistente Volumes können verwendet werden, um einen Administrator zu warnen, wenn persistente Volumes vordefinierte Leistungserwartungen überschreiten, was sich möglicherweise auf andere persistente Volumes auswirkt. Durch die Aktivierung dieses Monitors werden Warnungen generiert, die für das typische Durchsatzprofil persistenter Volumes auf SSDs geeignet sind. Dieser Monitor deckt alle persistenten Volumes Ihres Mandanten ab. Die Warn- und kritischen Schwellenwerte können basierend auf Ihren Überwachungszielen angepasst werden, indem Sie diesen Monitor duplizieren und für Ihre Speicherklasse geeignete Schwellenwerte festlegen. Ein duplizierter Monitor kann außerdem auf eine Teilmenge der persistenten Volumes Ihres Mandanten ausgerichtet werden.	**Sofortmaßnahmen** Wenn ein kritischer Schwellenwert überschritten wird, planen Sie Sofortmaßnahmen, um die Dienstunterbrechung zu minimieren: 1. Führen Sie QoS-MBPS-Grenzwerte für das Volume ein. 2. Überprüfen Sie die Anwendung, die die Arbeitslast auf dem Datenträger steuert, auf Anomalien. **Bald zu ergreifende Maßnahmen** Wenn der Warnschwellenwert überschritten wird, planen Sie die folgenden sofortigen Maßnahmen: 1. Führen Sie QoS-MBPS-Grenzwerte für das Volume ein. 2. Überprüfen Sie die Anwendung, die die Arbeitslast auf dem Datenträger steuert, auf Anomalien.	Warnung @ > 10.000 MB/s Kritisch @ > 15.000 MB/s
Container, dem die Gefahr besteht, OOM zu werden, wurden getötet	Die Speichergrenzen des Containers sind zu niedrig eingestellt. Es besteht die Gefahr einer Räumung des Containers (Out of Memory Kill).	Erhöhen Sie die Speichergrenzen des Containers.	Warnung @ > 95 %
Arbeitsbelastung reduziert	Die Arbeitslast hat keine gesunden Pods.		Kritisch @ < 1
Bindung des Anspruchs auf persistentes Volume fehlgeschlagen	Diese Warnung wird angezeigt, wenn eine Bindung auf einem PVC fehlschlägt.		Warnung

ResourceQuota-Speicherlimits werden bald überschritten	Die Speichergrenzen für den Namespace überschreiten bald ResourceQuota		Warnung @ > 80 % Kritisch @ > 90 %
ResourceQuota-Speicheranforderungen werden bald überschritten	Speicheranforderungen für Namespace überschreiten bald ResourceQuota		Warnung @ > 80 % Kritisch @ > 90 %
Knotenerstellung fehlgeschlagen	Der Knoten konnte aufgrund eines Konfigurationsfehlers nicht geplant werden.	Suchen Sie im Kubernetes-Ereignisprotokoll nach der Ursache des Konfigurationsfehlers.	Kritisch
Die Wiederherstellung des persistenten Volumes ist fehlgeschlagen	Die automatische Wiederherstellung des Datenträgers ist fehlgeschlagen.		Warnung @ > 0 B
CPU-Drosselung für Container	Die CPU-Grenzen des Containers sind zu niedrig eingestellt. Containerprozesse werden verlangsamt.	Erhöhen Sie die CPU-Grenzen des Containers.	Warnung @ > 95 % Kritisch @ > 98 %
Service Load Balancer konnte nicht gelöscht werden			Warnung

Persistente Volume-IOPS	IOPS-Schwellenwerte für persistente Volumes können verwendet werden, um einen Administrator zu warnen, wenn persistente Volumes vordefinierte Leistungserwartungen überschreiten. Durch die Aktivierung dieses Monitors werden Warnungen generiert, die für das typische IOPS-Profil von Persistenzvolumes geeignet sind. Dieser Monitor deckt alle persistenten Volumes Ihres Mandanten ab. Die Warn- und kritischen Schwellenwerte können basierend auf Ihren Überwachungszielen angepasst werden, indem Sie diesen Monitor duplizieren und für Ihre Arbeitslast geeignete Schwellenwerte festlegen.	**Sofortmaßnahmen** Wenn ein kritischer Schwellenwert überschritten wird, planen Sie Sofortmaßnahmen, um die Dienstunterbrechung zu minimieren: 1. Führen Sie QoS-IOPS-Grenzwerte für das Volume ein. 2. Überprüfen Sie die Anwendung, die die Arbeitslast auf dem Datenträger steuert, auf Anomalien. **Bald zu ergreifende Maßnahmen** Wenn der Warnschwellenwert überschritten wird, planen Sie die folgenden Sofortmaßnahmen: 1. Führen Sie QoS-IOPS-Grenzwerte für das Volume ein. 2. Überprüfen Sie die Anwendung, die die Arbeitslast auf dem Datenträger steuert, auf Anomalien.	Warnung bei > 20.000 IO/s Kritisch bei > 25.000 IO/s
Service Load Balancer konnte nicht aktualisiert werden			Warnung
POD-Mount fehlgeschlagen	Diese Warnung wird angezeigt, wenn die Bereitstellung eines POD fehlgeschlagen ist.		Warnung
Knoten-PID-Druck	Die Anzahl der verfügbaren Prozesskennungen auf dem (Linux-)Knoten ist unter einen Räumungsschwellenwert gefallen.	Suchen und beheben Sie Pods, die viele Prozesse generieren und dem Knoten die verfügbaren Prozess-IDs vorenthalten. Richten Sie PodPidsLimit ein, um Ihren Knoten vor Pods oder Containern zu schützen, die zu viele Prozesse erzeugen.	Kritisch @ > 0

Fehler beim Abrufen des Pod-Images	Kubernetes konnte das Pod-Container-Image nicht abrufen.	- Stellen Sie sicher, dass das Bild des Pods in der Pod-Konfiguration richtig geschrieben ist. - Überprüfen Sie, ob das Bild-Tag in Ihrer Registrierung vorhanden ist. – Überprüfen Sie die Anmeldeinformationen für die Image-Registrierung. - Überprüfen Sie, ob Probleme mit der Registrierungskonnektivität vorliegen. - Stellen Sie sicher, dass Sie die von öffentlichen Registrierungsanbietern auferlegten Ratenbeschränkungen nicht erreichen.	Warnung
Job läuft zu lange	Der Job läuft zu lange		Warnung @ > 1 Std. Kritisch @ > 5 Std.
Knotenspeicher hoch	Die Knotenspeichernutzung ist hoch	Knoten hinzufügen. Reparieren Sie alle nicht geplanten Knoten. Passen Sie die Größe der Pods an, um Speicher auf Knoten freizugeben.	Warnung @ > 85 % Kritisch @ > 90 %
ResourceQuota-CPU-Grenzwerte werden bald überschritten	CPU-Grenzwerte für Namespace überschreiten bald ResourceQuota		Warnung @ > 80 % Kritisch @ > 90 %
Pod Crash Loop Backoff	Pod ist abgestürzt und hat mehrere Neustartversuche unternommen.		Kritisch @ > 3
Knoten-CPU hoch	Die CPU-Auslastung des Knotens ist hoch.	Knoten hinzufügen. Reparieren Sie alle nicht geplanten Knoten. Passen Sie die Größe der Pods an, um CPU-Leistung auf Knoten freizugeben.	Warnung @ > 80 % Kritisch @ > 90 %

Arbeitslast-Netzwerklatenz RTT Hoch	Hohe TCP RTT (Round Trip Time)-Latenz	Auf Netzwerküberlastung prüfen ▒ Identifizieren Sie Arbeitslasten, die viel Netzwerkbandbreite verbrauchen. Überprüfen Sie, ob die CPU-Auslastung des Pods hoch ist. Überprüfen Sie die Hardware-Netzwerkleistung.	Warnung @ > 150 ms Kritisch @ > 300 ms
Auftrag fehlgeschlagen	Der Auftrag wurde aufgrund eines Knotenabsturzes oder Neustarts, einer Ressourcenerschöpfung, einer Auftragszeitüberschreitung oder eines Pod-Planungsfehlers nicht erfolgreich abgeschlossen.	Überprüfen Sie die Kubernetes-Ereignisprotokolle auf Fehlerursachen.	Warnung @ > 1
Dauerhaftes Volumen in wenigen Tagen voll	Der Speicherplatz des persistenten Volumes wird in einigen Tagen erschöpft sein	-Erhöhen Sie die Volumegröße, um sicherzustellen, dass ausreichend Platz für die Anwendungsdateien vorhanden ist. - Reduzieren Sie die in Anwendungen gespeicherte Datenmenge.	Warnung @ < 8 Tage Kritisch @ < 3 Tage
Knotenspeicherdruck	Dem Knoten geht der Speicher aus. Der verfügbare Speicher hat den Auslagerungsschwellenwert erreicht.	Knoten hinzufügen. Reparieren Sie alle nicht geplanten Knoten. Passen Sie die Größe der Pods an, um Speicher auf Knoten freizugeben.	Kritisch @ > 0
Knoten nicht bereit	Knoten ist seit 5 Minuten nicht bereit	Überprüfen Sie, ob der Knoten über genügend CPU-, Speicher- und Festplattenressourcen verfügt. Überprüfen Sie die Netzwerkkonnektivität des Knotens. Überprüfen Sie die Kubernetes-Ereignisprotokolle auf Fehlerursachen.	Kritisch @ < 1

Hohe persistente Volume-Kapazität	Die genutzte Kapazität des Persistent Volume-Backends ist hoch.	- Erhöhen Sie die Volumegröße, um sicherzustellen, dass ausreichend Platz für die Anwendungsdateien vorhanden ist. - Reduzieren Sie die in Anwendungen gespeicherte Datenmenge.	Warnung @ > 80 % Kritisch @ > 90 %
Service Load Balancer konnte nicht erstellt werden	Erstellen des Service Load Balancers fehlgeschlagen		Kritisch
Workload-Replikat-Missverhältnis	Einige Pods sind derzeit nicht für eine Bereitstellung oder ein DaemonSet verfügbar.		Warnung @ > 1
ResourceQuota-CPU-Anfragen werden bald überschritten	CPU-Anforderungen für Namespace überschreiten bald ResourceQuota		Warnung @ > 80 % Kritisch @ > 90 %
Hohe Neuübertragungsrate	Hohe TCP-Neuübertragungsrate	Auf Netzwerküberlastung prüfen – Identifizieren Sie Arbeitslasten, die viel Netzwerkbandbreite verbrauchen. Überprüfen Sie, ob die CPU-Auslastung des Pods hoch ist. Überprüfen Sie die Hardware-Netzwerkleistung.	Warnung @ > 10 % Kritisch @ > 25 %
Knotenplattendruck	Der verfügbare Speicherplatz und die Inodes im Root-Dateisystem oder im Image-Dateisystem des Knotens haben einen Räumungsschwellenwert erreicht.	- Erhöhen Sie die Größe der Knotenfestplatten, um sicherzustellen, dass ausreichend Platz für die Anwendungsdateien vorhanden ist. - Reduzieren Sie die Verwendung von Anwendungsdateien.	Kritisch @ > 0
Cluster-CPU-Sättigung hoch	Die dem Cluster zuweisbare CPU-Sättigung ist hoch. Die CPU-Sättigung des Clusters wird berechnet als Summe der CPU-Auslastung geteilt durch die Summe der zuweisbaren CPUs aller K8s-Knoten.	Knoten hinzufügen. Reparieren Sie alle nicht geplanten Knoten. Passen Sie die Größe der Pods an, um CPU-Leistung auf Knoten freizugeben.	Warnung @ > 80 % Kritisch @ > 90 %

Zurück nach oben

Änderungsprotokoll-Monitore

Monitorname	Schwere	Monitorbeschreibung
Internes Volume entdeckt	Informativ	Diese Meldung wird angezeigt, wenn ein internes Volume erkannt wird.
Internes Volumen geändert	Informativ	Diese Meldung wird angezeigt, wenn ein internes Volume geändert wird.
Speicherknoten erkannt	Informativ	Diese Meldung wird angezeigt, wenn ein Speicherknoten erkannt wird.
Speicherknoten entfernt	Informativ	Diese Meldung wird angezeigt, wenn ein Speicherknoten entfernt wird.
Speicherpool erkannt	Informativ	Diese Meldung wird angezeigt, wenn ein Speicherpool erkannt wird.
Virtuelle Speichermaschine erkannt	Informativ	Diese Meldung wird angezeigt, wenn eine Storage Virtual Machine erkannt wird.
Geänderte virtuelle Speichermaschine	Informativ	Diese Meldung wird angezeigt, wenn eine Storage Virtual Machine geändert wird.

Zurück nach oben

Datenerfassungsmonitore

Monitorname	Beschreibung	Korrekturmaßnahme

Abschaltung der Erfassungseinheit	Data Infrastructure Insights Acquisition Units werden im Rahmen von Upgrades regelmäßig neu gestartet, um neue Funktionen einzuführen. Dies geschieht in einer typischen Umgebung einmal im Monat oder seltener. Auf eine Warnmeldung, dass eine Erfassungseinheit heruntergefahren wurde, sollte bald darauf eine Lösung folgen, in der darauf hingewiesen wird, dass die neu gestartete Erfassungseinheit eine Registrierung bei Data Infrastructure Insights abgeschlossen hat. Normalerweise dauert dieser Zyklus vom Herunterfahren bis zur Registrierung 5 bis 15 Minuten.	Wenn der Alarm häufig auftritt oder länger als 15 Minuten anhält, überprüfen Sie den Betrieb des Systems, auf dem die Erfassungseinheit gehostet wird, des Netzwerks und aller Proxys, die die AU mit dem Internet verbinden.
Collector fehlgeschlagen	Bei der Abfrage eines Datensammlers ist eine unerwartete Fehlersituation aufgetreten.	Besuchen Sie die Datensammlerseite in Data Infrastructure Insights, um mehr über die Situation zu erfahren.
Sammlerwarnung	Dieser Alarm kann typischerweise aufgrund einer fehlerhaften Konfiguration des Datensammlers oder des Zielsystems auftreten. Überprüfen Sie die Konfigurationen erneut, um zukünftige Warnungen zu verhindern. Es kann auch daran liegen, dass unvollständige Daten abgerufen wurden, obwohl der Datensammler alle Daten gesammelt hat, die er konnte. Dies kann passieren, wenn sich die Situation während der Datenerfassung ändert (z. B. wenn eine zu Beginn der Datenerfassung vorhandene virtuelle Maschine während der Datenerfassung und vor der Erfassung ihrer Daten gelöscht wird).	Überprüfen Sie die Konfiguration des Datensammlers oder Zielsystems. Beachten Sie, dass der Monitor für Collector-Warnungen mehr Warnungen senden kann als andere Monitortypen. Daher wird empfohlen, keine Warnungsempfänger festzulegen, es sei denn, Sie führen eine Fehlerbehebung durch.

Zurück nach oben

Sicherheitsmonitore

Monitorname	Schwelle	Monitorbeschreibung	Korrekturmaßnahme

AutoSupport HTTPS-Transport deaktiviert	Warnung @ < 1	AutoSupport unterstützt HTTPS, HTTP und SMTP als Transportprotokolle. Aufgrund der sensiblen Natur von AutoSupport Nachrichten empfiehlt NetApp dringend, HTTPS als Standardtransportprotokoll zum Senden von AutoSupport -Nachrichten an den NetApp Support zu verwenden.	Um HTTPS als Transportprotokoll für AutoSupport Nachrichten festzulegen, führen Sie den folgenden ONTAP Befehl aus: …system node autosupport modify -transport https
Cluster Unsichere Chiffren für SSH	Warnung @ < 1	Zeigt an, dass SSH unsichere Chiffren verwendet, beispielsweise Chiffren, die mit *cbc beginnen.	Um die CBC-Chiffren zu entfernen, führen Sie den folgenden ONTAP Befehl aus: …security ssh remove -vserver <admin vserver> -ciphers aes256-cbc,aes192-cbc,aes128-cbc,3des-cbc
Cluster-Anmeldebanner deaktiviert	Warnung @ < 1	Zeigt an, dass das Anmeldebanner für Benutzer deaktiviert ist, die auf das ONTAP -System zugreifen. Das Anzeigen eines Anmeldebanners ist hilfreich, um Erwartungen hinsichtlich des Zugriffs auf das System und seiner Nutzung zu wecken.	Um das Anmeldebanner für einen Cluster zu konfigurieren, führen Sie den folgenden ONTAP -Befehl aus: …security login banner modify -vserver <admin svm> -message "Access restricted to authorized users"

Cluster-Peer-Kommunikation nicht verschlüsselt	Warnung @ < 1	Wenn Sie Daten für die Notfallwiederherstellung, das Caching oder die Sicherung replizieren, müssen Sie diese Daten während des Transports über die Leitung von einem ONTAP Cluster zu einem anderen schützen. Die Verschlüsselung muss sowohl auf dem Quell- als auch auf dem Zielcluster konfiguriert werden.	Um die Verschlüsselung für Cluster-Peer-Beziehungen zu aktivieren, die vor ONTAP 9.6 erstellt wurden, müssen der Quell- und der Zielcluster auf 9.6 aktualisiert werden. Verwenden Sie dann den Befehl „Cluster Peer Modify“, um sowohl die Quell- als auch die Ziel-Cluster-Peers so zu ändern, dass sie die Cluster-Peering-Verschlüsselung verwenden. … Weitere Informationen finden Sie im NetApp Security Hardening Guide für ONTAP 9.
Standardmäßiger lokaler Administratorbenutzer aktiviert	Warnung @ > 0	NetApp empfiehlt, alle nicht benötigten Standard-Admin-Benutzerkonten (integriert) mit dem Sperrbefehl zu sperren (deaktivieren). Dabei handelt es sich in erster Linie um Standardkonten, deren Passwörter nie aktualisiert oder geändert wurden.	Um das integrierte „Admin“-Konto zu sperren, führen Sie den folgenden ONTAP Befehl aus: …security login lock -username admin
FIPS-Modus deaktiviert	Warnung @ < 1	Wenn die FIPS 140-2-Konformität aktiviert ist, werden TLSv1 und SSLv3 deaktiviert und nur TLSv1.1 und TLSv1.2 bleiben aktiviert. ONTAP verhindert, dass Sie TLSv1 und SSLv3 aktivieren, wenn die FIPS 140-2-Konformität aktiviert ist.	Um die FIPS 140-2-Konformität auf einem Cluster zu aktivieren, führen Sie den folgenden ONTAP -Befehl im erweiterten Berechtigungsmodus aus: …security config modify -interface SSL -is-fips -enabled true

Protokollweiterleitung nicht verschlüsselt	Warnung @ < 1	Das Auslagern von Syslog-Informationen ist notwendig, um den Umfang oder die Auswirkungen einer Sicherheitsverletzung auf ein einzelnes System oder eine einzelne Lösung zu beschränken. Daher empfiehlt NetApp , Syslog-Informationen sicher an einen sicheren Speicher- oder Aufbewahrungsort auszulagern.	Sobald ein Protokollweiterleitungsziel erstellt wurde, kann sein Protokoll nicht mehr geändert werden. Um zu einem verschlüsselten Protokoll zu wechseln, löschen Sie das Protokollweiterleitungsziel und erstellen Sie es mit dem folgenden ONTAP -Befehl neu: …cluster log-forwarding create -destination <Ziel-IP> -protocol tcp-encrypted
MD5-gehashtes Passwort	Warnung @ > 0	NetApp empfiehlt dringend, für ONTAP Benutzerkontenkennwörter die sicherere Hash-Funktion SHA-512 zu verwenden. Konten, die die weniger sichere MD5-Hashfunktion verwenden, sollten zur SHA-512-Hashfunktion migrieren.	NetApp empfiehlt dringend, Benutzerkonten auf die sicherere SHA-512-Lösung zu migrieren, indem Benutzer ihre Passwörter ändern. …Um Konten mit Passwörtern zu sperren, die die MD5-Hash-Funktion verwenden, führen Sie den folgenden ONTAP Befehl aus: …security login lock -vserver * -username * -hash -function md5
Es sind keine NTP-Server konfiguriert	Warnung @ < 1	Zeigt an, dass für den Cluster keine NTP-Server konfiguriert sind. Aus Redundanzgründen und für optimalen Service empfiehlt NetApp , dem Cluster mindestens drei NTP-Server zuzuordnen.	Um einen NTP-Server mit dem Cluster zu verknüpfen, führen Sie den folgenden ONTAP Befehl aus: cluster time-service ntp server create -server <ntp server host name or ip address>
Die Anzahl der NTP-Server ist niedrig	Warnung @ < 3	Zeigt an, dass der Cluster weniger als 3 konfigurierte NTP-Server hat. Aus Redundanzgründen und für optimalen Service empfiehlt NetApp , dem Cluster mindestens drei NTP-Server zuzuordnen.	Um einen NTP-Server mit dem Cluster zu verknüpfen, führen Sie den folgenden ONTAP Befehl aus: …cluster time-service ntp server create -server <ntp server host name or ip address>

Remote Shell aktiviert	Warnung @ > 0	Remote Shell ist keine sichere Methode zum Einrichten des Befehlszeilenzugriffs auf die ONTAP Lösung. Für einen sicheren Fernzugriff sollte Remote Shell deaktiviert werden.	NetApp empfiehlt Secure Shell (SSH) für sicheren Remote-Zugriff. …Um Remote Shell auf einem Cluster zu deaktivieren, führen Sie den folgenden ONTAP -Befehl im erweiterten Berechtigungsmodus aus: …security protocol modify -application rsh- enabled false
Speicher-VM-Auditprotokoll deaktiviert	Warnung @ < 1	Zeigt an, dass die Audit-Protokollierung für SVM deaktiviert ist.	Um das Audit-Protokoll für einen virtuellen Server zu konfigurieren, führen Sie den folgenden ONTAP -Befehl aus: …vserver audit enable -vserver <svm>
Unsichere Verschlüsselungsverfahren für Storage-VMs für SSH	Warnung @ < 1	Zeigt an, dass SSH unsichere Chiffren verwendet, beispielsweise Chiffren, die mit *cbc beginnen.	Um die CBC-Chiffren zu entfernen, führen Sie den folgenden ONTAP Befehl aus: …security ssh remove -vserver <vserver> -ciphers aes256-cbc,aes192-cbc,aes128-cbc,3des-cbc
Storage VM-Anmeldebanner deaktiviert	Warnung @ < 1	Zeigt an, dass das Anmeldebanner für Benutzer deaktiviert ist, die auf SVMs im System zugreifen. Das Anzeigen eines Anmeldebanners ist hilfreich, um Erwartungen hinsichtlich des Zugriffs auf das System und seiner Nutzung zu wecken.	Um das Anmeldebanner für einen Cluster zu konfigurieren, führen Sie den folgenden ONTAP -Befehl aus: …security login banner modify -vserver <svm> -message "Access restricted to authorized users"
Telnet-Protokoll aktiviert	Warnung @ > 0	Telnet ist keine sichere Methode zum Herstellen eines Befehlszeilenzugriffs auf die ONTAP Lösung. Für einen sicheren Fernzugriff sollte Telnet deaktiviert werden.	NetApp empfiehlt Secure Shell (SSH) für sicheren Fernzugriff. Um Telnet auf einem Cluster zu deaktivieren, führen Sie den folgenden ONTAP -Befehl im erweiterten Berechtigungsmodus aus: …security protocol modify -application telnet -enabled false

Zurück nach oben

Datenschutzmonitore

Monitorname	Schwellenwerte	Monitorbeschreibung	Korrekturmaßnahme
Nicht genügend Speicherplatz für die LUN-Snapshot-Kopie	(Filter contains_luns = Ja) Warnung @ > 95 %…Kritisch @ > 100 %	Die Speicherkapazität eines Datenträgers ist zum Speichern von Anwendungs- und Kundendaten erforderlich. Ein Teil dieses Speicherplatzes, der sogenannte reservierte Snapshot-Speicherplatz, wird zum Speichern von Snapshots verwendet, die einen lokalen Schutz der Daten ermöglichen. Je mehr neue und aktualisierte Daten im ONTAP Volume gespeichert werden, desto mehr Snapshot-Kapazität wird verwendet und desto weniger Snapshot-Speicherkapazität steht für zukünftige neue oder aktualisierte Daten zur Verfügung. Wenn die Snapshot-Datenkapazität innerhalb eines Volumes den gesamten Snapshot-Reservespeicherplatz erreicht, kann dies dazu führen, dass der Kunde keine neuen Snapshot-Daten speichern kann und der Schutzgrad der Daten in den LUNs des Volumes verringert wird. Durch die Überwachung der Snapshot-Kapazität des verwendeten Volumes wird die Kontinuität der Datendienste sichergestellt.	**Sofortmaßnahmen** Wenn ein kritischer Schwellenwert überschritten wird, sollten Sie sofortige Maßnahmen in Betracht ziehen, um die Dienstunterbrechung zu minimieren: 1. Konfigurieren Sie Snapshots, um den Datenspeicherplatz im Volume zu nutzen, wenn die Snapshot-Reserve voll ist. 2. Löschen Sie einige ältere, nicht mehr benötigte Snapshots, um Speicherplatz freizugeben. **Bald zu ergreifende Maßnahmen** Wenn der Warnschwellenwert überschritten wird, planen Sie die folgenden sofortigen Maßnahmen: 1. Erhöhen Sie den Snapshot-Reservespeicherplatz innerhalb des Volumes, um dem Wachstum Rechnung zu tragen. 2. Konfigurieren Sie Snapshots, um den Datenspeicherplatz im Volume zu nutzen, wenn die Snapshot-Reserve voll ist.

SnapMirror -Beziehungsverzögerung	Warnung bei > 150 % … Kritisch bei > 300 %	Die SnapMirror Beziehungsverzögerung ist die Differenz zwischen dem Zeitstempel des Snapshots und der Zeit auf dem Zielsystem. Der lag_time_percent ist das Verhältnis der Verzögerungszeit zum Zeitplanintervall der SnapMirror -Richtlinie. Wenn die Verzögerungszeit dem Zeitplanintervall entspricht, beträgt der lag_time_percent 100 %. Wenn die SnapMirror -Richtlinie keinen Zeitplan hat, wird lag_time_percent nicht berechnet.	Überwachen Sie den SnapMirror -Status mit dem Befehl „snapmirror show“. Überprüfen Sie den SnapMirror Übertragungsverlauf mit dem Befehl „snapmirror show-history“

Zurück nach oben

Cloud Volume (CVO)-Monitore

Monitorname	CI-Schweregrad	Monitorbeschreibung	Korrekturmaßnahme
CVO-Festplatte außer Betrieb	INFO	Dieses Ereignis tritt ein, wenn eine Festplatte außer Betrieb genommen wird, weil sie als fehlerhaft markiert wurde, bereinigt wird oder in das Wartungscenter gelangt ist.	Keine

CVO-Rückgabe des Speicherpools fehlgeschlagen	KRITISCH	Dieses Ereignis tritt während der Migration eines Aggregats im Rahmen einer Speicher-Failover-(SFO)-Rückgabe auf, wenn der Zielknoten die Objektspeicher nicht erreichen kann.	Führen Sie die folgenden Korrekturmaßnahmen durch: Überprüfen Sie mit dem Befehl „Network Interface Show“, ob Ihr Intercluster-LIF online und funktionsfähig ist. Überprüfen Sie die Netzwerkkonnektivität zum Objektspeicherserver, indem Sie den Befehl „Ping“ über den Intercluster-LIF des Zielknotens verwenden. Überprüfen Sie mit dem Befehl „aggregate object-store config show“, ob sich die Konfiguration Ihres Objektspeichers geändert hat und ob die Anmelde- und Verbindungsinformationen noch immer korrekt sind. Alternativ können Sie den Fehler überschreiben, indem Sie für den Parameter „require-partner-waiting“ des Giveback-Befehls „false“ angeben. Wenden Sie sich an den technischen Support von NetApp , um weitere Informationen oder Unterstützung zu erhalten.

CVO HA-Verbindung ausgefallen	WARNING (Warnung)	Die Hochverfügbarkeitsverbindung (HA) ist ausgefallen. Risiko eines Dienstausfalls, wenn kein Failover verfügbar ist.	Korrekturmaßnahmen hängen von der Anzahl und Art der von der Plattform unterstützten HA-Verbindungslinks sowie vom Grund für den Verbindungsausfall ab. Wenn die Links ausgefallen sind: Überprüfen Sie, ob beide Controller im HA-Paar betriebsbereit sind. Stellen Sie bei extern angeschlossenen Links sicher, dass die Verbindungskabel richtig angeschlossen sind und dass die Small Form-Factor Pluggables (SFPs), falls vorhanden, richtig auf beiden Controllern sitzen. Deaktivieren und aktivieren Sie intern verbundene Links nacheinander mit den Befehlen „ic link off“ und „ic link on“. Wenn Links deaktiviert sind, aktivieren Sie die Links mit dem Befehl „ic link on“. Wenn kein Peer verbunden ist, deaktivieren und aktivieren Sie die Links nacheinander mit den Befehlen „ic link off“ und „ic link on“. Wenden Sie sich an den technischen Support von NetApp, wenn das Problem weiterhin besteht.

CVO-Maximale Sitzungen pro Benutzer überschritten	WARNING (Warnung)	Sie haben die maximal zulässige Anzahl von Sitzungen pro Benutzer über eine TCP-Verbindung überschritten. Jede Anfrage zum Herstellen einer Sitzung wird abgelehnt, bis einige Sitzungen freigegeben werden.	Führen Sie die folgenden Korrekturmaßnahmen durch: Überprüfen Sie alle auf dem Client ausgeführten Anwendungen und beenden Sie alle, die nicht ordnungsgemäß funktionieren. Starten Sie den Client neu. Überprüfen Sie, ob das Problem durch eine neue oder vorhandene Anwendung verursacht wird: Wenn die Anwendung neu ist, legen Sie mit dem Befehl „cifs option modify -max-opens -same-file-per-tree“ einen höheren Schwellenwert für den Client fest. In einigen Fällen funktionieren die Clients wie erwartet, erfordern jedoch eine höhere Schwelle. Sie sollten über erweiterte Berechtigungen verfügen, um einen höheren Schwellenwert für den Client festzulegen. Wenn das Problem durch eine vorhandene Anwendung verursacht wird, liegt möglicherweise ein Problem mit dem Client vor. Wenden Sie sich an den technischen Support von NetApp , um weitere Informationen oder Unterstützung zu erhalten.

CVO NetBIOS-Namenskonflikt	KRITISCH	Der NetBIOS-Namensdienst hat von einem Remotecomputer eine negative Antwort auf eine Namensregistrierungsanforderung erhalten. Dies wird normalerweise durch einen Konflikt im NetBIOS-Namen oder einem Alias verursacht. Dies hat zur Folge, dass Clients möglicherweise nicht auf Daten zugreifen oder keine Verbindung zum richtigen Datenbereitstellungsknoten im Cluster herstellen können.	Führen Sie eine der folgenden Korrekturmaßnahmen durch: Wenn ein Konflikt im NetBIOS-Namen oder einem Alias vorliegt, führen Sie einen der folgenden Schritte aus: Löschen Sie den doppelten NetBIOS-Alias mit dem Befehl „vserver cifs delete -aliases alias -vserver vserver“. Benennen Sie einen NetBIOS-Alias um, indem Sie den doppelten Namen löschen und einen Alias mit einem neuen Namen hinzufügen, indem Sie den Befehl „vserver cifs create -aliases alias -vserver vserver“ verwenden. Wenn keine Aliase konfiguriert sind und ein Konflikt im NetBIOS-Namen vorliegt, benennen Sie den CIFS-Server mit den Befehlen „vserver cifs delete -vserver vserver“ und „vserver cifs create -cifs -server netbiosname“ um. HINWEIS: Durch das Löschen eines CIFS-Servers kann der Zugriff auf die Daten unzugänglich werden. Entfernen Sie den NetBIOS-Namen oder benennen Sie das NetBIOS auf dem Remotecomputer um.
CVO NFSv4-Speicherpool erschöpft	KRITISCH	Ein NFSv4-Speicherpool ist erschöpft.	Wenn der NFS-Server nach diesem Ereignis länger als 10 Minuten nicht reagiert, wenden Sie sich an den technischen Support von NetApp .
CVO-Knotenpanik	WARNING (Warnung)	Dieses Ereignis wird ausgelöst, wenn eine Panik auftritt	Wenden Sie sich an den NetApp Kundensupport.

CVO-Knoten-Root-Volume-Speicherplatz niedrig	KRITISCH	Das System hat festgestellt, dass auf dem Stammvolume gefährlich wenig Speicherplatz vorhanden ist. Der Knoten ist nicht voll funktionsfähig. Möglicherweise ist innerhalb des Clusters ein Failover der Daten-LIFs aufgetreten, weshalb der NFS- und CIFS-Zugriff auf den Knoten eingeschränkt ist. Die Verwaltungsfunktionen sind auf lokale Wiederherstellungsverfahren für den Knoten beschränkt, um Speicherplatz auf dem Stammvolume freizugeben.	Führen Sie die folgenden Korrekturmaßnahmen durch: Schaffen Sie Speicherplatz auf dem Stammvolume, indem Sie alte Snapshot-Kopien löschen, nicht mehr benötigte Dateien aus dem Verzeichnis /mroot löschen oder die Kapazität des Stammvolumes erweitern. Starten Sie den Controller neu. Wenden Sie sich an den technischen Support von NetApp , um weitere Informationen oder Unterstützung zu erhalten.
CVO Nicht vorhandene Admin-Freigabe	KRITISCH	Vscan-Problem: Ein Client hat versucht, eine Verbindung zu einer nicht vorhandenen ONTAP_ADMIN$-Freigabe herzustellen.	Stellen Sie sicher, dass Vscan für die angegebene SVM-ID aktiviert ist. Durch die Aktivierung von Vscan auf einer SVM wird die ONTAP_ADMIN$-Freigabe automatisch für die SVM erstellt.
CVO Object Store Host nicht auflösbar	KRITISCH	Der Hostname des Objektspeicherservers kann nicht in eine IP-Adresse aufgelöst werden. Der Objektspeicherclient kann ohne Auflösung in eine IP-Adresse nicht mit dem Objektspeicherserver kommunizieren. Dies kann dazu führen, dass auf die Daten nicht zugegriffen werden kann.	Überprüfen Sie die DNS-Konfiguration, um sicherzustellen, dass der Hostname korrekt mit einer IP-Adresse konfiguriert ist.

CVO Object Store Intercluster LIF Down	KRITISCH	Der Objektspeicher-Client kann kein funktionsfähiges LIF für die Kommunikation mit dem Objektspeicher-Server finden. Der Knoten lässt keinen Objektspeicher-Clientverkehr zu, bis das Intercluster-LIF betriebsbereit ist. Dies kann dazu führen, dass auf die Daten nicht zugegriffen werden kann.	Führen Sie die folgenden Korrekturmaßnahmen durch: Überprüfen Sie den LIF-Status zwischen Clustern mit dem Befehl „network interface show -role intercluster“. Überprüfen Sie, ob das Intercluster-LIF richtig konfiguriert und betriebsbereit ist. Wenn kein Intercluster-LIF konfiguriert ist, fügen Sie es mit dem Befehl „network interface create -role intercluster“ hinzu.
CVO-Objektspeichersignatur stimmt nicht überein	KRITISCH	Die an den Objektspeicherserver gesendete Anforderungssignatur stimmt nicht mit der vom Client berechneten Signatur überein. Dies kann dazu führen, dass auf die Daten nicht zugegriffen werden kann.	Überprüfen Sie, ob der geheime Zugriffsschlüssel richtig konfiguriert ist. Wenn es richtig konfiguriert ist, wenden Sie sich an den technischen Support von NetApp , um Hilfe zu erhalten.
CVO QoS-Monitor-Speicher voll ausgelastet	KRITISCH	Der dynamische Speicher des QoS-Subsystems hat für die aktuelle Plattformhardware seine Grenze erreicht. Einige QoS-Funktionen sind möglicherweise nur eingeschränkt verfügbar.	Löschen Sie einige aktive Workloads oder Streams, um Speicher freizugeben. Verwenden Sie den Befehl „statistics show -object workload -counter ops“, um zu ermitteln, welche Workloads aktiv sind. Aktive Workloads zeigen Operationen ungleich Null. Verwenden Sie dann den Befehl „workload delete <workload_name>“ mehrmals, um bestimmte Workloads zu entfernen. Alternativ können Sie den Befehl „stream delete -workload <workload name> *“ verwenden, um die zugehörigen Streams aus der aktiven Workload zu löschen.

CVO READDIR-Zeitüberschreitung	KRITISCH	Ein READDIR-Dateivorgang hat das zulässige Zeitlimit für die Ausführung in WAFL überschritten. Dies kann an sehr großen oder spärlich gefüllten Verzeichnissen liegen. Es werden Korrekturmaßnahmen empfohlen.	Führen Sie die folgenden Korrekturmaßnahmen durch: Suchen Sie nach spezifischen Informationen zu aktuellen Verzeichnissen, bei denen READDIR-Dateivorgänge abgelaufen sind, indem Sie den folgenden NodeShell-CLI-Befehl mit der Berechtigung „diag“ verwenden: wafl readdir notice show. Überprüfen Sie, ob Verzeichnisse als spärlich gekennzeichnet sind oder nicht: Wenn ein Verzeichnis als spärlich gekennzeichnet ist, wird empfohlen, den Inhalt des Verzeichnisses in ein neues Verzeichnis zu kopieren, um die spärliche Verzeichnisdatei zu entfernen. Wenn ein Verzeichnis nicht als spärlich gekennzeichnet ist und das Verzeichnis groß ist, wird empfohlen, die Größe der Verzeichnisdatei zu reduzieren, indem Sie die Anzahl der Dateieinträge im Verzeichnis verringern.

CVO-Verlagerung des Speicherpools fehlgeschlagen	KRITISCH	Dieses Ereignis tritt während der Verschiebung eines Aggregats auf, wenn der Zielknoten die Objektspeicher nicht erreichen kann.	Führen Sie die folgenden Korrekturmaßnahmen durch: Überprüfen Sie mit dem Befehl „Network Interface Show“, ob Ihr Intercluster-LIF online und funktionsfähig ist. Überprüfen Sie die Netzwerkkonnektivität zum Objektspeicherserver, indem Sie den Befehl „Ping“ über den Intercluster-LIF des Zielknotens verwenden. Überprüfen Sie mit dem Befehl „aggregate object-store config show“, ob sich die Konfiguration Ihres Objektspeichers geändert hat und ob die Anmelde- und Verbindungsinformationen noch immer korrekt sind. Alternativ können Sie den Fehler überschreiben, indem Sie den Parameter „override-destination-checks“ des Umzugsbefehls verwenden. Wenden Sie sich an den technischen Support von NetApp , um weitere Informationen oder Unterstützung zu erhalten.

CVO-Schattenkopie fehlgeschlagen	KRITISCH	Ein Volume Shadow Copy Service (VSS), ein Sicherungs- und Wiederherstellungsdienstvorgang von Microsoft Server, ist fehlgeschlagen.	Überprüfen Sie anhand der in der Ereignismeldung bereitgestellten Informationen Folgendes: Ist die Schattenkopiekonfiguration aktiviert? Sind die entsprechenden Lizenzen installiert? Auf welchen Freigaben wird der Schattenkopievorgang ausgeführt? Ist der Freigabename korrekt? Existiert der Freigabepfad? Wie ist der Status des Schattenkopiesatzes und seiner Schattenkopien?
CVO Storage VM-Stopp erfolgreich	INFO	Diese Meldung wird angezeigt, wenn ein „vServer-Stopp“-Vorgang erfolgreich ist.	Verwenden Sie den Befehl „vserver start“, um den Datenzugriff auf einer Speicher-VM zu starten.
CVO Zu viele CIFS-Authentifizierungen	WARNING (Warnung)	Viele Authentifizierungsverhandlungen fanden gleichzeitig statt. Von diesem Client liegen 256 unvollständige neue Sitzungsanforderungen vor.	Untersuchen Sie, warum der Client 256 oder mehr neue Verbindungsanforderungen erstellt hat. Möglicherweise müssen Sie sich an den Anbieter des Clients oder der Anwendung wenden, um die Ursache des Fehlers zu ermitteln.
Nicht zugewiesene CVO-Datenträger	INFO	Dem System sind keine Festplatten zugewiesen – Kapazität wird verschwendet und Ihr System weist möglicherweise eine Fehlkonfiguration auf oder es wurden teilweise Konfigurationsänderungen vorgenommen.	Führen Sie die folgenden Korrekturmaßnahmen durch: Ermitteln Sie mit dem Befehl „disk show -n“, welche Datenträger nicht zugewiesen sind. Weisen Sie die Datenträger mit dem Befehl „disk assign“ einem System zu.

CVO: Unbefugter Benutzerzugriff auf die Admin-Freigabe	WARNING (Warnung)	Ein Client hat versucht, eine Verbindung zur privilegierten Freigabe ONTAP_ADMIN$ herzustellen, obwohl der angemeldete Benutzer kein zulässiger Benutzer ist.	Führen Sie die folgenden Korrekturmaßnahmen durch: Stellen Sie sicher, dass der angegebene Benutzername und die IP-Adresse in einem der aktiven Vscan-Scannerpools konfiguriert sind. Überprüfen Sie die aktuell aktive Scannerpool-Konfiguration mit dem Befehl „vserver vscan scanner pool show-active“.
CVO-Virus erkannt	WARNING (Warnung)	Ein Vscan-Server hat dem Speichersystem einen Fehler gemeldet. Dies weist normalerweise darauf hin, dass ein Virus gefunden wurde. Dieses Ereignis kann jedoch auch durch andere Fehler auf dem Vscan-Server verursacht werden. Der Clientzugriff auf die Datei wird verweigert. Der Vscan-Server kann die Datei je nach seinen Einstellungen und seiner Konfiguration bereinigen, unter Quarantäne stellen oder löschen.	Überprüfen Sie das im „Syslog“-Ereignis gemeldete Protokoll des Vscan-Servers, um festzustellen, ob die infizierte Datei erfolgreich bereinigt, unter Quarantäne gestellt oder gelöscht werden konnte. Wenn dies nicht möglich ist, muss ein Systemadministrator die Datei möglicherweise manuell löschen.
CVO-Volumen offline	INFO	Diese Meldung zeigt an, dass ein Volume offline geschaltet wurde.	Bringen Sie das Volume wieder online.
CVO-Volumen beschränkt	INFO	Dieses Ereignis zeigt an, dass ein flexibles Volumen eingeschränkt wird.	Bringen Sie das Volume wieder online.

Zurück nach oben

SnapMirror für Business Continuity (SMBC) Mediator Log Monitors

Monitorname	Schwere	Monitorbeschreibung	Korrekturmaßnahme
ONTAP Mediator hinzugefügt	INFO	Diese Meldung wird angezeigt, wenn ONTAP Mediator erfolgreich zu einem Cluster hinzugefügt wurde.	Keine

ONTAP Mediator nicht zugänglich	KRITISCH	Diese Meldung wird angezeigt, wenn entweder der ONTAP Mediator einem anderen Zweck zugeführt wird oder das Mediator-Paket nicht mehr auf dem Mediator-Server installiert ist. Daher ist ein SnapMirror Failover nicht möglich.	Entfernen Sie die Konfiguration des aktuellen ONTAP Mediators mit dem Befehl „snapmirror mediator remove“. Konfigurieren Sie den Zugriff auf den ONTAP Mediator neu, indem Sie den Befehl „snapmirror mediator add“ verwenden.
ONTAP Mediator entfernt	INFO	Diese Meldung wird angezeigt, wenn ONTAP Mediator erfolgreich aus einem Cluster entfernt wurde.	Keine
ONTAP Mediator nicht erreichbar	WARNING (Warnung)	Diese Meldung wird angezeigt, wenn der ONTAP Mediator in einem Cluster nicht erreichbar ist. Daher ist ein SnapMirror Failover nicht möglich.	Überprüfen Sie die Netzwerkkonnektivität zum ONTAP Mediator mithilfe der Befehle „Network Ping“ und „Network Traceroute“. Wenn das Problem weiterhin besteht, entfernen Sie die Konfiguration des aktuellen ONTAP Mediators mit dem Befehl „snapmirror mediator remove“. Konfigurieren Sie den Zugriff auf den ONTAP Mediator neu, indem Sie den Befehl „snapmirror mediator add“ verwenden.
SMBC CA-Zertifikat abgelaufen	KRITISCH	Diese Meldung wird angezeigt, wenn das Zertifikat der ONTAP Mediator-Zertifizierungsstelle (CA) abgelaufen ist. Infolgedessen ist jegliche weitere Kommunikation mit dem ONTAP Mediator nicht möglich.	Entfernen Sie die Konfiguration des aktuellen ONTAP Mediators mit dem Befehl „snapmirror mediator remove“. Aktualisieren Sie ein neues CA-Zertifikat auf dem ONTAP Mediator-Server. Konfigurieren Sie den Zugriff auf den ONTAP Mediator neu, indem Sie den Befehl „snapmirror mediator add“ verwenden.

SMBC CA-Zertifikat läuft ab	WARNING (Warnung)	Diese Meldung wird angezeigt, wenn das Zertifikat der ONTAP Mediator-Zertifizierungsstelle (CA) innerhalb der nächsten 30 Tage abläuft.	Entfernen Sie vor Ablauf dieses Zertifikats die Konfiguration des aktuellen ONTAP Mediators mit dem Befehl „snapmirror mediator remove“. Aktualisieren Sie ein neues CA-Zertifikat auf dem ONTAP Mediator-Server. Konfigurieren Sie den Zugriff auf den ONTAP Mediator neu, indem Sie den Befehl „snapmirror mediator add“ verwenden.
SMBC-Client-Zertifikat abgelaufen	KRITISCH	Diese Meldung wird angezeigt, wenn das ONTAP Mediator-Client-Zertifikat abgelaufen ist. Infolgedessen ist jegliche weitere Kommunikation mit dem ONTAP Mediator nicht möglich.	Entfernen Sie die Konfiguration des aktuellen ONTAP Mediators mit dem Befehl „snapmirror mediator remove“. Konfigurieren Sie den Zugriff auf den ONTAP Mediator neu, indem Sie den Befehl „snapmirror mediator add“ verwenden.
SMBC-Client-Zertifikat läuft ab	WARNING (Warnung)	Diese Meldung wird angezeigt, wenn das Client-Zertifikat des ONTAP Mediators innerhalb der nächsten 30 Tage abläuft.	Entfernen Sie vor Ablauf dieses Zertifikats die Konfiguration des aktuellen ONTAP Mediators mit dem Befehl „snapmirror mediator remove“. Konfigurieren Sie den Zugriff auf den ONTAP Mediator neu, indem Sie den Befehl „snapmirror mediator add“ verwenden.

SMBC-Beziehung nicht synchron Hinweis: UM hat diese nicht	KRITISCH	Diese Meldung wird angezeigt, wenn sich der Status einer SnapMirror for Business Continuity (SMBC)-Beziehung von „synchronisiert“ in „nicht synchron“ ändert. Dadurch wird der Datenschutz bei RPO=0 gestört.	Überprüfen Sie die Netzwerkverbindung zwischen dem Quell- und dem Zielvolume. Überwachen Sie den SMBC-Beziehungsstatus, indem Sie auf dem Ziel den Befehl „snapmirror show“ und auf der Quelle den Befehl „snapmirror list-destinations“ verwenden. Durch die automatische Neusynchronisierung wird versucht, die Beziehung wieder in den Status „synchronisiert“ zu versetzen. Wenn die Neusynchronisierung fehlschlägt, überprüfen Sie, ob alle Knoten im Cluster im Quorum sind und fehlerfrei funktionieren.
SMBC-Serverzertifikat abgelaufen	KRITISCH	Diese Meldung wird angezeigt, wenn das ONTAP Mediator-Serverzertifikat abgelaufen ist. Infolgedessen ist jegliche weitere Kommunikation mit dem ONTAP Mediator nicht möglich.	Entfernen Sie die Konfiguration des aktuellen ONTAP Mediators mit dem Befehl „snapmirror mediator remove“. Aktualisieren Sie ein neues Serverzertifikat auf dem ONTAP Mediator-Server. Konfigurieren Sie den Zugriff auf den ONTAP Mediator neu, indem Sie den Befehl „snapmirror mediator add“ verwenden.
SMBC-Serverzertifikat läuft ab	WARNING (Warnung)	Diese Meldung wird angezeigt, wenn das ONTAP Mediator-Serverzertifikat innerhalb der nächsten 30 Tage abläuft.	Entfernen Sie vor Ablauf dieses Zertifikats die Konfiguration des aktuellen ONTAP Mediators mit dem Befehl „snapmirror mediator remove“. Aktualisieren Sie ein neues Serverzertifikat auf dem ONTAP Mediator-Server. Konfigurieren Sie den Zugriff auf den ONTAP Mediator neu, indem Sie den Befehl „snapmirror mediator add“ verwenden.

Zurück nach oben

Zusätzliche Strom-, Heartbeat- und sonstige Systemmonitore

Monitorname	Schwere	Monitorbeschreibung	Korrekturmaßnahme
Disk Shelf-Stromversorgung entdeckt	INFORMATIONS	Diese Meldung wird angezeigt, wenn dem Festplattenregal ein Netzteil hinzugefügt wird.	KEINER
Stromversorgung der Festplattenregale entfernt	INFORMATIONS	Diese Meldung tritt auf, wenn ein Netzteil aus dem Festplattenregal entfernt wird.	KEINER
Automatische ungeplante Umschaltung von MetroCluster deaktiviert	KRITISCH	Diese Meldung wird angezeigt, wenn die Funktion zur automatischen ungeplanten Umschaltung deaktiviert ist.	Führen Sie den Befehl „metrocluster modify -node-name <Knotenname> -automatic -switchover-onfailure true“ für jeden Knoten im Cluster aus, um die automatische Umschaltung zu aktivieren.
MetroCluster Speicherbrücke nicht erreichbar	KRITISCH	Die Speicherbrücke ist über das Verwaltungsnetzwerk nicht erreichbar	1) Wenn die Bridge per SNMP überwacht wird, überprüfen Sie mit dem Befehl „Network Interface Show“, ob das Knotenverwaltungs-LIF aktiv ist. Überprüfen Sie mit dem Befehl „Netzwerk-Ping“, ob die Bridge aktiv ist. 2) Wenn die Bridge In-Band überwacht wird, überprüfen Sie die Fabric-Verkabelung zur Bridge und stellen Sie dann sicher, dass die Bridge eingeschaltet ist.
MetroCluster Bridge-Temperatur anormal – unter dem kritischen Wert	KRITISCH	Der Sensor auf der Fibre Channel Bridge meldet eine Temperatur, die unterhalb des kritischen Schwellenwerts liegt.	1) Überprüfen Sie den Betriebsstatus der Lüfter auf der Speicherbrücke. 2) Stellen Sie sicher, dass die Brücke unter den empfohlenen Temperaturbedingungen betrieben wird.

Monitorname	Schwere	Monitorbeschreibung	Korrekturmaßnahme
Temperatur der MetroCluster -Brücke abnormal – über dem kritischen Wert	KRITISCH	Der Sensor auf der Fibre Channel Bridge meldet eine Temperatur, die über dem kritischen Schwellenwert liegt.	1) Überprüfen Sie den Betriebsstatus des Gehäusetemperatursensors auf der Speicherbrücke mit dem Befehl „storage bridge show -cooling“. 2) Stellen Sie sicher, dass die Speicherbrücke unter den empfohlenen Temperaturbedingungen betrieben wird.
MetroCluster -Aggregat bleibt zurück	WARNING (Warnung)	Das Aggregat wurde beim Zurückfahren zurückgelassen.	1) Überprüfen Sie den Aggregatzustand mit dem Befehl „aggr show“. 2) Wenn das Aggregat online ist, geben Sie es mit dem Befehl „metrocluster switchback“ an seinen ursprünglichen Besitzer zurück.

Monitorname	Schwere	Monitorbeschreibung	Korrekturmaßnahme
Alle Verbindungen zwischen Metrocluster-Partnern unterbrochen	KRITISCH	RDMA-Verbindungsadapter und Intercluster-LIFs haben die Verbindung zum Peering-Cluster unterbrochen oder der Peering-Cluster ist ausgefallen.	1) Stellen Sie sicher, dass die Intercluster-LIFs betriebsbereit sind. Reparieren Sie die Intercluster-LIFs, wenn sie ausgefallen sind. 2) Überprüfen Sie mit dem Befehl „Cluster Peer Ping“, ob der Peering-Cluster betriebsbereit ist. Wenn der Peering-Cluster ausgefallen ist, lesen Sie den MetroCluster Disaster Recovery Guide. 3) Überprüfen Sie für Fabric MetroCluster, ob die Back-End-Fabric-ISLs betriebsbereit sind. Reparieren Sie die Back-End-Fabric-ISLs, wenn sie ausgefallen sind. 4) Überprüfen Sie bei MetroCluster -Konfigurationen ohne Fabric, ob die Verkabelung zwischen den RDMA-Verbindungsadaptern korrekt ist. Konfigurieren Sie die Verkabelung neu, wenn die Verbindungen unterbrochen sind.
MetroCluster Partner über Peering-Netzwerk nicht erreichbar	KRITISCH	Die Verbindung zum Peer-Cluster ist unterbrochen.	1) Stellen Sie sicher, dass der Port mit dem richtigen Netzwerk/Switch verbunden ist. 2) Stellen Sie sicher, dass das Intercluster-LIF mit dem Peered-Cluster verbunden ist. 3) Stellen Sie mit dem Befehl „Cluster Peer Ping“ sicher, dass der Peering-Cluster betriebsbereit ist. Wenn der Peering-Cluster ausgefallen ist, lesen Sie den MetroCluster Disaster Recovery Guide.

Monitorname	Schwere	Monitorbeschreibung	Korrekturmaßnahme
MetroCluster Inter Switch: Alle Links ausgefallen	KRITISCH	Alle Inter-Switch Links (ISLs) auf dem Speicher-Switch sind ausgefallen.	1) Reparieren Sie die Back-End-Fabric-ISLs auf dem Speicher-Switch. 2) Stellen Sie sicher, dass der Partner-Switch aktiv ist und seine ISLs betriebsbereit sind. 3) Stellen Sie sicher, dass Zwischengeräte wie xWDM-Geräte betriebsbereit sind.
MetroCluster -Knoten zum Speicherstapel SAS-Verbindung unterbrochen	WARNING (Warnung)	Möglicherweise liegt ein Fehler am SAS-Adapter oder am daran angeschlossenen Kabel vor.	1. Stellen Sie sicher, dass der SAS-Adapter online und betriebsbereit ist. 2. Überprüfen Sie, ob die physische Kabelverbindung sicher und funktionsfähig ist, und ersetzen Sie das Kabel bei Bedarf. 3. Wenn der SAS-Adapter an Festplatten-Shelves angeschlossen ist, stellen Sie sicher, dass die IOMs und Festplatten richtig sitzen.
Links zum MetroClusterFC-Initiator ausgefallen	KRITISCH	Der FC-Initiatoradapter ist fehlerhaft.	1. Stellen Sie sicher, dass die FC-Initiatorverbindung nicht manipuliert wurde. 2. Überprüfen Sie den Betriebsstatus des FC-Initiatoradapters mit dem Befehl „system node run -node local -command storage show adapter“.
FC-VI-Verbindungsverbindung unterbrochen	KRITISCH	Die physische Verbindung am FC-VI-Port ist offline.	1. Stellen Sie sicher, dass die FC-VI-Verbindung nicht manipuliert wurde. 2. Überprüfen Sie mit dem Befehl „metrocluster interconnect adapter show“, ob der physische Status des FC-VI-Adapters „Aktiv“ lautet. 3. Wenn die Konfiguration Fabric-Switches umfasst, stellen Sie sicher, dass diese ordnungsgemäß verkabelt und konfiguriert sind.

Monitorname	Schwere	Monitorbeschreibung	Korrekturmaßnahme
Zurückgelassene MetroCluster -Ersatzfestplatten	WARNING (Warnung)	Die Ersatzfestplatte wurde beim Switchback zurückgelassen.	Wenn die Festplatte nicht ausgefallen ist, geben Sie sie mit dem Befehl „metrocluster switchback“ an ihren ursprünglichen Besitzer zurück.
MetroCluster Speicherbrücken-Port ausgefallen	KRITISCH	Der Port auf der Speicherbrücke ist offline.	1) Überprüfen Sie den Betriebsstatus der Ports auf der Speicherbrücke mit dem Befehl „storage bridge show -ports“. 2) Überprüfen Sie die logische und physische Konnektivität zum Port.
Lüfter des MetroCluster Speicher-Switches ausgefallen	KRITISCH	Der Lüfter am Speicherschalter ist ausgefallen.	1) Stellen Sie sicher, dass die Lüfter im Switch ordnungsgemäß funktionieren, indem Sie den Befehl „storage switch show -cooling“ verwenden. 2) Stellen Sie sicher, dass die Lüfter-FRUs richtig eingesetzt und betriebsbereit sind.
MetroCluster Speicher-Switch nicht erreichbar	KRITISCH	Der Speicher-Switch ist über das Verwaltungsnetzwerk nicht erreichbar.	1) Stellen Sie sicher, dass das Knotenverwaltungs-LIF aktiv ist, indem Sie den Befehl „Network Interface Show“ verwenden. 2) Stellen Sie mit dem Befehl „Netzwerk-Ping“ sicher, dass der Switch aktiv ist. 3) Stellen Sie sicher, dass der Switch über SNMP erreichbar ist, indem Sie nach der Anmeldung beim Switch seine SNMP-Einstellungen überprüfen.

Monitorname	Schwere	Monitorbeschreibung	Korrekturmaßnahme
Stromversorgung des MetroCluster -Switches ausgefallen	KRITISCH	Ein Netzteil am Speicherswitch ist nicht betriebsbereit.	1) Überprüfen Sie die Fehlerdetails mit dem Befehl „storage switch show -error -switch-name <switch name>“. 2) Identifizieren Sie das fehlerhafte Netzteil mit dem Befehl „storage switch show -power -switch-name <switch name>“. 3) Stellen Sie sicher, dass das Netzteil ordnungsgemäß in das Gehäuse des Speicherschalters eingesetzt und voll funktionsfähig ist.
Temperatursensoren des MetroCluster -Switches ausgefallen	KRITISCH	Der Sensor am Fibre-Channel-Switch ist ausgefallen.	1) Überprüfen Sie den Betriebszustand der Temperatursensoren am Speicherswitch mit dem Befehl „storage switch show -cooling“. 2) Stellen Sie sicher, dass der Schalter unter den empfohlenen Temperaturbedingungen arbeitet.
MetroCluster -Switch -Temperatur abnormal	KRITISCH	Der Temperatursensor am Fibre-Channel-Switch hat eine abnormale Temperatur gemeldet.	1) Überprüfen Sie den Betriebszustand der Temperatursensoren am Speicherswitch mit dem Befehl „storage switch show -cooling“. 2) Stellen Sie sicher, dass der Schalter unter den empfohlenen Temperaturbedingungen arbeitet.

Monitorname	Schwere	Monitorbeschreibung	Korrekturmaßnahme
Heartbeat des Serviceprozessors verpasst	INFORMATIONS	Diese Meldung wird angezeigt, wenn ONTAP kein erwartetes „Heartbeat“-Signal vom Serviceprozessor (SP) empfängt. Zusammen mit dieser Nachricht werden Protokolldateien vom SP zum Debuggen gesendet. ONTAP setzt den SP zurück, um zu versuchen, die Kommunikation wiederherzustellen. Während des Neustarts ist der SP bis zu zwei Minuten lang nicht verfügbar.	Wenden Sie sich an den technischen Support von NetApp .

Monitorname	Schwere	Monitorbeschreibung	Korrekturmaßnahme
Heartbeat des Serviceprozessors gestoppt	WARNING (Warnung)	Diese Meldung wird angezeigt, wenn ONTAP keine Heartbeats mehr vom Serviceprozessor (SP) empfängt. Je nach Hardwaredesign kann das System weiterhin Daten bereitstellen oder sich zum Herunterfahren entschließen, um Datenverlust oder Hardwareschäden zu verhindern. Das System stellt weiterhin Daten bereit, aber da der SP möglicherweise nicht funktioniert, kann das System keine Benachrichtigungen über ausgefallene Geräte, Startfehler oder Power-On Self-Test (POST)-Fehler der Open Firmware (OFW) senden. Wenn Ihr System entsprechend konfiguriert ist, generiert und überträgt es eine AutoSupport Nachricht (oder „Call Home“-Nachricht) an den technischen Support von NetApp und an die konfigurierten Ziele. Die erfolgreiche Übermittlung einer AutoSupport -Nachricht verbessert die Problembestimmung und -lösung erheblich.	Wenn das System heruntergefahren wurde, versuchen Sie einen Hard Power Cycle: Ziehen Sie den Controller aus dem Gehäuse, drücken Sie ihn wieder hinein und schalten Sie dann das System ein. Wenden Sie sich an den technischen Support von NetApp, wenn das Problem nach dem Aus- und Wiedereinschalten weiterhin besteht oder wenn ein anderer Zustand vorliegt, der Ihre Aufmerksamkeit erfordert.

Zurück nach oben

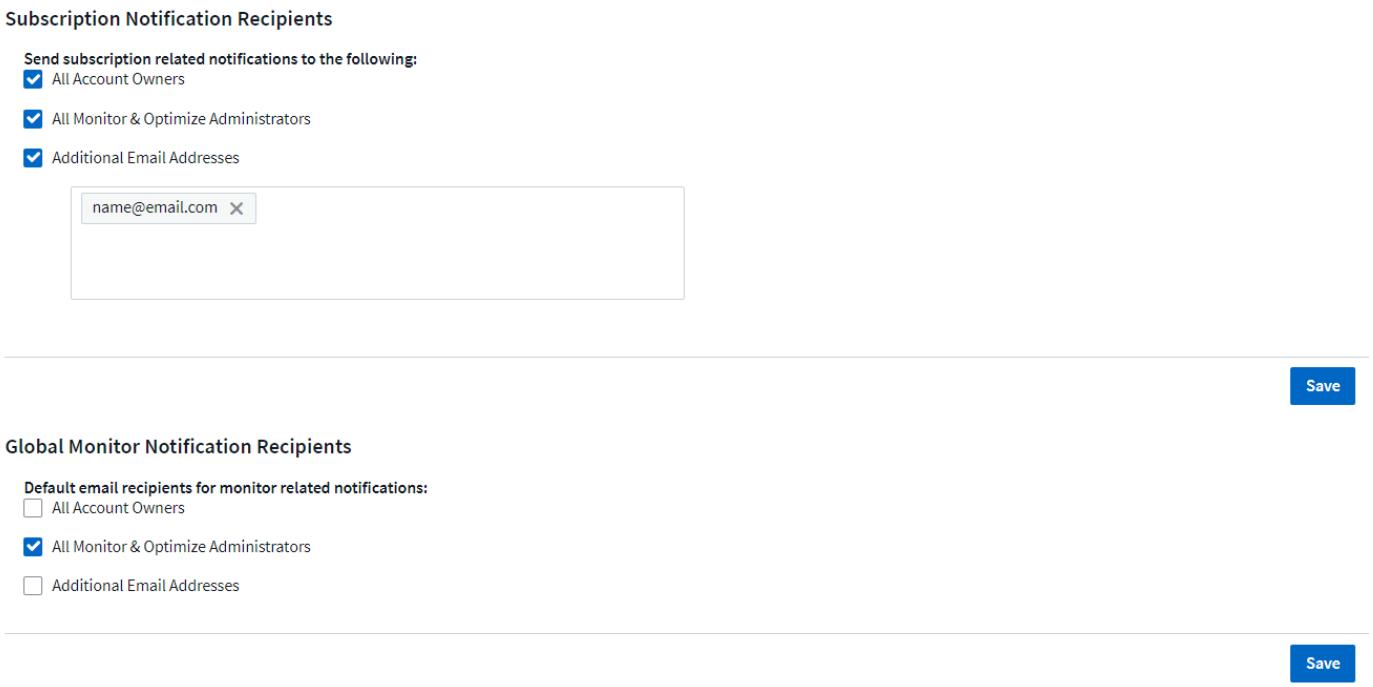
Weitere Informationen

- "Anzeigen und Verwerfen von Warnungen"

Konfigurieren von E-Mail-Benachrichtigungen

Sie können eine E-Mail-Liste für abonnementbezogene Benachrichtigungen sowie eine globale E-Mail-Liste mit Empfängern für Benachrichtigungen über Verstöße gegen Schwellenwerte der Leistungsrichtlinie konfigurieren.

Um die Einstellungen für den Empfänger von Benachrichtigungs-E-Mails zu konfigurieren, gehen Sie zur Seite **Admin > Benachrichtigungen** und wählen Sie die Registerkarte *E-Mail*.



Empfänger von Abonnementbenachrichtigungen

Um Empfänger für abonnementbezogene Ereignisbenachrichtigungen zu konfigurieren, gehen Sie zum Abschnitt „Empfänger von Abonnementbenachrichtigungen“. Sie können festlegen, dass E-Mail-Benachrichtigungen zu abonnementbezogenen Ereignissen an einen oder alle der folgenden Empfänger gesendet werden:

- Alle Kontoinhaber
- Alle *Monitor & Optimize*-Administratoren
- Zusätzliche E-Mail-Adressen, die Sie angeben

Im Folgenden finden Sie Beispiele für die Arten von Benachrichtigungen, die gesendet werden können, und für Benutzeraktionen, die Sie ausführen können.

Benachrichtigung:	**Benutzeraktion:**
Testversion oder Abonnement wurde aktualisiert	Überprüfen Sie die Abonnementdetails auf der"Abonnement" Seite
Das Abonnement läuft in 90 Tagen ab. Das Abonnement läuft in 30 Tagen ab.	Wenn „Automatische Verlängerung“ aktiviert ist, sind keine Maßnahmen erforderlich. Wenden Sie sich an den NetApp -Vertrieb, um das Abonnement zu verlängern.
Testversion endet in 2 Tagen	Testversion erneuern von"Abonnement" Seite. Sie können eine Testversion einmal verlängern. Kontaktieren Sie den NetApp -Vertrieb, um ein Abonnement zu erwerben

Testversion oder Abonnement ist abgelaufen. Das Konto wird in 48 Stunden keine Daten mehr sammeln. Das Konto wird nach 48 Stunden gelöscht.	Kontaktieren Sie den NetApp -Vertrieb, um ein Abonnement zu erwerben

Um sicherzustellen, dass Ihre Empfänger Benachrichtigungen von Data Infrastructure Insights erhalten, fügen Sie die folgenden E-Mail-Adressen zu allen Zulassungslisten hinzu:

- accounts@service.cloudinsights.netapp.com
- DoNotReply@cloudinsights.netapp.com

Globale Empfängerliste für Warnmeldungen

Für jede Aktion im Zusammenhang mit der Warnung werden E-Mail-Benachrichtigungen zu Warnungen an die Warnungsempfängerliste gesendet. Sie können Warnbenachrichtigungen an eine globale Empfängerliste senden.

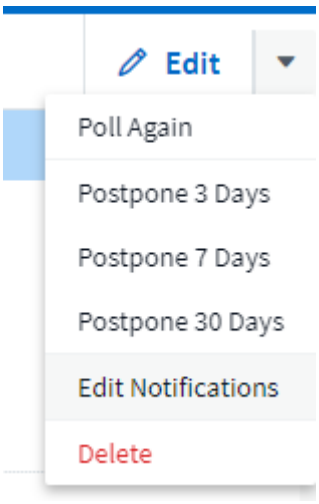
Um globale Alarmempfänger zu konfigurieren, wählen Sie die gewünschten Empfänger im Abschnitt **Globale Monitor-Benachrichtigungsempfänger** aus.

Sie können die globale Empfängerliste für einen einzelnen Monitor jederzeit überschreiben, wenn Sie den Monitor erstellen oder ändern.

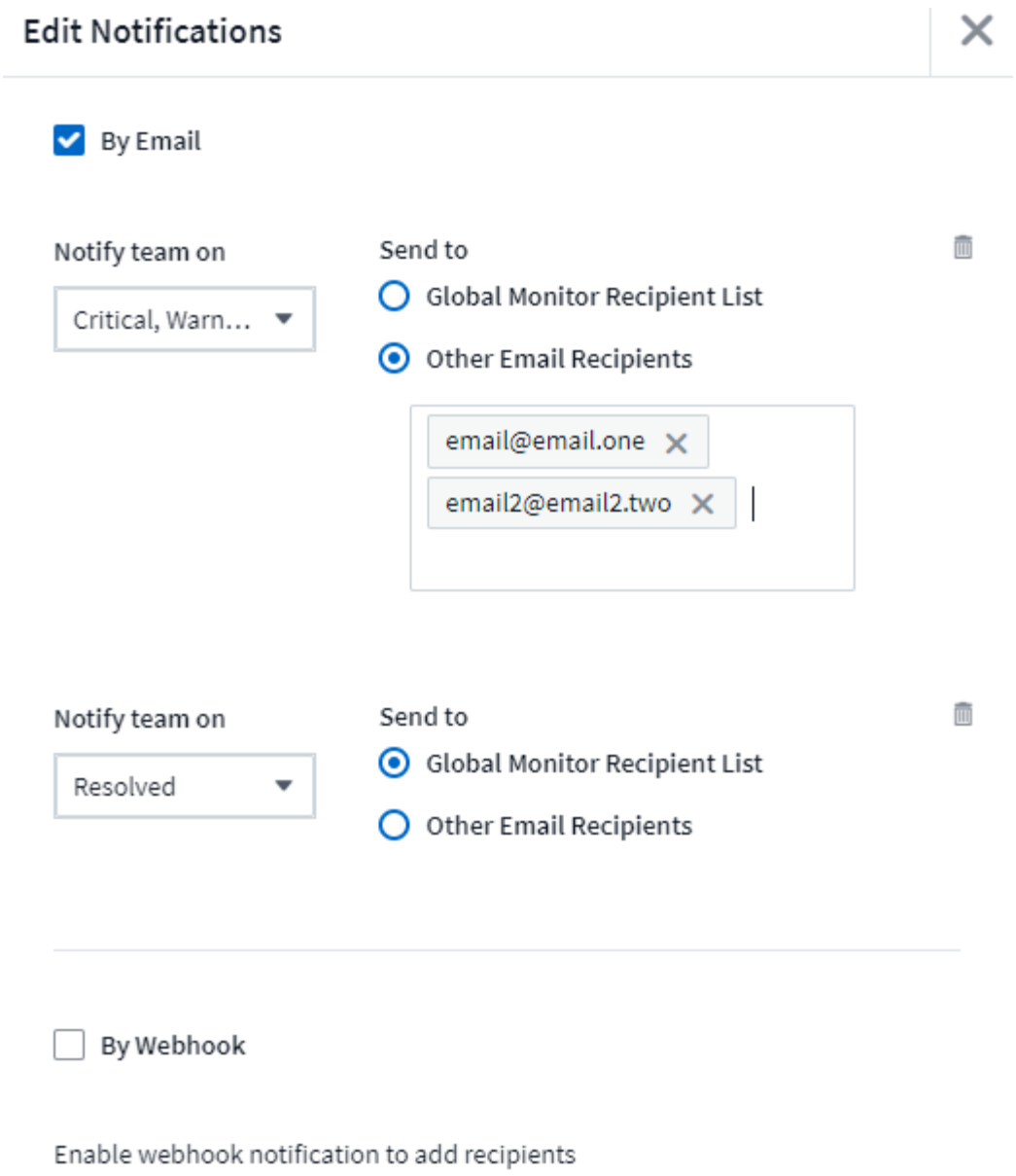
ONTAP Data Collector-Benachrichtigungen haben Vorrang vor allen spezifischen Monitor-Benachrichtigungen, die für den Cluster/Data Collector relevant sind. Die Empfängerliste, die Sie für den Datensammler selbst festlegen, erhält die Warnungen des Datensammlers. Wenn keine aktiven Datensammlerwarnungen vorliegen, werden vom Monitor generierte Warnungen an bestimmte Monitorempfänger gesendet.

Bearbeiten von Benachrichtigungen für ONTAP

Sie können Benachrichtigungen für ONTAP Cluster ändern, indem Sie auf einer Speicher-Landingpage im Dropdown-Menü oben rechts „Benachrichtigungen bearbeiten“ auswählen.



Von hier aus können Sie Benachrichtigungen für kritische, Warn-, Informations- und/oder behobene Alarme festlegen. Jedes Szenario kann die globale Empfängerliste oder andere von Ihnen ausgewählte Empfänger benachrichtigen.



Webhook-Benachrichtigungen

Benachrichtigung mittels Webhooks

Mithilfe von Webhooks können Benutzer über einen benutzerdefinierten Webhook-Kanal Warnbenachrichtigungen an verschiedene Anwendungen senden.

Viele kommerzielle Anwendungen unterstützen Webhooks als Standardeingabeschnittstelle, beispielsweise: Slack, PagerDuty, Teams und Discord unterstützen alle Webhooks. Durch die Unterstützung eines generischen, anpassbaren Webhook-Kanals kann Data Infrastructure Insights viele dieser Bereitstellungskanäle unterstützen. Informationen zu Webhooks finden Sie auf diesen Anwendungswebsites. Slack bietet beispielsweise"dieser nützliche Leitfaden" .

Sie können mehrere Webhook-Kanäle erstellen, wobei jeder Kanal einem anderen Zweck dient: separaten Anwendungen, verschiedenen Empfängern usw.

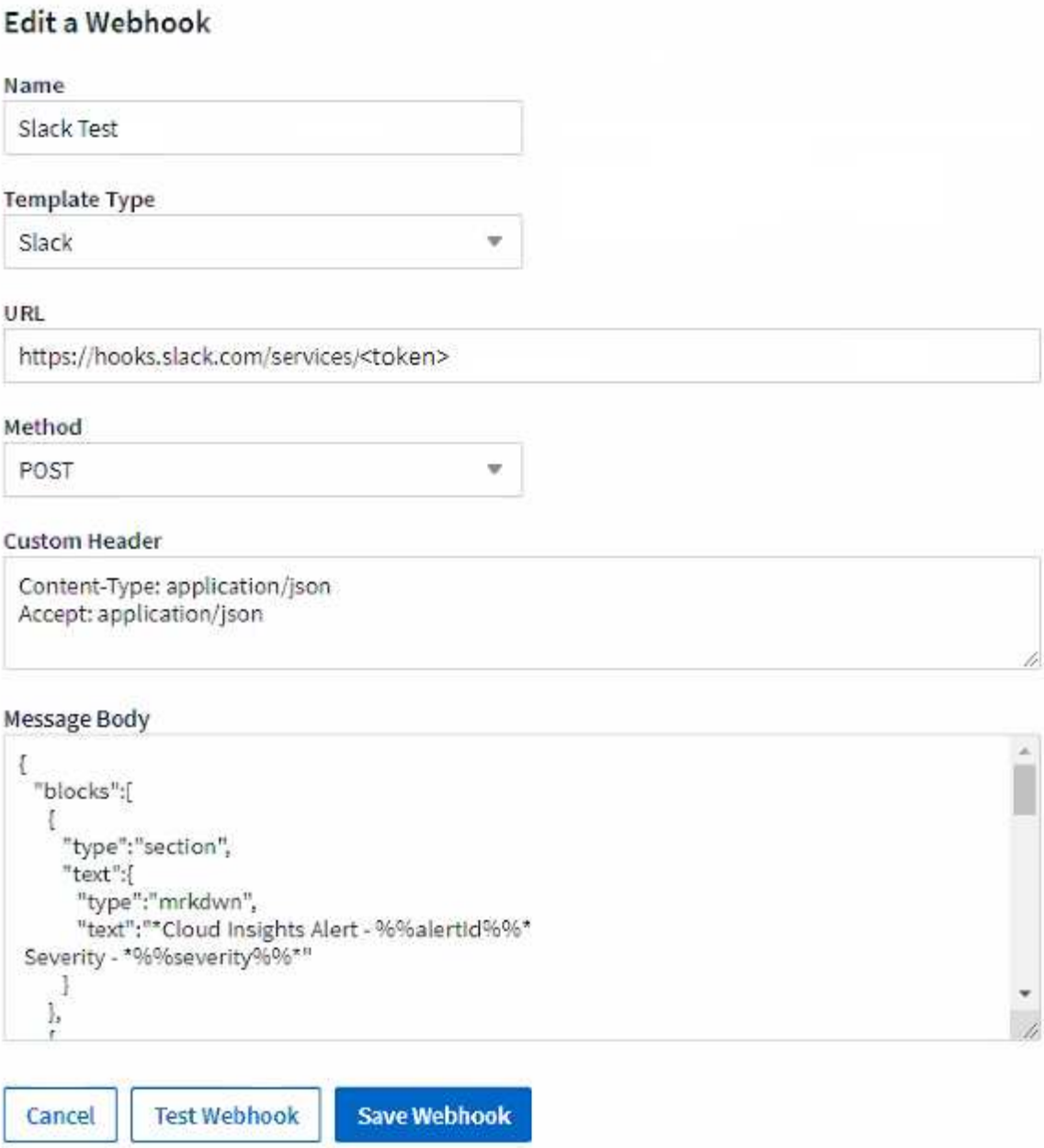
Die Webhook-Kanalinstanz besteht aus den folgenden Elementen:

Name	Eindeutiger Name
URL	Webhook-Ziel-URL, einschließlich des Präfixes *http://* oder *https://* zusammen mit den URL-Parametern
Verfahren	GET, POST – Standard ist POST
Benutzerdefinierter Header	Geben Sie hier alle benutzerdefinierten Kopfzeilen an
Nachrichtentext	Geben Sie hier den Text Ihrer Nachricht ein
Standard-Alarmparameter	Listet die Standardparameter für den Webhook auf
Benutzerdefinierte Parameter und Geheimnisse	Benutzerdefinierte Parameter und Geheimnisse ermöglichen Ihnen das Hinzufügen einzigartiger Parameter und sicherer Elemente wie Passwörter

Erstellen eines Webhooks

Um einen Data Infrastructure Insights -Webhook zu erstellen, gehen Sie zu **Admin > Benachrichtigungen** und wählen Sie die Registerkarte **Webhooks** aus.

Das folgende Bild zeigt ein Beispiel für einen für Slack konfigurierten Webhook:



Geben Sie in jedes Feld die entsprechenden Informationen ein und klicken Sie nach Abschluss auf „Speichern“.

Sie können auch auf die Schaltfläche „Webhook testen“ klicken, um die Verbindung zu testen. Beachten Sie, dass dadurch der „Nachrichtentext“ (ohne Ersetzungen) gemäß der ausgewählten Methode an die definierte URL gesendet wird.

Data Infrastructure Insights -Webhooks umfassen eine Reihe von Standardparametern. Darüber hinaus können Sie Ihre eigenen benutzerdefinierten Parameter oder Geheimnisse erstellen.

Default Alert Parameters

Name	Description
%%alertDescription%%	Alert description
%%alertId%%	Alert ID
%%alertRelativeUrl%%	Relative URL to the Alert page. To build alert link use https://%%cloudInsightsHostName%%%%alertRelativeUrl%%
%%metricName%%	Monitored metric
%%monitorName%%	Monitor name
%%objectType%%	Monitored object type
%%severity%%	Alert severity level
%%alertCondition%%	Alert condition
%%triggerTime%%	Alert trigger time in GMT ('Tue, 27 Oct 2020 01:20:30 GMT')
%%triggerTimeEpoch%%	Alert trigger time in Epoch format (milliseconds)
%%triggeredOn%%	Triggered On (key:value pairs separated by commas)
%%value%%	Metric value that triggered the alert
%%cloudInsightsLogoUrl%%	Cloud Insights logo URL
%%cloudInsightsHostname%%	Cloud Insights Hostname (concatenate with relative URL to build alert link)

Custom Parameters and Secrets

Name	Value	Description
No Data Available		

+ Parameter

Parameter: Was sind sie und wie verwende ich sie?

Alarmparameter sind dynamische Werte, die pro Alarm ausgefüllt werden. Beispielsweise wird der Parameter *%%TriggeredOn%%* durch das Objekt ersetzt, bei dem der Alarm ausgelöst wurde.

Sie können einem Webhook jedes beliebige Objektattribut (z. B. Speichername) als Parameter hinzufügen. Sie können beispielsweise Parameter für den Volumenamen und den Speichernamen in einer Webhook-Beschreibung wie folgt festlegen: „Hohe Latenz für Volume: *%%relatedObject.volume.name%%*, Speicher: *%%relatedObject.storage.name%%*“.

Beachten Sie, dass in diesem Abschnitt beim Klicken auf die Schaltfläche „Webhook testen“ *keine* Ersetzungen durchgeführt werden. Die Schaltfläche sendet eine Nutzlast, die die *%%* Ersetzungen anzeigt, sie jedoch nicht durch Daten ersetzt.

Benutzerdefinierte Parameter und Geheimnisse

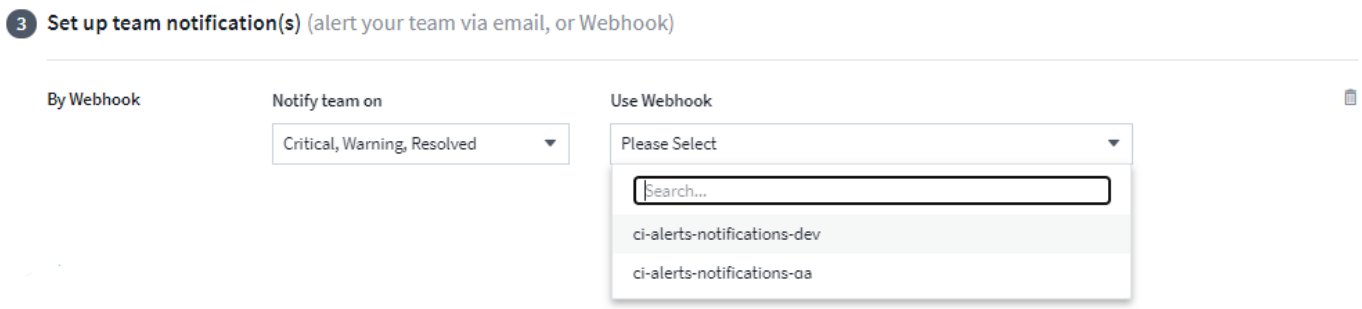
In diesem Abschnitt können Sie beliebige benutzerdefinierte Parameter und/oder Geheimnisse hinzufügen. Aus Sicherheitsgründen kann nur der Ersteller des Webhooks diesen Webhook-Kanal ändern, wenn ein Geheimnis definiert ist. Für andere ist es schreibgeschützt. Sie können Geheimnisse in URLs/Headern als *%%<secret_name>%%* verwenden.

Webhooks-Listenseite

Auf der Webhook-Listenseite werden die Felder „Name“, „Erstellt von“, „Erstellt am“, „Status“, „Sicher“ und „Zuletzt gemeldet“ angezeigt.

Auswählen einer Webhook-Benachrichtigung in einem Monitor

Um die Webhook-Benachrichtigung in einem"Monitor" , gehen Sie zu **Warnungen > Monitore verwalten** und wählen Sie den gewünschten Monitor aus oder fügen Sie einen neuen Monitor hinzu. Wählen Sie im Abschnitt „Teambenachrichtigungen einrichten“ „Webhook“ als Übermittlungsmethode. Wählen Sie die Warnstufen (Kritisch, Warnung, Gelöst) und dann den gewünschten Webhook aus.



Webhook-Beispiele:

Webhooks für"Locker" Webhooks für"PagerDuty" Webhooks für"Teams" Webhooks für"Zwietracht"

Webhook-Beispiel für Discord

Mithilfe von Webhooks können Benutzer über einen benutzerdefinierten Webhook-Kanal Warnbenachrichtigungen an verschiedene Anwendungen senden. Diese Seite bietet ein Beispiel zum Einrichten von Webhooks für Discord.

Diese Seite verweist auf Anweisungen von Drittanbietern, die Änderungen unterliegen können. Weitere Informationen finden Sie im"Discord-Dokumentation" für die aktuellsten Informationen.

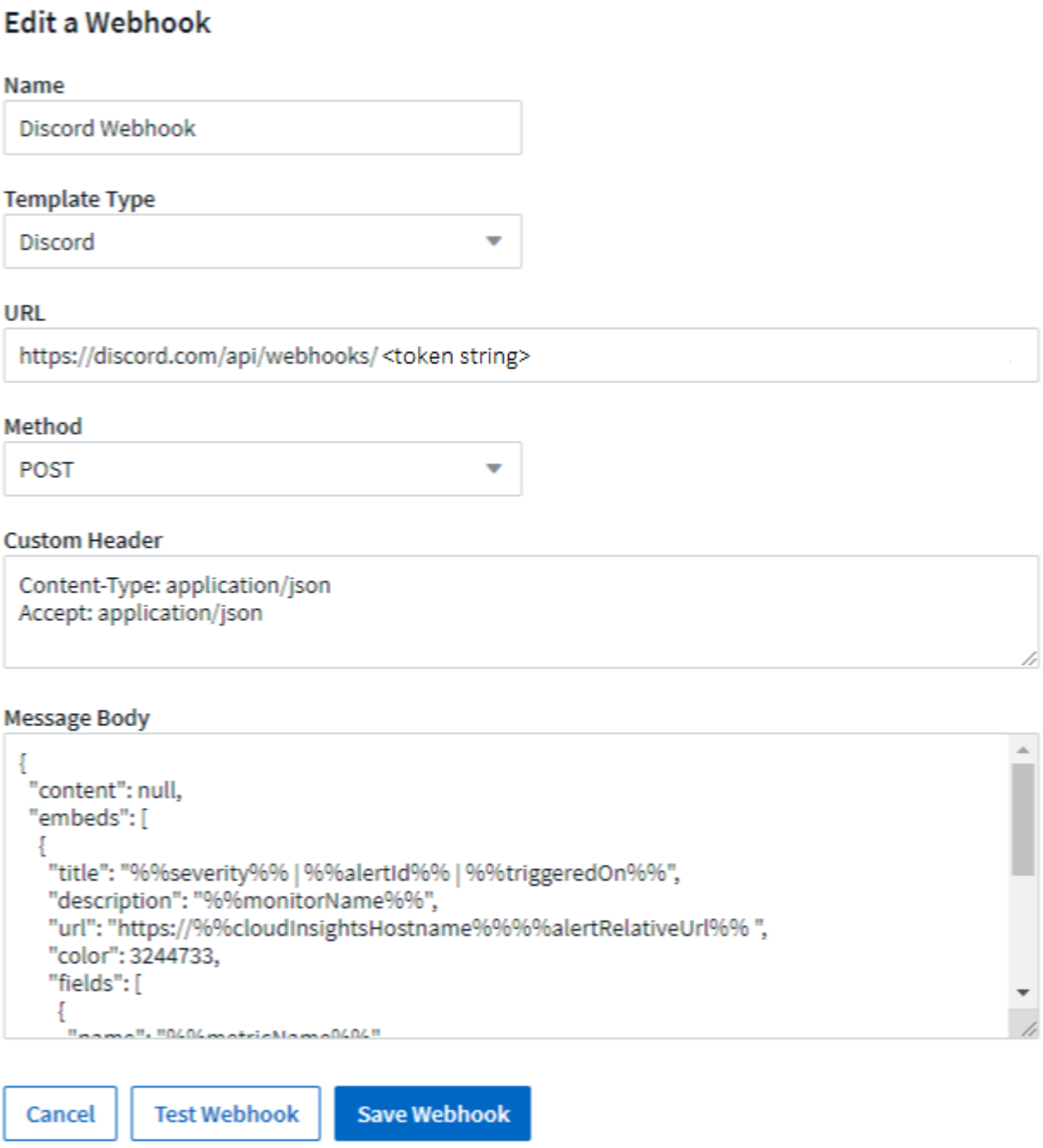
Discord-Setup:

- Wählen Sie in Discord den Server aus und wählen Sie unter „Textkanäle“ die Option „Kanal bearbeiten“ (Zahnradsymbol).
- Wählen Sie **Integrationen > Webhooks anzeigen** und klicken Sie auf **Neuer Webhook**

- Kopieren Sie die Webhook-URL. Sie müssen dies in die Webhook-Konfiguration von Data Infrastructure Insights einfügen.

Erstellen Sie einen Data Infrastructure Insights -Webhook:

1. Navigieren Sie in Data Infrastructure Insights zu **Admin > Benachrichtigungen** und wählen Sie die Registerkarte **Webhooks** aus. Klicken Sie auf **+Webhook**, um einen neuen Webhook zu erstellen.
2. Geben Sie dem Webhook einen aussagekräftigen Namen, beispielsweise „Discord“.
3. Wählen Sie im Dropdown-Menü „Vorlagentyp“ **Discord** aus.
4. Fügen Sie die URL von oben in das Feld *URL* ein.

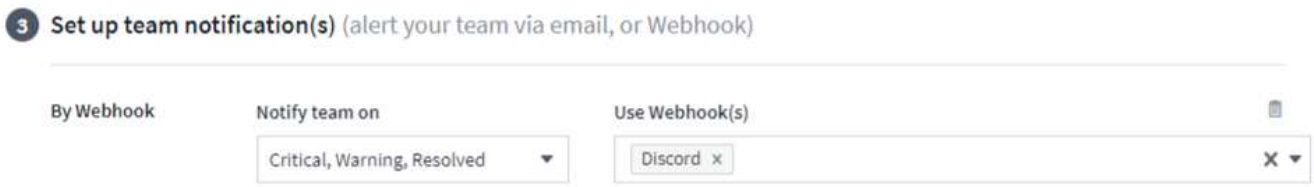


Um den Webhook zu testen, ersetzen Sie den URL-Wert im Nachrichtentext vorübergehend durch eine beliebige gültige URL (z. B. *https://netapp.com*) und klicken Sie dann auf die Schaltfläche *Webhook testen*. Denken Sie daran, den Nachrichtentext nach Abschluss des Tests wiederherzustellen.

Benachrichtigungen per Webhook

Um über Ereignisse per Webhook zu benachrichtigen, navigieren Sie in Data Infrastructure Insights zu **Alerts > Monitors** und klicken Sie auf **+Monitor**, um einen neuen"Monitor" .

- Wählen Sie eine Metrik aus und definieren Sie die Bedingungen des Monitors.
- Wählen Sie unter „Teambenachrichtigung(en) einrichten“ die Übermittlungsmethode „Webhook“ aus.
- Wählen Sie den „Discord“-Webhook für die gewünschten Ereignisse (Kritisch, Warnung, Gelöst)



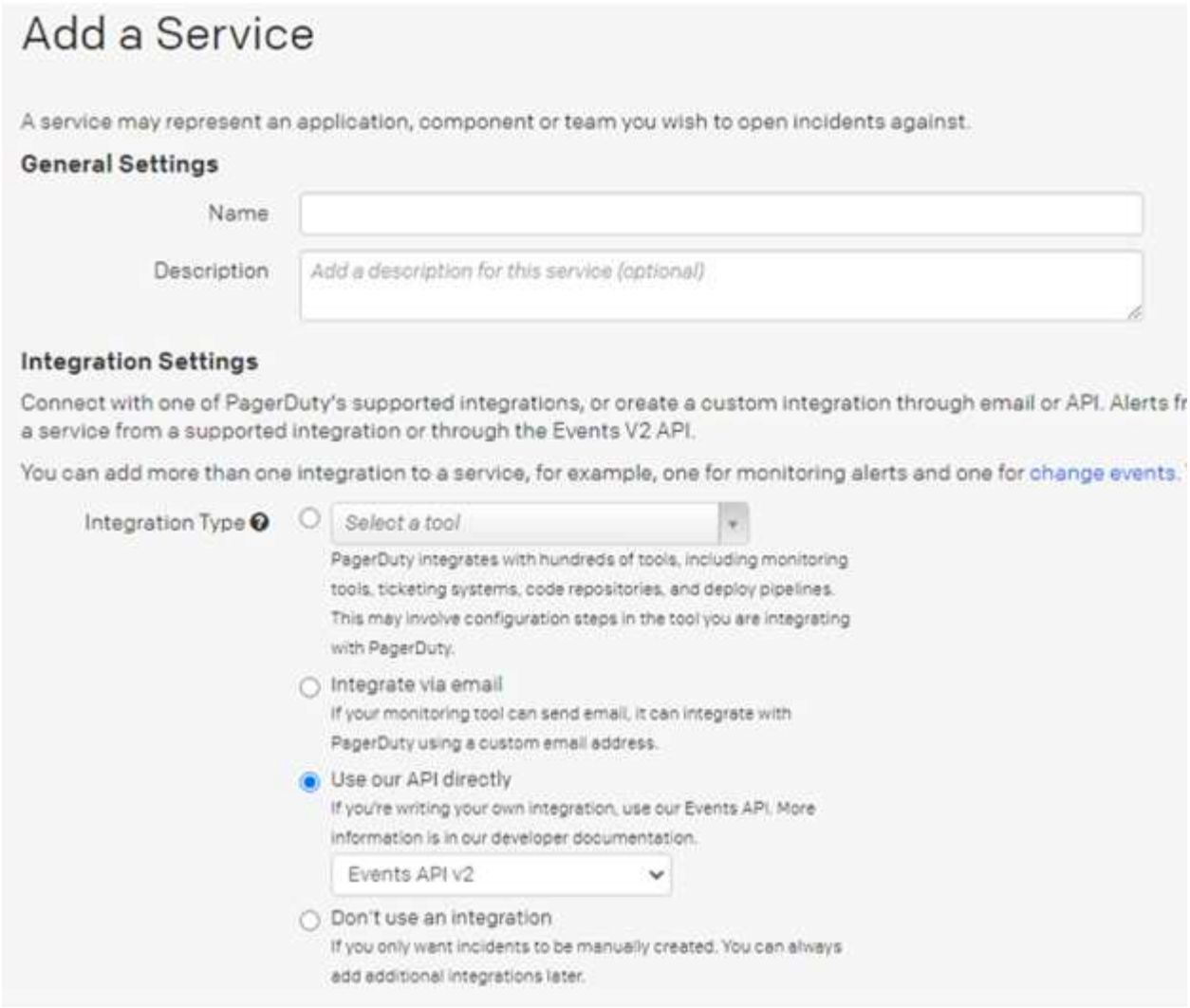
Webhook-Beispiel für PagerDuty

Mithilfe von Webhooks können Benutzer über einen benutzerdefinierten Webhook-Kanal Warnbenachrichtigungen an verschiedene Anwendungen senden. Diese Seite bietet ein Beispiel zum Einrichten von Webhooks für PagerDuty.

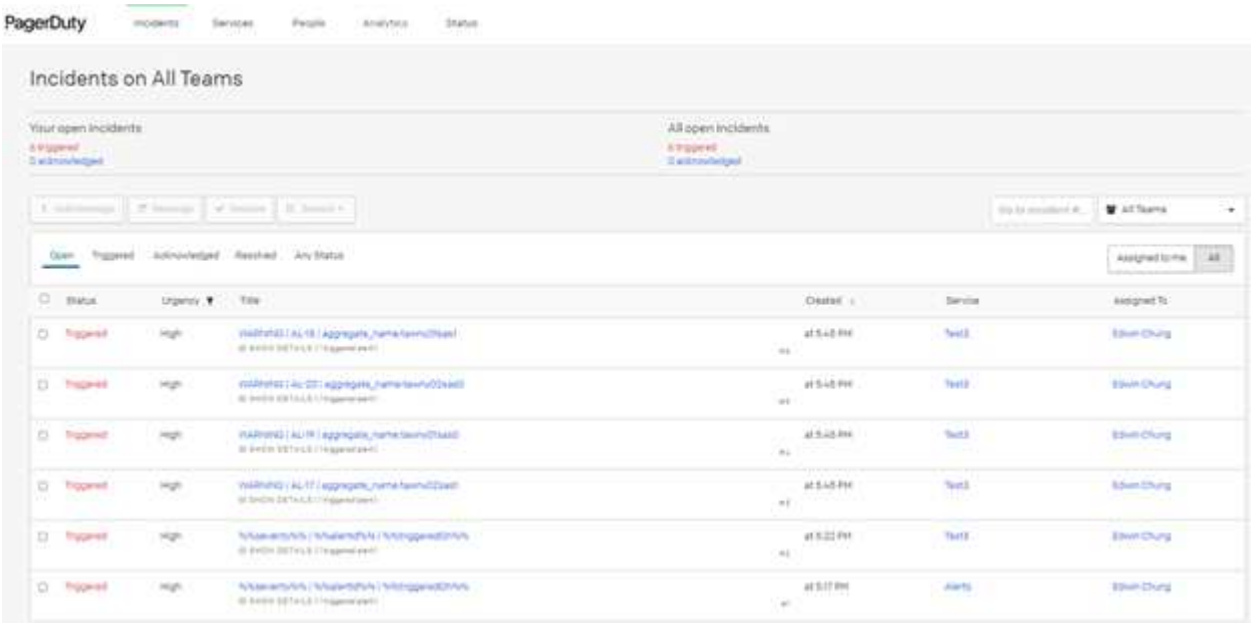
Diese Seite verweist auf Anweisungen von Drittanbietern, die Änderungen unterliegen können. Weitere Informationen finden Sie im"PagerDuty-Dokumentation" für die aktuellsten Informationen.

PagerDuty-Setup:

1. Navigieren Sie in PagerDuty zu **Dienste > Dienstverzeichnis** und klicken Sie auf die Schaltfläche **+Neuer Dienst**
2. Geben Sie einen *Namen* ein und wählen Sie *Unsere API direkt verwenden*. Klicken Sie auf *Dienst hinzufügen*.

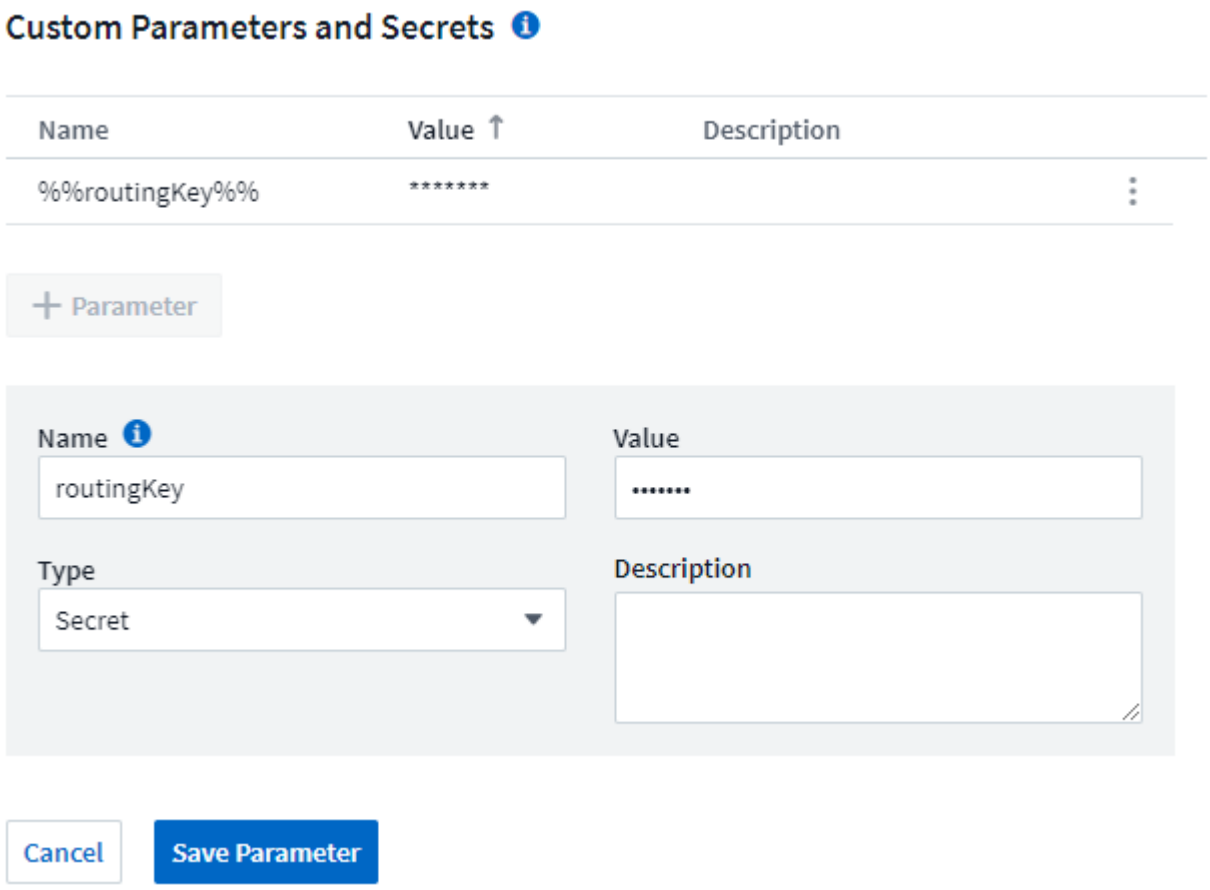


3. Klicken Sie auf die Registerkarte *Integrationen*, um den **Integrationsschlüssel** anzuzeigen. Sie benötigen diesen Schlüssel, wenn Sie unten den Data Infrastructure Insights -Webhook erstellen.
4. Gehen Sie zu **Vorfälle** oder **Dienste**, um Warnungen anzuzeigen.



Erstellen Sie einen Data Infrastructure Insights -Webhook:

1. Navigieren Sie in Data Infrastructure Insights zu **Admin > Benachrichtigungen** und wählen Sie die Registerkarte **Webhooks** aus. Klicken Sie auf **+Webhook**, um einen neuen Webhook zu erstellen.
2. Geben Sie dem Webhook einen aussagekräftigen Namen, beispielsweise „PagerDuty Trigger“. Sie verwenden diesen Webhook für Ereignisse der Stufen „kritisch“ und „Warnung“.
3. Wählen Sie im Dropdown-Menü „Vorlagentyp“ die Option „PagerDuty“ aus.
4. Erstellen Sie ein benutzerdefiniertes Parametergeheimnis mit dem Namen *routingKey* und legen Sie den Wert auf den PagerDuty-*Integrationsschlüssel*-Wert von oben fest.



Wiederholen Sie diese Schritte, um einen „PagerDuty Resolve“-Webhook für gelöste Ereignisse zu erstellen.

PagerDuty zur Data Infrastructure Insights -Feldzuordnung

Die folgende Tabelle und das Bild zeigen die Zuordnung der Felder zwischen PagerDuty und Data Infrastructure Insights:

PagerDuty	Data Infrastructure Insights
Alarmschlüssel	Warnmeldungs-ID
Quelle	Ausgelöst am
Komponente	Metrikname
Gruppe	Objekttyp

PagerDuty	Data Infrastructure Insights
Klasse	Monitorname

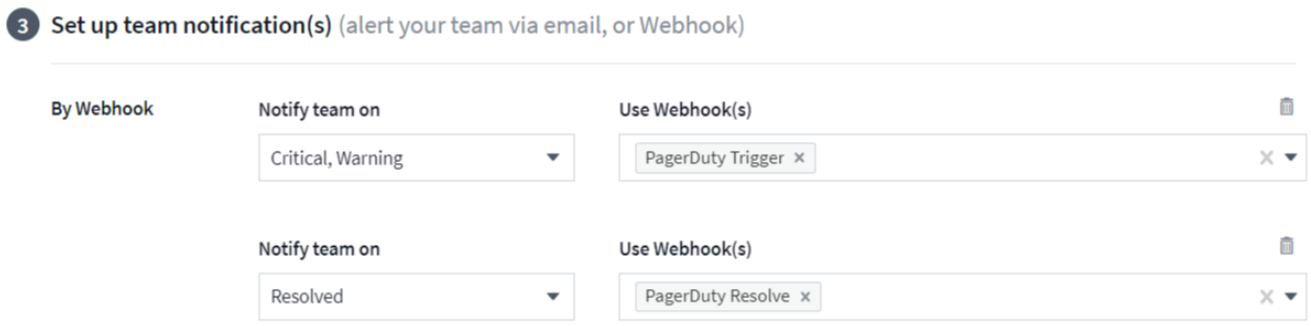
Message Body

```
{
 "dedup_key": "%%alertId%%",
 "event_action": "trigger",
 "links": [
  {
   "href": "https://%%cloudInsightsHostname%%%%alertRelativeUrl%%",
   "text": "'%%metricName%%' value of %%value%% (%%alertCondition%%) for
%%triggeredOn%%"
  }
 ],
 "payload": {
  "class": "%%monitorName%%",
  "component": "%%metricName%%",
  "group": "%%objectType%%",
  "severity": "critical",
  "source": "%%triggeredOn%%",
  "summary": "%%severity%% | %%alertId%% | %%triggeredOn%%"
 },
 "routing_key": "%%routingKey%%"
}
```

Benachrichtigungen per Webhook

Um über Ereignisse per Webhook zu benachrichtigen, navigieren Sie in Data Infrastructure Insights zu **Alerts > Monitors** und klicken Sie auf **+Monitor**, um einen neuen"Monitor" .

- Wählen Sie eine Metrik aus und definieren Sie die Bedingungen des Monitors.
- Wählen Sie unter „Teambenachrichtigung(en) einrichten“ die Übermittlungsmethode „Webhook“ aus.
- Wählen Sie den Webhook „PagerDuty Trigger“ für Ereignisse der Stufen „Kritisch“ und „Warnung“.
- Wählen Sie „PagerDuty Resolve“ für gelöste Ereignisse.



Das Festlegen separater Benachrichtigungen für Trigger-Ereignisse im Vergleich zu aufgelösten Ereignissen ist eine bewährte Methode, da PagerDuty Trigger-Ereignisse anders behandelt als aufgelöste Ereignisse.

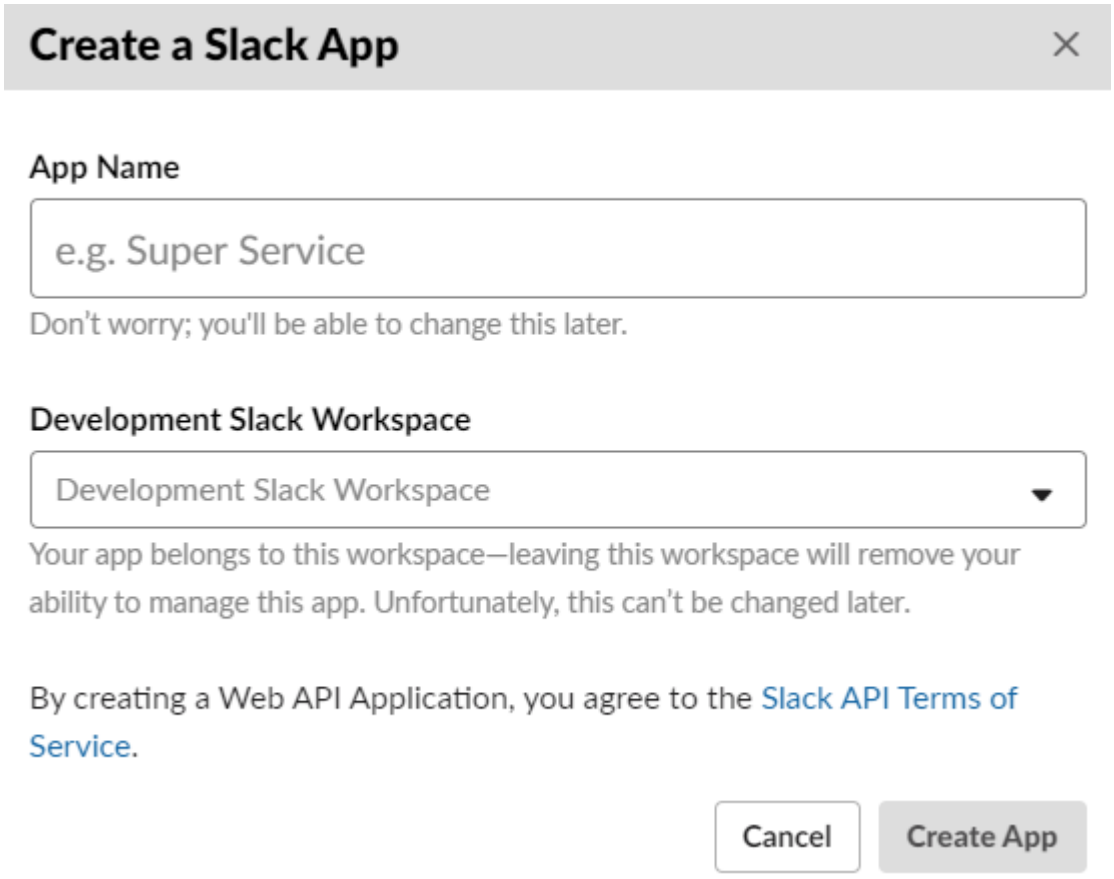
Webhook-Beispiel für Slack

Mithilfe von Webhooks können Benutzer über einen benutzerdefinierten Webhook-Kanal Warnbenachrichtigungen an verschiedene Anwendungen senden. Diese Seite bietet ein Beispiel zum Einrichten von Webhooks für Slack.

Diese Seite verweist auf Anweisungen von Drittanbietern, die Änderungen unterliegen können. Weitere Informationen finden Sie im"Slack-Dokumentation" für die aktuellsten Informationen.

Slack-Beispiel:

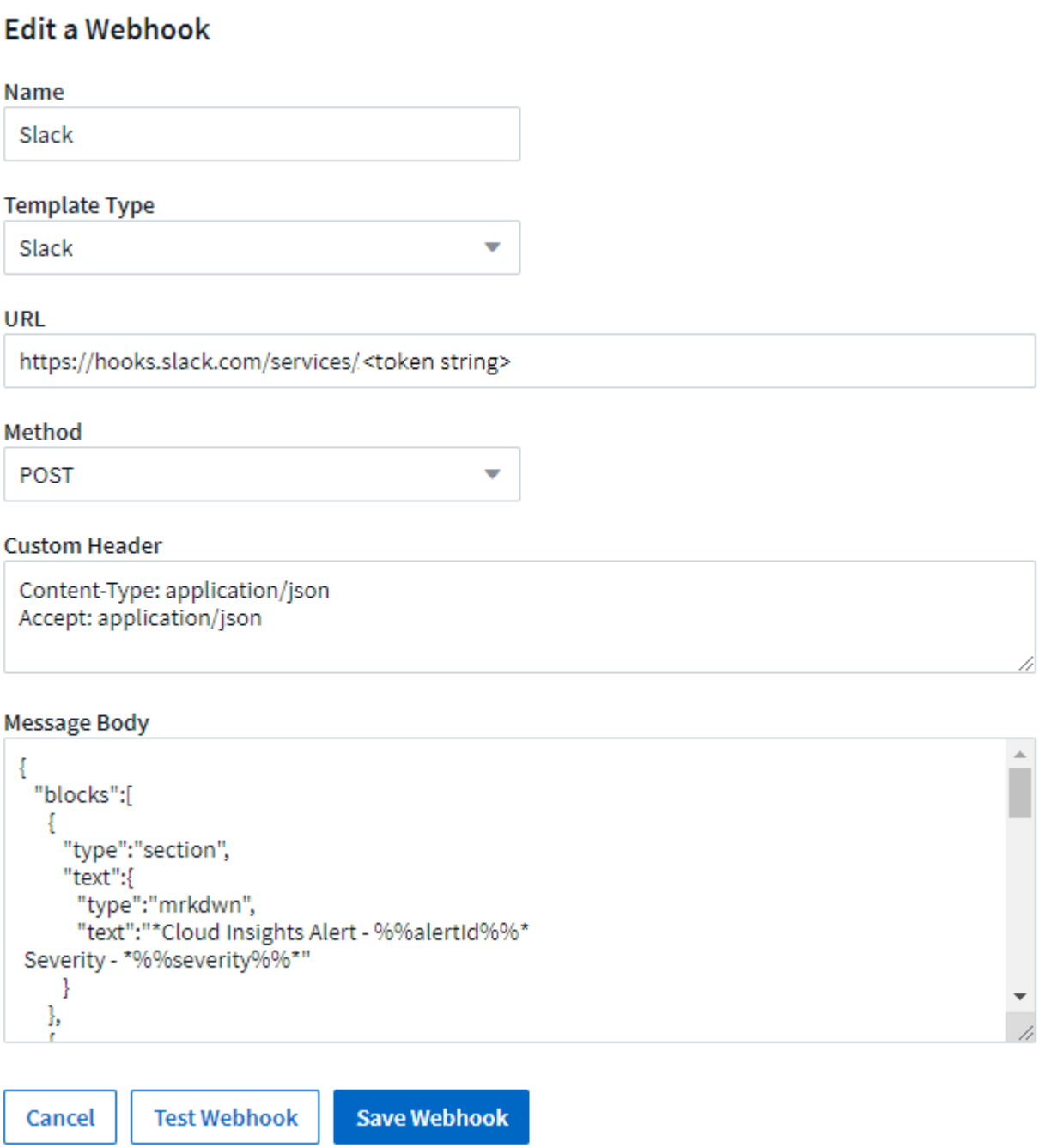
- Gehe zu https://api.slack.com/apps und erstellen Sie eine neue App. Geben Sie ihm einen aussagekräftigen Namen und wählen Sie den Slack-Arbeitsbereich aus.



- Gehen Sie zu „Eingehende Webhooks“, klicken Sie auf „Eingehende Webhooks aktivieren“, „Anforderung zum Hinzufügen eines neuen Webhooks“ und wählen Sie den Kanal aus, auf dem gepostet werden soll.
- Kopieren Sie die Webhook-URL. Sie müssen dies in die Webhook-Konfiguration von Data Infrastructure Insights einfügen.

Erstellen Sie einen Data Infrastructure Insights -Webhook:

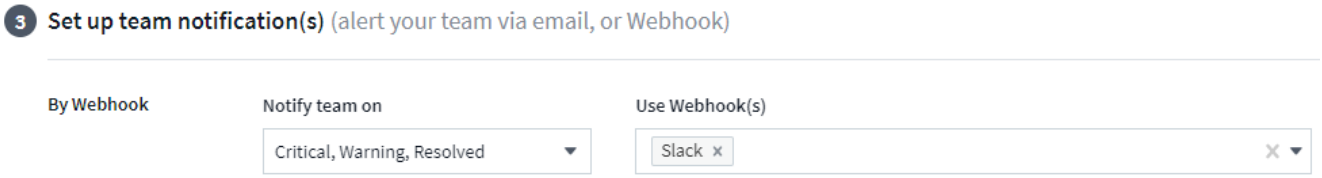
1. Navigieren Sie in Data Infrastructure Insights zu **Admin > Benachrichtigungen** und wählen Sie die Registerkarte **Webhooks** aus. Klicken Sie auf **+Webhook**, um einen neuen Webhook zu erstellen.
2. Geben Sie dem Webhook einen aussagekräftigen Namen, beispielsweise „Slack Webhook“.
3. Wählen Sie im Dropdown-Menü „Vorlagentyp“ **Slack** aus.
4. Fügen Sie die URL von oben in das Feld *URL* ein.



Benachrichtigungen per Webhook

Um über Ereignisse per Webhook zu benachrichtigen, navigieren Sie in Data Infrastructure Insights zu **Alerts > Monitors** und klicken Sie auf **+Monitor**, um einen neuen"Monitor" .

- Wählen Sie eine Metrik aus und definieren Sie die Bedingungen des Monitors.
- Wählen Sie unter „Teambenachrichtigung(en) einrichten“ die Übermittlungsmethode „Webhook“ aus.
- Wählen Sie den „Slack“-Webhook für die gewünschten Ereignisse (Kritisch, Warnung, Gelöst)



Weitere Informationen:

- Informationen zum Ändern des Nachrichtenformats und -layouts finden Sie unter https://api.slack.com/messaging/composing
- Fehlerbehandlung: https://api.slack.com/messaging/webhooks#handling_errors

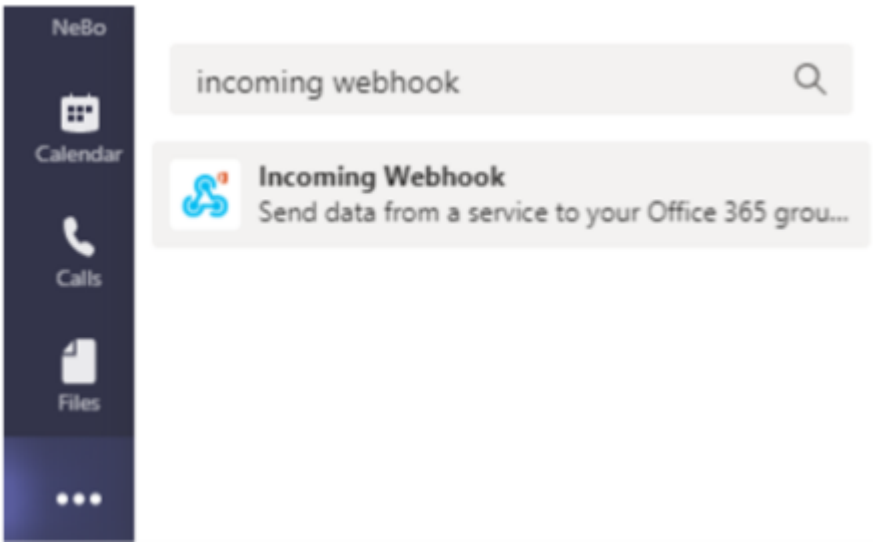
Webhook-Beispiel für Microsoft Teams

Mithilfe von Webhooks können Benutzer über einen benutzerdefinierten Webhook-Kanal Warnbenachrichtigungen an verschiedene Anwendungen senden. Diese Seite bietet ein Beispiel zum Einrichten von Webhooks für Teams.

Diese Seite verweist auf Anweisungen von Drittanbietern, die Änderungen unterliegen können. Weitere Informationen finden Sie im"Teams-Dokumentation" für die aktuellsten Informationen.

Teams-Setup:

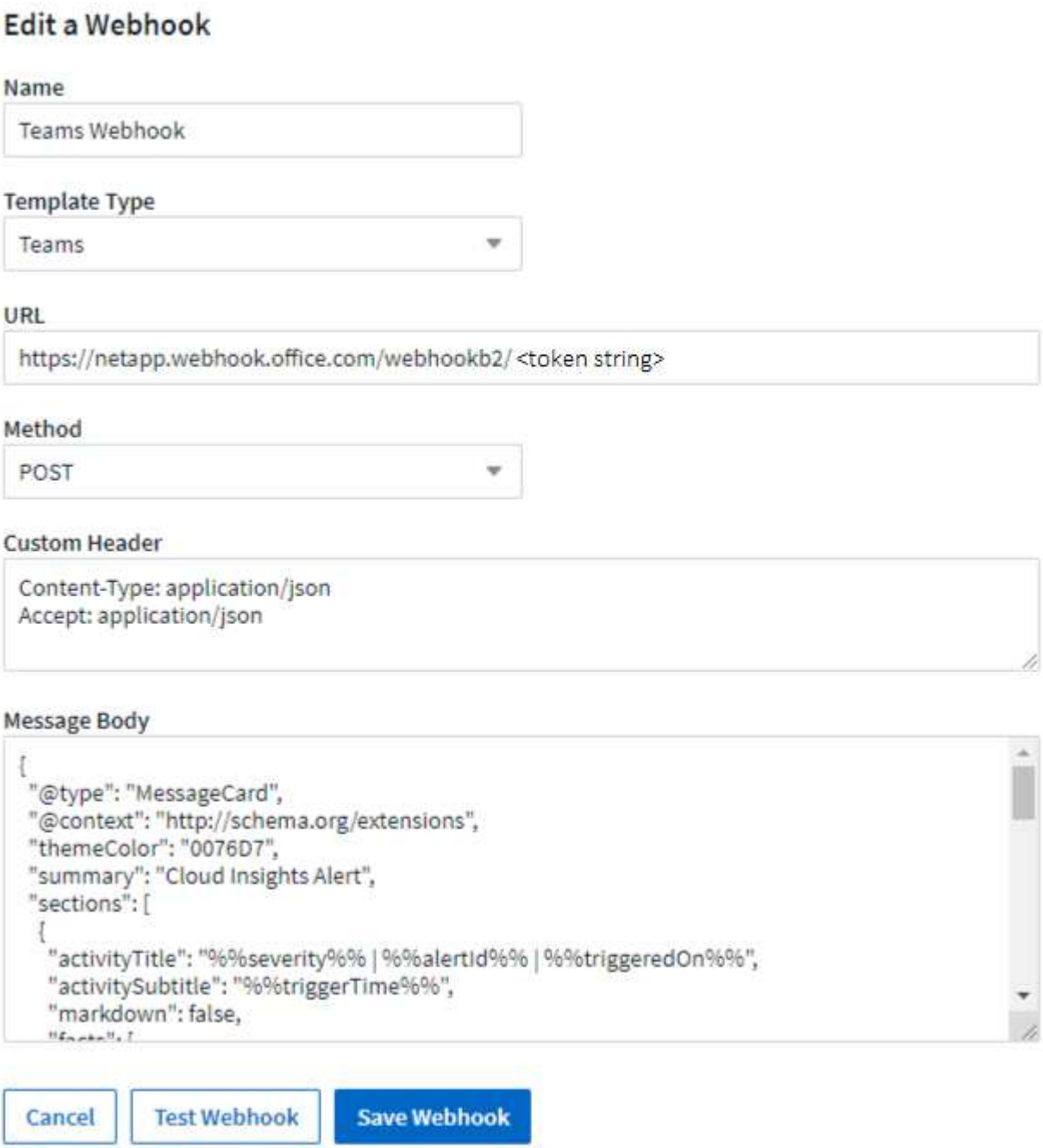
1. Wählen Sie in Teams den Kebab aus und suchen Sie nach „Eingehender Webhook“.



2. Wählen Sie **Zu einem Team hinzufügen > Ein Team auswählen > Einen Connector einrichten**.
3. Kopieren Sie die Webhook-URL. Sie müssen dies in die Webhook-Konfiguration von Data Infrastructure Insights einfügen.

Erstellen Sie einen Data Infrastructure Insights -Webhook:

1. Navigieren Sie in Data Infrastructure Insights zu **Admin > Benachrichtigungen** und wählen Sie die Registerkarte **Webhooks** aus. Klicken Sie auf **+Webhook**, um einen neuen Webhook zu erstellen.
2. Geben Sie dem Webhook einen aussagekräftigen Namen, beispielsweise „Teams Webhook“.
3. Wählen Sie im Dropdown-Menü „Vorlagentyp“ die Option „Teams“ aus.

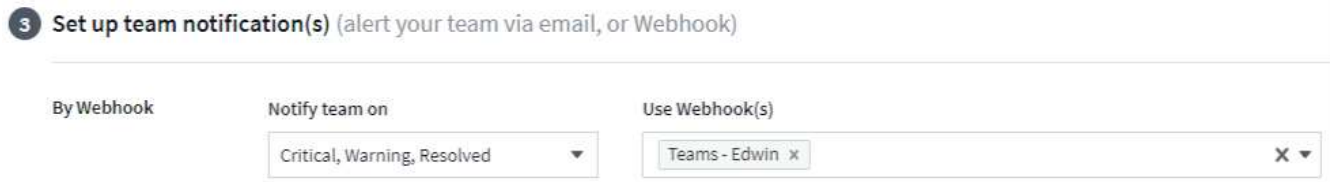


1. Fügen Sie die URL von oben in das Feld *URL* ein.

Benachrichtigungen per Webhook

Um über Ereignisse per Webhook zu benachrichtigen, navigieren Sie in Data Infrastructure Insights zu **Alerts > Monitors** und klicken Sie auf **+Monitor**, um einen neuen"Monitor" .

- Wählen Sie eine Metrik aus und definieren Sie die Bedingungen des Monitors.
- Wählen Sie unter „Teambenachrichtigung(en) einrichten“ die Übermittlungsmethode „Webhook“ aus.
- Wählen Sie den „Teams“-Webhook für die gewünschten Ereignisse (Kritisch, Warnung, Gelöst)



Arbeiten mit Anmerkungen

Anmerkungen definieren

Wenn Sie Data Infrastructure Insights anpassen, um Daten für Ihre Unternehmensanforderungen zu verfolgen, können Sie spezielle Notizen, sogenannte Anmerkungen, definieren und sie Ihren Assets zuweisen.

Sie können Assets Anmerkungen mit Informationen wie dem Ende der Lebensdauer des Assets, dem Rechenzentrum, dem Gebäudestandort, der Speicherebene oder dem Volume-Servicelevel zuweisen.

Die Verwendung von Anmerkungen zur Überwachung Ihrer Umgebung umfasst die folgenden übergeordneten Aufgaben:

- Erstellen oder Bearbeiten von Definitionen für alle Anmerkungstypen.
- Anzeigen von Asset-Seiten und Zuordnen jedes Assets zu einer oder mehreren Anmerkungen.

  Wenn beispielsweise ein Vermögenswert geleast wird und der Leasingvertrag innerhalb von zwei Monaten abläuft, möchten Sie dem Vermögenswert möglicherweise eine End-of-Life-Anmerkung hinzufügen. Dadurch wird verhindert, dass andere dieses Gut über einen längeren Zeitraum hinweg verwenden.

- Erstellen von Regeln zum automatischen Anwenden von Anmerkungen auf mehrere Assets desselben Typs.
- Filtern Sie Assets nach ihren Anmerkungen.

Standard-Annotationstypen

Data Infrastructure Insights bietet einige Standardanmerkungstypen. Diese Anmerkungen können zum Filtern oder Gruppieren von Daten verwendet werden.

Sie können Assets mit Standardanmerkungstypen wie den folgenden verknüpfen:

- Lebenszyklus von Anlagen, z. B. Geburtstag, Sonnenuntergang oder Ende der Lebensdauer
- Standortinformationen zu einem Gerät, z. B. Rechenzentrum, Gebäude oder Stockwerk
- Klassifizierung von Assets, beispielsweise nach Qualität (Tiers), nach angeschlossenen Geräten (Switch-Level) oder nach Service-Level
- Status, z. B. „heiß“ (hohe Auslastung)

In der folgenden Tabelle sind die von Data Infrastructure Insights bereitgestellten Anmerkungstypen aufgeführt.

Anmerkungstypen	Beschreibung	Typ
Alias	Benutzerfreundlicher Name für eine Ressource	Text
Compute-Ressourcengruppe	Vom Host- und VM-Dateisystem-Datensammler verwendete Gruppenzuweisung	Liste
Rechenzentrum	Physischer Standort	Liste
Heiß	Geräte, die regelmäßig stark beansprucht werden oder an der Grenze ihrer Kapazität stehen	Boolescher Wert
Hinweis	Mit einer Ressource verknüpfte Kommentare	Prüfen
Service-Level	Eine Reihe unterstützter Servicelevel, die Sie Ressourcen zuweisen können. Bietet eine geordnete Optionsliste für interne Volumes, Qtree und Volumes. Bearbeiten Sie Service-Levels, um Leistungsrichtlinien für verschiedene Level festzulegen.	Liste
Sonnenuntergang	Festgelegter Schwellenwert, nach dessen Überschreitung keine neuen Zuweisungen mehr zu diesem Gerät vorgenommen werden können. Nützlich für geplante Migrationen und andere anstehende Netzwerkänderungen.	Datum
Schalterebene	Vordefinierte Optionen zum Einrichten von Kategorien für Schalter. Normalerweise bleiben diese Bezeichnungen für die gesamte Lebensdauer des Geräts bestehen, Sie können sie jedoch bearbeiten. Nur für Schalter verfügbar.	Liste
Stufe	Kann verwendet werden, um verschiedene Serviceebenen innerhalb Ihrer Umgebung zu definieren. Mit den Stufen kann die Art des Levels definiert werden, beispielsweise die erforderliche Geschwindigkeit (z. B. Gold oder Silber). Diese Funktion ist nur auf internen Volumes, Qtrees, Speicher-Arrays, Speicherpools und Volumes verfügbar.	Liste
Schweregrad des Verstoßes	Rang (z. B. schwerwiegend) eines Verstoßes (z. B. fehlende Host-Ports oder fehlende Redundanz) in einer Hierarchie von der höchsten bis zur niedrigsten Wichtigkeit.	Liste

Alias, Data Center, Hot, Service Level, Sunset, Switch Level, Tier und Violation Severity sind Anmerkungen auf Systemebene, die Sie nicht löschen oder umbenennen können. Sie können nur die ihnen zugewiesenen Werte ändern.

Erstellen benutzerdefinierter Anmerkungen

Mithilfe von Anmerkungen können Sie den Assets benutzerdefinierte, geschäftsspezifische Daten hinzufügen, die Ihren Geschäftsanforderungen entsprechen. Obwohl Data Infrastructure Insights eine Reihe von Standardanmerkungen bereitstellt, möchten Sie die Daten möglicherweise auf andere Weise anzeigen. Die Daten in benutzerdefinierten Anmerkungen ergänzen bereits erfasste Gerätedaten, wie etwa Speicherhersteller, Anzahl der Datenträger und Leistungsstatistiken. Die Daten, die Sie mithilfe von Anmerkungen hinzufügen, werden von Data Infrastructure Insights nicht erkannt.

Schritte

1. Klicken Sie im Data Infrastructure Insights -Menü auf **Verwalten > Anmerkungen**.

   Auf der Seite „Anmerkungen“ wird die Liste der Anmerkungen angezeigt.

2. Klicken Sie auf **+Hinzufügen**
3. Geben Sie einen **Namen** und eine **Beschreibung** der Anmerkung ein.

   Sie können in diese Felder bis zu 255 Zeichen eingeben.

4. Klicken Sie auf **Typ** und wählen Sie dann eine der folgenden Optionen aus, die den in dieser Anmerkung zulässigen Datentyp darstellt:

Anmerkungstypen

- Boolesch: Erstellt eine Dropdownliste mit den Auswahlmöglichkeiten „Ja“ und „Nein“. Beispielsweise ist die Anmerkung „Direkt verbunden“ boolesch.
- Datum: Dadurch wird ein Feld erstellt, das ein Datum enthält. Wenn die Anmerkung beispielsweise ein Datum sein soll, wählen Sie dies aus.
- Liste: Erstellt eines der folgenden Elemente:
  - Eine Dropdown-Liste mit festen

    Wenn andere diesen Anmerkungstyp einem Gerät zuweisen, können sie der Liste keine weiteren Werte hinzufügen.

  - Eine flexible Dropdown-Liste

    Wenn Sie beim Erstellen dieser Liste die Option „Neue Werte spontan hinzufügen“ auswählen, können andere Personen, die diesen Anmerkungstyp einem Gerät zuweisen, der Liste weitere Werte hinzufügen.

- Nummer: Erstellt ein Feld, in das der Benutzer, der die Anmerkung zuweist, eine Nummer eingeben kann. Wenn der Anmerkungstyp beispielsweise „Etage“ ist, kann der Benutzer den Werttyp „Nummer“ auswählen und die Etagennummer eingeben.
- Text: Erstellt ein Feld, das Freitext zulässt. Sie können beispielsweise „Sprache“ als Anmerkungstyp eingeben, „Text“ als Werttyp auswählen und eine Sprache als Wert eingeben.

Nachdem Sie den Typ festgelegt und Ihre Änderungen gespeichert haben, können Sie den Typ der Anmerkung nicht mehr ändern. Wenn Sie den Typ ändern müssen, müssen Sie die Anmerkung löschen und eine neue erstellen.

1. Wenn Sie „Liste“ als Anmerkungstyp auswählen, gehen Sie wie folgt vor:
   a. Wählen Sie **Neue Werte spontan hinzufügen**, wenn Sie der Anmerkung auf einer Asset-Seite weitere Werte hinzufügen möchten, wodurch eine flexible Liste erstellt wird.

      Angenommen, Sie befinden sich auf einer Asset-Seite und das Asset verfügt über die Stadtanmerkung mit den Werten Detroit, Tampa und Boston. Wenn Sie die Option **Neue Werte spontan hinzufügen** ausgewählt haben, können Sie der Stadt zusätzliche Werte wie San Francisco und Chicago direkt auf der Asset-Seite hinzufügen, anstatt sie auf der Anmerkungsseite hinzufügen zu müssen. Wenn Sie diese Option nicht wählen, können Sie beim Anwenden der Annotation keine neuen Annotationswerte hinzufügen. Dadurch wird eine feste Liste erstellt.

b. Geben Sie in die Felder **Wert** und **Beschreibung** einen Wert und eine Beschreibung ein.

c. Klicken Sie auf **Hinzufügen**, um weitere Werte hinzuzufügen.

d. Klicken Sie auf das Papierkorbsymbol, um einen Wert zu löschen.

2. Klicken Sie auf **Speichern**

   Ihre Anmerkungen werden in der Liste auf der Anmerkungsseite angezeigt.

Ein Hinweis zu Booleschen Anmerkungen

Beim Filtern nach einer Booleschen Anmerkung werden Ihnen möglicherweise die folgenden Werte zum Filtern angezeigt:

- **Beliebig**: Dies gibt *alle* Ergebnisse zurück, einschließlich der Ergebnisse, die auf „Ja“, „Nein“ oder gar nicht festgelegt sind.
- **Ja**: Gibt nur „Ja“-Ergebnisse zurück. Beachten Sie, dass DII in den meisten Tabellen „Ja“ als Häkchen anzeigt. Die Werte können auf „True“, „On“ usw. gesetzt werden; DII behandelt alle diese Werte als „Yes“.
- **Nein**: Gibt nur „Nein“-Ergebnisse zurück. Beachten Sie, dass DII in den meisten Tabellen „Nein“ als „X“ anzeigt. Die Werte können auf „Falsch“, „Aus“ usw. gesetzt werden; DII behandelt alle diese Werte als „Nein“.
- **Keine**: Gibt nur Ergebnisse zurück, bei denen die Anmerkung überhaupt nicht festgelegt wurde. Auch als „Null“-Werte bezeichnet.

Nach Abschluss

In der Benutzeroberfläche steht die Anmerkung sofort zur Verwendung bereit.

Verwenden von Anmerkungen

Sie erstellen Anmerkungen und weisen sie den von Ihnen überwachten Assets zu. Anmerkungen sind Hinweise, die Informationen zu einem Asset liefern, beispielsweise den physischen Standort, das Ende der Lebensdauer, die Speicherebene oder die Volumen-Servicelevel.

Anmerkungen definieren

Mithilfe von Anmerkungen können Sie den Assets benutzerdefinierte, geschäftsspezifische Daten hinzufügen, die Ihren Geschäftsanforderungen entsprechen. Obwohl Data Infrastructure Insights eine Reihe von Standardanmerkungen bereitstellt, wie etwa den Lebenszyklus der Anlage (Geburtstag oder Ende der Lebensdauer), den Standort des Gebäudes oder Rechenzentrums und die Ebene, möchten Sie die Daten möglicherweise auf andere Weise anzeigen.

Die Daten in benutzerdefinierten Anmerkungen ergänzen bereits erfasste Gerätedaten, wie etwa Switch-Hersteller, Anzahl der Ports und Leistungsstatistiken. Die Daten, die Sie mithilfe von Anmerkungen hinzufügen, werden von Data Infrastructure Insights nicht erkannt.

Bevor Sie beginnen

- Listen Sie alle Branchenterminologien auf, mit denen Umgebungsdaten verknüpft werden müssen.
- Listen Sie die Unternehmensterminologie auf, mit der Umgebungsdaten verknüpft werden müssen.
- Identifizieren Sie alle Standardanmerkungstypen, die Sie möglicherweise verwenden können.
- Ermitteln Sie, welche benutzerdefinierten Anmerkungen Sie erstellen müssen. Sie müssen die Anmerkung

erstellen, bevor sie einem Asset zugewiesen werden kann.

Führen Sie die folgenden Schritte aus, um eine Anmerkung zu erstellen.

Schritte

1. Klicken Sie im Menü „Data Infrastructure Insights“ auf **Observability > Enrich > Annotations**
2. Klicken Sie auf **+ Anmerkung**, um eine neue Anmerkung zu erstellen.
3. Geben Sie einen Namen, eine Beschreibung und einen Typ für die neue Anmerkung ein.

   Geben Sie beispielsweise Folgendes ein, um eine Textanmerkung zu erstellen, die den physischen Standort eines Assets im Rechenzentrum 4 definiert:

   - Geben Sie einen Namen für die Anmerkung ein, beispielsweise „Standort“.
   - Geben Sie eine Beschreibung der Anmerkung ein, z. B. „Physischer Standort ist Rechenzentrum 4“.
   - Geben Sie den „Typ“ der Anmerkung ein, beispielsweise „Text“.

Manuelles Zuweisen von Anmerkungen zu Assets

Durch die Zuweisung von Anmerkungen zu Anlagen können Sie Anlagen auf für Ihr Unternehmen relevante Weise sortieren, gruppieren und darüber berichten. Obwohl Sie mithilfe von Anmerkungsregeln automatisch Anmerkungen zu Assets eines bestimmten Typs zuweisen können, können Sie Anmerkungen zu einem einzelnen Asset über die Asset-Seite zuweisen.

Bevor Sie beginnen

- Sie müssen die Anmerkung, die Sie zuweisen möchten, erstellt haben.

Schritte

1. Melden Sie sich bei Ihrer Data Infrastructure Insights Umgebung an.
2. Suchen Sie das Asset, auf das Sie die Anmerkung anwenden möchten.
   - Sie können Assets durch Abfragen, Auswählen aus einem Dashboard-Widget oder Suchen finden. Wenn Sie das gewünschte Asset gefunden haben, klicken Sie auf den Link, um die Zielseite des Assets zu öffnen.
3. Klicken Sie auf der Asset-Seite im Abschnitt „Benutzerdaten“ auf **+ Anmerkung**.
4. Das Dialogfeld „Anmerkung hinzufügen“ wird angezeigt.
5. Wählen Sie eine Anmerkung aus der Liste aus.
6. Klicken Sie auf „Wert“ und führen Sie je nach ausgewähltem Anmerkungstyp einen der folgenden Schritte aus:
   - Wenn der Anmerkungstyp „Liste“, „Datum“ oder „Boolesch“ ist, wählen Sie einen Wert aus der Liste aus.
   - Wenn der Anmerkungstyp Text ist, geben Sie einen Wert ein.
7. Klicken Sie auf **Speichern**.

Wenn Sie den Wert der Anmerkung nach der Zuweisung ändern möchten, klicken Sie auf das Anmerkungsfeld und wählen Sie einen anderen Wert aus. Wenn die Anmerkung vom Typ Liste ist und die Option „Neue Werte spontan hinzufügen“ ausgewählt ist, können Sie zusätzlich zur Auswahl eines vorhandenen Werts einen neuen Wert eingeben.

Zuweisen von Anmerkungen mithilfe von Anmerkungsregeln

Um Assets basierend auf von Ihnen definierten Kriterien automatisch Anmerkungen zuzuweisen, konfigurieren Sie Anmerkungsregeln. Data Infrastructure Insights weist die Anmerkungen den Assets basierend auf diesen Regeln zu. Data Infrastructure Insights bietet außerdem zwei Standardanmerkungsregeln, die Sie Ihren Anforderungen entsprechend ändern oder entfernen können, wenn Sie sie nicht verwenden möchten.

Erstellen von Anmerkungsregeln

Als Alternative zum manuellen Anwenden von Anmerkungen auf einzelne Assets können Sie mithilfe von Anmerkungsregeln automatisch Anmerkungen auf mehrere Assets anwenden. Manuell auf einzelnen Asset-Seiten festgelegte Anmerkungen haben Vorrang vor regelbasierten Anmerkungen, wenn Insight die Anmerkungsregeln auswertet.

Bevor Sie beginnen

Sie müssen eine Abfrage für die Anmerkungsregel erstellt haben.

Informationen zu diesem Vorgang

Obwohl Sie die Anmerkungstypen beim Erstellen der Regeln bearbeiten können, sollten Sie die Typen vorher definiert haben.

Schritte

1. Klicken Sie auf **Verwalten > Anmerkungsregeln**

   Auf der Seite „Annotationsregeln“ wird die Liste der vorhandenen Annotationsregeln angezeigt.

2. Klicken Sie auf **+ Hinzufügen**.
3. Gehen Sie folgendermaßen vor:
   a. Geben Sie im Feld **Name** einen eindeutigen Namen ein, der die Regel beschreibt.

      Dieser Name wird auf der Seite „Annotationsregeln“ angezeigt.

   b. Klicken Sie auf **Abfrage** und wählen Sie die Abfrage aus, die zum Anwenden der Anmerkung auf Assets verwendet wird.
   c. Klicken Sie auf **Anmerkung** und wählen Sie die Anmerkung aus, die Sie anwenden möchten.
   d. Klicken Sie auf **Wert** und wählen Sie einen Wert für die Anmerkung aus.

      Wenn Sie beispielsweise „Geburtstag“ als Anmerkung wählen, geben Sie ein Datum für den Wert an.

   e. Klicken Sie auf **Speichern**
   f. Klicken Sie auf **Alle Regeln ausführen**, wenn Sie alle Regeln sofort ausführen möchten. Andernfalls werden die Regeln in regelmäßigen Abständen ausgeführt.

Erstellen von Anmerkungsregeln

Mithilfe von Anmerkungsregeln können Sie Anmerkungen basierend auf den von Ihnen definierten Kriterien automatisch auf mehrere Assets anwenden. Data Infrastructure Insights weist die Anmerkungen den Assets basierend auf diesen Regeln zu. Manuell auf einzelnen Asset-Seiten festgelegte Anmerkungen haben Vorrang vor regelbasierten Anmerkungen, wenn Cloud Insight die Anmerkungsregeln auswertet.

Bevor Sie beginnen

Sie müssen eine Abfrage für die Anmerkungsregel erstellt haben.

Schritte

1. Klicken Sie im Data Infrastructure Insights -Menü auf **Verwalten > Anmerkungsregeln**.
2. Klicken Sie auf **+ Regel**, um eine neue Anmerkungsregel hinzuzufügen.

   Das Dialogfeld „Regel hinzufügen“ wird angezeigt.

3. Gehen Sie folgendermaßen vor:
   a. Geben Sie im Feld **Name** einen eindeutigen Namen ein, der die Regel beschreibt.

      Der Name wird auf der Seite „Anmerkungsregeln“ angezeigt.

   b. Klicken Sie auf **Abfrage** und wählen Sie die Abfrage aus, die Data Infrastructure Insights verwendet, um die Assets zu identifizieren, auf die sich die Anmerkung bezieht.
   c. Klicken Sie auf **Anmerkung** und wählen Sie die Anmerkung aus, die Sie anwenden möchten.
   d. Klicken Sie auf **Wert** und wählen Sie einen Wert für die Anmerkung aus.

      Wenn Sie beispielsweise „Geburtstag“ als Anmerkung wählen, geben Sie ein Datum für den Wert an.

   e. Klicken Sie auf **Speichern**
   f. Klicken Sie auf **Alle Regeln ausführen**, wenn Sie alle Regeln sofort ausführen möchten. Andernfalls werden die Regeln in regelmäßigen Abständen ausgeführt.

> In einer großen Data Infrastructure Insights -Umgebung stellen Sie möglicherweise fest, dass die Ausführung von Anmerkungsregeln eine Weile zu dauern scheint. Dies liegt daran, dass der Indexer zuerst ausgeführt wird und vor der Ausführung der Regeln abgeschlossen sein muss. Der Indexer gibt Data Infrastructure Insights die Möglichkeit, in Ihren Daten nach neuen oder aktualisierten Objekten und Zählern zu suchen oder diese zu filtern. Die Regel-Engine wartet, bis der Indexer seine Aktualisierung abgeschlossen hat, bevor sie die Regeln anwendet.

Ändern von Anmerkungsregeln

Sie können eine Anmerkungsregel ändern, um den Namen der Regel, ihre Anmerkung, den Wert der Anmerkung oder die mit der Regel verknüpfte Abfrage zu ändern.

Schritte

1. Klicken Sie im Data Infrastructure Insights -Menü auf **Verwalten > Anmerkungsregeln**.

   Auf der Seite „Annotationsregeln“ wird die Liste der vorhandenen Annotationsregeln angezeigt.

2. Suchen Sie die Anmerkungsregel, die Sie ändern möchten.

   Sie können die Anmerkungsregeln filtern, indem Sie einen Wert in das Filterfeld eingeben oder auf eine Seitenzahl klicken, um die Anmerkungsregeln seitenweise zu durchsuchen.

3. Klicken Sie auf das Menüsymbol für die Regel, die Sie ändern möchten.
4. Klicken Sie auf **Bearbeiten**

Das Dialogfeld „Regel bearbeiten“ wird angezeigt.

5. Ändern Sie den Namen, die Anmerkung, den Wert oder die Abfrage der Anmerkungsregel.

Ändern der Reihenfolge der Regeln

Anmerkungsregeln werden von oben nach unten in der Regelliste verarbeitet. Um die Reihenfolge zu ändern, in der eine Regel verarbeitet wird, gehen Sie wie folgt vor:

Schritte

1. Klicken Sie auf das Menüsymbol für die Regel, die Sie verschieben möchten.
2. Klicken Sie je nach Bedarf auf **Nach oben verschieben** oder **Nach unten verschieben**, bis die Regel an der gewünschten Stelle angezeigt wird.

Beachten Sie, dass beim Ausführen mehrerer Regeln, die dieselbe Anmerkung zu einem Asset aktualisieren, die erste Regel (von oben nach unten ausgeführt) die Anmerkung anwendet und das Asset aktualisiert. Anschließend wird die zweite Regel angewendet, ändert jedoch keine Anmerkungen, die bereits von der vorherigen Regel festgelegt wurden.

Löschen von Anmerkungsregeln

Möglicherweise möchten Sie Anmerkungsregeln löschen, die nicht mehr verwendet werden.

Schritte

1. Klicken Sie im Data Infrastructure Insights -Menü auf **Verwalten > Anmerkungsregeln**.

   Auf der Seite „Annotationsregeln“ wird die Liste der vorhandenen Annotationsregeln angezeigt.

2. Suchen Sie die Anmerkungsregel, die Sie löschen möchten.

   Sie können die Anmerkungsregeln filtern, indem Sie einen Wert in das Filterfeld eingeben oder auf eine Seitenzahl klicken, um die Anmerkungsregeln seitenweise zu durchsuchen.

3. Klicken Sie auf das Menüsymbol für die Regel, die Sie löschen möchten.
4. Klicken Sie auf **Löschen**

   Es wird eine Bestätigungsmeldung angezeigt, in der Sie gefragt werden, ob Sie die Regel löschen möchten.

5. Klicken Sie auf **OK**

Anmerkungen importieren

Data Infrastructure Insights enthält eine API zum Importieren von Anmerkungen oder Anwendungen aus einer CSV-Datei und zum Zuweisen dieser zu von Ihnen angegebenen Objekten.

Die Data Infrastructure Insights API ist in der * Data Infrastructure Insights Premium Edition* verfügbar.

Importieren

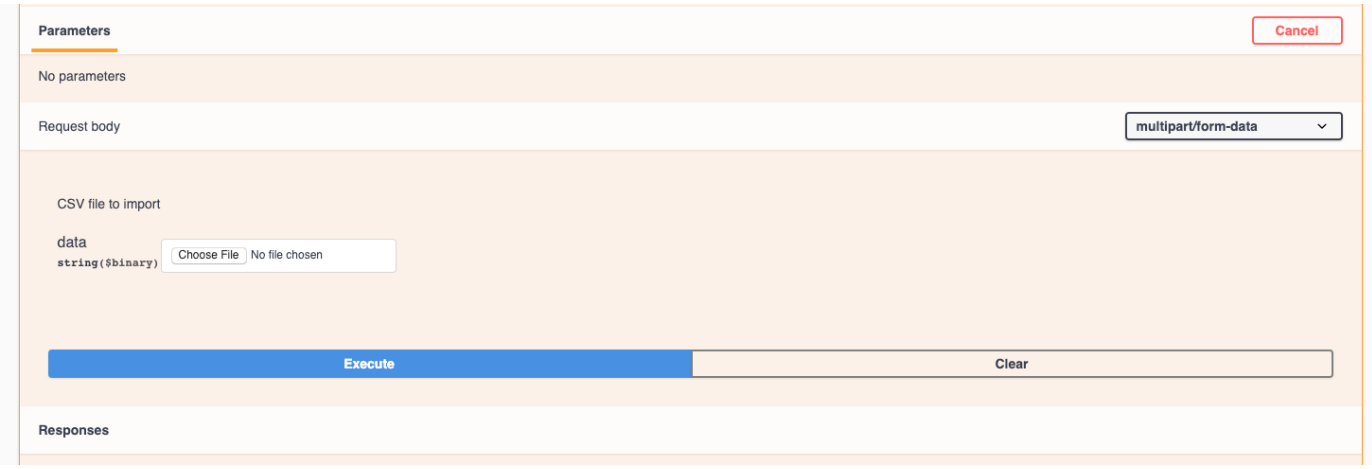
Die Links **Admin > API-Zugriff** enthalten"Dokumentation" für die **Assets/Import**-API. Diese Dokumentation enthält Informationen zum CSV-Dateiformat.

CSV-Dateiformat

Das allgemeine Format der CSV-Datei ist wie folgt. Die erste Zeile der Datei definiert die Importfelder und gibt die Reihenfolge der Felder an. Anschließend folgen für jede Anmerkung bzw. Anwendung separate Zeilen. Sie müssen nicht jedes Feld definieren. Die nachfolgenden Anmerkungszeilen müssen jedoch der gleichen Reihenfolge wie die Definitionszeile folgen.

```
 [Object Type] , [Object Name or ID] , Annotation Type [, Annotation
Type,  ...] [, Application] [, Tenant] [, Line_Of_Business] [,
Business_Unit] [, Project]
Beispiele für CSV-Dateien finden Sie in der API-Dokumentation.
```

Sie können Anmerkungen aus einer CSV-Datei direkt aus dem API-Swagger importieren und zuweisen. Wählen Sie einfach die zu verwendende Datei aus und klicken Sie auf die Schaltfläche *Ausführen*:



Importverhalten

Während des Importvorgangs werden Daten hinzugefügt, zusammengeführt oder ersetzt, je nachdem, welche Objekte und Objekttypen importiert werden. Beachten Sie beim Importieren die folgenden Verhaltensweisen.

- Fügt eine Anmerkung oder Anwendung hinzu, wenn im Zielsystem keine mit demselben Namen vorhanden ist.

- Führt eine Annotation zusammen, wenn der Annotationstyp eine Liste ist und im Zielsystem eine Annotation mit demselben Namen vorhanden ist.
- Ersetzt eine Annotation, wenn der Annotationstyp nicht eine Liste ist und im Zielsystem eine Annotation mit demselben Namen vorhanden ist.

  Hinweis: Wenn im Zielsystem eine Annotation mit demselben Namen, aber einem anderen Typ vorhanden ist, schlägt der Import fehl. Wenn Objekte von der fehlgeschlagenen Annotation abhängen, können diese Objekte falsche oder unerwünschte Informationen anzeigen. Sie müssen alle Anmerkungsabhängigkeiten überprüfen, nachdem der Importvorgang abgeschlossen ist.

- Wenn ein Annotationswert leer ist, wird diese Annotation aus dem Objekt entfernt. Vererbte Anmerkungen sind davon nicht betroffen.
- Annotationswerte vom Typ „Datum“ müssen als Unix-Zeit in Millisekunden übergeben werden.
- Beim Kommentieren von Volumes oder internen Volumes ist der Objektname eine Kombination aus Speichername und Volumename unter Verwendung des Trennzeichens "->". Beispiel: *<Speichername>-><Volumename>*
- Wenn ein Objektname ein Komma enthält, muss der gesamte Name in doppelte Anführungszeichen gesetzt werden. Beispiel: *"NetApp1,NetApp2"->023F*
- Beim Anhängen von Anmerkungen an Speicher, Switches und Ports wird die Spalte „Anwendung“ ignoriert.
- Mieter, Geschäftszweig, Geschäftseinheit und/oder Projekt bilden eine Geschäftseinheit. Wie bei allen Geschäftseinheiten kann jeder der Werte leer sein.

Die folgenden Objekttypen können mit Anmerkungen versehen werden.

OBJEKTTYP	NAME ODER SCHLÜSSEL
Gastgeber	id-><id> oder <Name> oder <IP>
VM	id-><id> oder <Name>
Speicherpool	id-><id> oder <Speichername>-><Speicherpoolname>
Internes Volumen	id-><id> oder <Speichername>-><Name des internen Datenträgers>
Volumen	id-><id> oder <Speichername>-><Volumename>
Storage	id-><id> oder <Name> oder <IP>
Schalten	id-><id> oder <Name> oder <IP>
Hafen	id-><id> oder <WWN>
Qtree	id-><id> oder <Speichername>-><Name des internen Datenträgers>-><Qtree-Name>
Aktie	id-><id> oder <Speichername>-><Name des internen Datenträgers>-><Freigabename>-><Protokoll>[-><Qtree-Name (optional im Fall des Standard-Qtree)>]

Arbeiten mit Anwendungen

Nachverfolgen der Asset-Nutzung nach Anwendung

Wenn Sie wissen, welche Anwendungen in der Umgebung Ihres Unternehmens verwendet werden, können Sie die Nutzung und Kosten Ihrer Anlagen besser im Auge behalten.

Bevor Sie Daten zu den auf Ihrem Mandanten ausgeführten Anwendungen verfolgen können, müssen Sie diese Anwendungen zunächst definieren und sie den entsprechenden Assets zuordnen. Sie können Anwendungen mit den folgenden Assets verknüpfen: Hosts, virtuelle Maschinen, Volumes, interne Volumes, Qtrees, Freigaben und Hypervisoren.

Dieses Thema bietet ein Beispiel für die Verfolgung der Nutzung virtueller Maschinen, die das Marketingteam für seine Exchange-E-Mails verwendet.

Sie können eine Tabelle ähnlich der folgenden erstellen, um die auf Ihrem Mandanten verwendeten Anwendungen zu identifizieren und die Gruppe oder Geschäftseinheit zu notieren, die die einzelnen Anwendungen verwendet.

Mieter	Geschäftszweig	Geschäftseinheit	Projekt	Anwendungen
NetApp	Datenspeicherung	Rechtliches	Patente	Oracle Identity Manager, Oracle On Demand, PatentWiz
NetApp	Datenspeicherung	Marketing	Verkaufsveranstaltungen	Exchange, Oracle Shared DataBase, BlastOff-Eventplaner

Die Tabelle zeigt, dass das Marketingteam die Exchange-Anwendung verwendet. Wir möchten die Auslastung ihrer virtuellen Maschinen für Exchange verfolgen, damit wir vorhersagen können, wann wir mehr Speicher hinzufügen müssen. Wir können die Exchange-Anwendung mit allen virtuellen Maschinen von Marketing verknüpfen:

1. Erstellen Sie eine Anwendung mit dem Namen *Exchange*
2. Gehen Sie zu **Abfragen > +Neue Abfrage**, um eine neue Abfrage für virtuelle Maschinen zu erstellen (oder wählen Sie ggf. eine vorhandene VM-Abfrage aus).

   Angenommen, alle VMs des Marketingteams haben einen Namen, der die Zeichenfolge „**mkt**“ enthält, erstellen Sie Ihre Abfrage, um den VM-Namen nach „mkt“ zu filtern.

3. Wählen Sie die VMs aus.
4. Verknüpfen Sie die VMs mit der *Exchange*-Anwendung mithilfe von **Massenaktionen > Anwendungen hinzufügen**.
5. Wählen Sie die gewünschte Anwendung aus und klicken Sie auf **Speichern**.
6. Wenn Sie fertig sind, **Speichern** Sie die Abfrage.

Erstellen von Anwendungen

Um Daten zu verfolgen, die mit bestimmten Anwendungen verknüpft sind, die auf Ihrem

Mandanten ausgeführt werden, können Sie die Anwendungen in Data Infrastructure Insights definieren.

Informationen zu diesem Vorgang

Mit Data Infrastructure Insights können Sie Daten von Assets, die mit Anwendungen verknüpft sind, für Zwecke wie Nutzungs- oder Kostenberichte verfolgen.

Schritte

1. Klicken Sie im Menü „Data Infrastructure Insights“ auf **Observability > Enrich > Applications**. Auswählen

   Das Dialogfeld „Anwendung hinzufügen“ wird angezeigt.

2. Geben Sie einen eindeutigen Namen für die Anwendung ein.
3. Wählen Sie eine Priorität für die Anwendung aus.
4. Klicken Sie auf **Speichern**.

Nachdem eine Anwendung definiert wurde, kann sie den Assets zugewiesen werden.

Zuweisen von Anwendungen zu Assets

Dieses Verfahren weist die Anwendung beispielhaft einem Host zu. Sie können einer Anwendung Host, virtuelle Maschine, Volume oder interne Volumes zuweisen.

Schritte

1. Suchen Sie das Asset, dem Sie die Anwendung zuweisen möchten:
2. Klicken Sie auf **Abfragen > +Neue Abfrage** und suchen Sie nach Host.
3. Aktivieren Sie das Kontrollkästchen links neben dem Host, den Sie mit der Anwendung verknüpfen möchten.
4. Klicken Sie auf **Massenaktionen > Anwendung hinzufügen**.
5. Wählen Sie die Anwendung aus, der Sie das Asset zuweisen.

Alle neuen Anwendungen, die Sie zuweisen, überschreiben alle Anwendungen auf dem Asset, die von einem anderen Asset abgeleitet wurden. Beispielsweise erben Volumes Anwendungen von Hosts, und wenn einem Volume neue Anwendungen zugewiesen werden, hat die neue Anwendung Vorrang vor der abgeleiteten Anwendung.

In Umgebungen mit einer großen Menge verwandter Assets kann die Vererbung von Anwendungszuweisungen zu diesen Assets mehrere Minuten dauern. Bitte rechnen Sie mit einer längeren Vererbungszeit, wenn Sie über viele zusammenhängende Vermögenswerte verfügen.

Nach Abschluss

Nachdem Sie der Anwendung den Host zugewiesen haben, können Sie der Anwendung die restlichen Assets zuweisen. Um auf die Zielseite der Anwendung zuzugreifen, klicken Sie auf **Verwalten > Anwendung** und wählen Sie die von Ihnen erstellte Anwendung aus.

Automatische Geräteauflösung

Übersicht über die automatische Geräteauflösung

Sie müssen alle Geräte identifizieren, die Sie mit Data Infrastructure Insights überwachen möchten. Eine Identifizierung ist erforderlich, um die Leistung und den Bestand Ihres Mieters genau zu verfolgen. Normalerweise wird die Mehrheit der auf Ihrem Mandanten erkannten Geräte durch die *Automatische Geräteauflösung* identifiziert.

Nachdem Sie Datensammler konfiguriert haben, werden Geräte auf Ihrem Mandanten identifiziert, darunter Switches, Speicher-Arrays und Ihre virtuelle Infrastruktur aus Hypervisoren und VMs. Allerdings werden dadurch normalerweise nicht 100 % der Geräte Ihres Mandanten identifiziert.

Nachdem Geräte vom Typ „Datensammler“ konfiguriert wurden, besteht die bewährte Vorgehensweise darin, Geräteauflösungsregeln zu nutzen, um die verbleibenden unbekannten Geräte auf Ihrem Mandanten zu identifizieren. Mithilfe der Geräteauflösung können Sie unbekannte Geräte als folgende Gerätetypen auflösen:

- Physische Hosts
- Speicher-Arrays
- Bänder

Geräte, die nach der Geräteauflösung als unbekannt verbleiben, gelten als generische Geräte, die Sie auch in Abfragen und auf Dashboards anzeigen können.

Die wiederum erstellten Regeln identifizieren automatisch neue Geräte mit ähnlichen Attributen, wenn sie Ihrer Umgebung hinzugefügt werden. In einigen Fällen ermöglicht die Geräteauflösung auch eine manuelle Identifizierung, indem die Geräteauflösungsregeln für nicht erkannte Geräte in Data Infrastructure Insights umgangen werden.

Eine unvollständige Identifizierung von Geräten kann zu folgenden Problemen führen:

- Unvollständige Pfade
- Nicht identifizierte Mehrwegeverbindungen
- Die Unfähigkeit, Anwendungen zu gruppieren
- Ungenaue Topologieansichten
- Ungenaue Daten im Data Warehouse und Reporting

Die Funktion zur Geräteauflösung (Verwalten > Geräteauflösung) umfasst die folgenden Registerkarten, die jeweils eine Rolle bei der Planung der Geräteauflösung und der Anzeige der Ergebnisse spielen:

- **Fibre Channel Identify** enthält eine Liste mit WWNs und Portinformationen von Fibre Channel-Geräten, die nicht durch die automatische Geräteauflösung aufgelöst wurden. Auf der Registerkarte wird auch der Prozentsatz der identifizierten Geräte angegeben.
- **IP-Adressidentifizierung** enthält eine Liste von Geräten, die auf CIFS-Freigaben und NFS-Freigaben zugreifen und nicht durch die automatische Geräteauflösung identifiziert wurden. Auf der Registerkarte wird auch der Prozentsatz der identifizierten Geräte angegeben.
- **Regeln zur automatischen Auflösung** enthält die Liste der Regeln, die bei der Auflösung von Fibre-Channel-Geräten ausgeführt werden. Dies sind Regeln, die Sie erstellen, um nicht identifizierte Fibre-Channel-Geräte aufzulösen.
- **Einstellungen** bietet Konfigurationsoptionen, mit denen Sie die Geräteauflösung an Ihre Umgebung anpassen können.

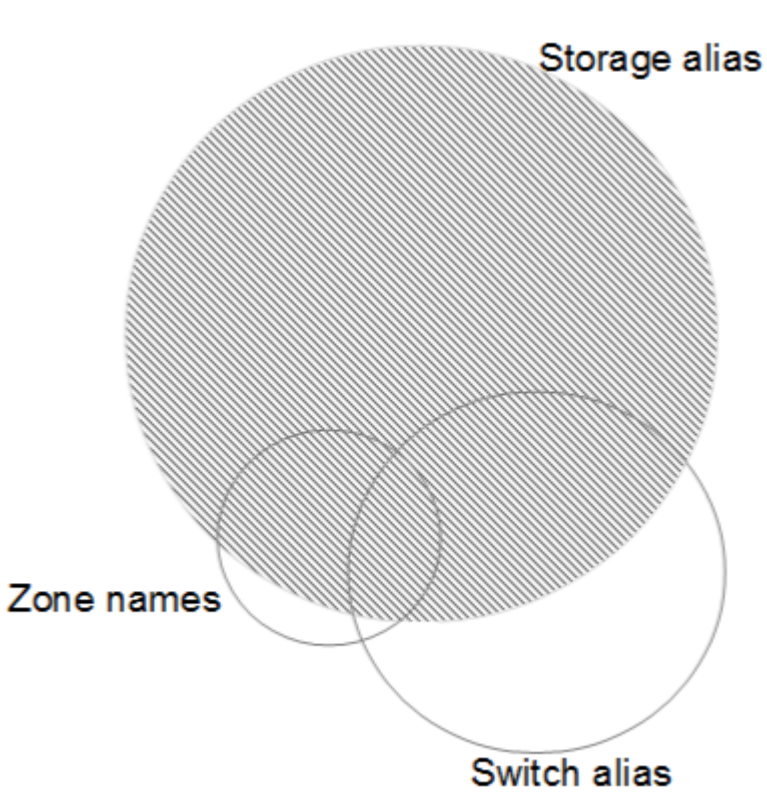
Bevor Sie beginnen

Sie müssen wissen, wie Ihre Umgebung konfiguriert ist, bevor Sie die Regeln zur Identifizierung von Geräten definieren. Je mehr Sie über Ihre Umgebung wissen, desto einfacher ist es, Geräte zu identifizieren.

Um genaue Regeln erstellen zu können, müssen Sie Fragen wie die folgenden beantworten:

- Verfügt Ihre Umgebung über Benennungsstandards für Zonen oder Hosts und wie viel Prozent davon sind korrekt?
- Verwendet Ihre Umgebung einen Switch-Alias oder Speicheralias und stimmen diese mit dem Hostnamen überein?
- Wie oft ändern sich die Benennungsschemata Ihres Mandanten?
- Gab es Übernahmen oder Fusionen, die zu unterschiedlichen Namensgebungen geführt haben?

Nach der Analyse Ihrer Umgebung sollten Sie in der Lage sein, die vorhandenen Namensstandards zu ermitteln, die Sie voraussichtlich zuverlässig antreffen werden. Die von Ihnen gesammelten Informationen können grafisch in einer Abbildung ähnlich der folgenden dargestellt werden:



In diesem Beispiel wird die größte Anzahl von Geräten zuverlässig durch Speicheraliase dargestellt. Regeln, die Hosts mithilfe von Speicheraliasen identifizieren, sollten zuerst geschrieben werden, Regeln mit Switch-Aliasen sollten als Nächstes geschrieben werden und die zuletzt erstellten Regeln sollten Zonen-Aliase verwenden. Aufgrund der Überschneidung bei der Verwendung von Zonenaliasen und Switch-Aliasen können einige Speicheraliasregeln zusätzliche Geräte identifizieren, sodass weniger Regeln für Zonenaliase und Switch-Aliase erforderlich sind.

Schritte zum Identifizieren von Geräten

Normalerweise verwenden Sie einen Workflow ähnlich dem folgenden, um Geräte auf Ihrem Mandanten zu identifizieren. Die Identifizierung ist ein iterativer Prozess und kann mehrere Schritte der Planung und

Verfeinerung von Regeln erfordern.

- Forschungsumfeld
- Planregeln
- Regeln erstellen/überarbeiten
- Ergebnisse überprüfen
- Erstellen Sie zusätzliche Regeln oder identifizieren Sie Geräte manuell
- Erledigt

> Wenn sich auf Ihrem Mandanten nicht identifizierte Geräte (auch als unbekannte oder generische Geräte bezeichnet) befinden und Sie anschließend eine Datenquelle konfigurieren, die diese Geräte bei der Abfrage identifiziert, werden sie nicht mehr als generische Geräte angezeigt oder gezählt.

Verwandt:"Erstellen von Geräteauflösungsregeln" "Fibre Channel-Geräteauflösung" "IP-Geräteauflösung" "Festlegen der Geräteauflösungseinstellungen"

Regeln zur Geräteauflösung

Sie erstellen Geräteauflösungsregeln, um Hosts, Speicher und Bänder zu identifizieren, die derzeit nicht automatisch von Data Infrastructure Insights identifiziert werden. Die von Ihnen erstellten Regeln identifizieren Geräte, die sich derzeit in Ihrer Umgebung befinden, und identifizieren auch ähnliche Geräte, wenn sie Ihrer Umgebung hinzugefügt werden.

Erstellen von Geräteauflösungsregeln

Wenn Sie Regeln erstellen, identifizieren Sie zunächst die Informationsquelle, auf die die Regel angewendet wird, die zum Extrahieren der Informationen verwendete Methode und ob auf die Ergebnisse der Regel eine DNS-Suche angewendet wird.

Quelle, die zur Identifizierung des Geräts verwendet wird	* SRM-Aliase für Hosts * Speicheralias mit eingebettetem Host- oder Bandnamen * Switch-Alias mit eingebettetem Host- oder Bandnamen * Zonennamen mit eingebettetem Hostnamen
Methode, die zum Extrahieren des Gerätenamens aus der Quelle verwendet wird	* Wie es ist (einen Namen aus einem SRM extrahieren) * Trennzeichen * Reguläre Ausdrücke
DNS-Suche	Gibt an, ob Sie DNS zur Überprüfung des Hostnamens verwenden

Sie erstellen Regeln auf der Registerkarte „Regeln für die automatische Auflösung“. Die folgenden Schritte beschreiben den Regelerstellungsprozess.

Verfahren

1. Klicken Sie auf **Verwalten > Geräteauflösung**
2. Klicken Sie auf der Registerkarte **Regeln zur automatischen Auflösung** auf **+ Host-Regel** oder **+ Bandregel**.

Der Bildschirm **Auflösungsregel** wird angezeigt.

Klicken Sie auf den Link „Übereinstimmungskriterien anzeigen“, um Hilfe und Beispiele zum Erstellen regulärer Ausdrücke zu erhalten.

3. Wählen Sie in der Liste **Typ** das Gerät aus, das Sie identifizieren möchten.

   Sie können *Host* oder *Tape* auswählen.

4. Wählen Sie in der Liste **Quelle** die Quelle aus, die Sie zur Identifizierung des Hosts verwenden möchten.

   Abhängig von der ausgewählten Quelle zeigt Data Infrastructure Insights die folgende Antwort an:

   a. **Zonen** listet die Zonen und WWN auf, die von Data Infrastructure Insights identifiziert werden müssen.
   b. **SRM** listet die nicht identifizierten Aliase auf, die von Data Infrastructure Insights identifiziert werden müssen
   c. **Speicheralias** listet Speicheraliase und WWN auf, die von Data Infrastructure Insights identifiziert werden müssen
   d. **Switch-Alias** listet die Switch-Aliase auf, die von Data Infrastructure Insights identifiziert werden müssen

5. Wählen Sie in der Liste **Methode** die Methode aus, die Sie zur Identifizierung des Hosts verwenden möchten.

Quelle	Verfahren
SRM	Wie es ist, Trennzeichen, reguläre Ausdrücke
Speicheralias	Trennzeichen, reguläre Ausdrücke
Alias wechseln	Trennzeichen, reguläre Ausdrücke
Zonen	Trennzeichen, reguläre Ausdrücke

   - Regeln mit Trennzeichen erfordern die Trennzeichen und die Mindestlänge des Hostnamens. Die Mindestlänge des Hostnamens ist die Anzahl der Zeichen, die Data Infrastructure Insights zur Identifizierung eines Hosts verwenden soll. Data Infrastructure Insights führt DNS-Lookups nur für Hostnamen durch, die so lang oder länger sind.

     Bei Regeln mit Trennzeichen wird die Eingabezeichenfolge durch das Trennzeichen tokenisiert und eine Liste mit Hostnamenkandidaten wird erstellt, indem mehrere Kombinationen des angrenzenden Tokens erstellt werden. Die Liste wird dann von groß nach klein sortiert. Beispielsweise würde die Liste bei einer Eingabezeichenfolge von *vipsnq03_hba3_emc3_12ep0* Folgendes ergeben:

     - vipsnq03_hba3_emc3_12ep0
     - vipsnq03_hba3_emc3
     - hba3 emc3_12ep0
     - vipsnq03_hba3
     - emc3_12ep0
     - hba3_emc3
     - vipsnq03

        - 12ep0
        - emc3
        - hba3
    - Regeln, die reguläre Ausdrücke verwenden, erfordern einen regulären Ausdruck, das Format und die Auswahl der Groß-/Kleinschreibung.
6. Klicken Sie auf **AR ausführen**, um alle Regeln auszuführen, oder klicken Sie auf den Abwärtspfeil in der Schaltfläche, um die von Ihnen erstellte Regel auszuführen (und alle anderen Regeln, die seit der letzten vollständigen Ausführung von AR erstellt wurden).

   Die Ergebnisse des Regellaufs werden auf der Registerkarte **FC-Identifizierung** angezeigt.

Starten einer automatischen Aktualisierung der Geräteauflösung

Bei einer Aktualisierung der Geräteauflösung werden manuelle Änderungen übernommen, die seit dem letzten vollautomatischen Geräteauflösungslauf hinzugefügt wurden. Durch Ausführen eines Updates können nur die neuen manuellen Einträge in der Geräteauflösungskonfiguration übernommen und ausgeführt werden. Es wird kein vollständiger Geräteauflösungslauf durchgeführt.

Verfahren

1. Melden Sie sich bei der Web-Benutzeroberfläche von Data Infrastructure Insights an.
2. Klicken Sie auf **Verwalten > Geräteauflösung**
3. Klicken Sie im Bildschirm **Geräteauflösung** auf den Abwärtspfeil in der Schaltfläche **AR ausführen**.
4. Klicken Sie auf **Aktualisieren**, um das Update zu starten.

Regelgestützte manuelle Identifikation

Diese Funktion wird für Sonderfälle verwendet, in denen Sie eine bestimmte Regel oder eine Liste von Regeln (mit oder ohne einmalige Neuordnung) ausführen möchten, um unbekannte Hosts, Speicher- und Bandgeräte aufzulösen.

Bevor Sie beginnen

Sie haben eine Reihe von Geräten, die nicht identifiziert wurden, und Sie haben auch mehrere Regeln, die andere Geräte erfolgreich identifiziert haben.

> Wenn Ihre Quelle nur einen Teil eines Host- oder Gerätenamens enthält, verwenden Sie eine reguläre Ausdrucksregel und formatieren Sie sie, um den fehlenden Text hinzuzufügen.

Verfahren

1. Melden Sie sich bei der Web-Benutzeroberfläche von Data Infrastructure Insights an.
2. Klicken Sie auf **Verwalten > Geräteauflösung**
3. Klicken Sie auf die Registerkarte **Fibre Channel Identify**.

   Das System zeigt die Geräte zusammen mit ihrem Auflösungsstatus an.

4. Wählen Sie mehrere nicht identifizierte Geräte aus.
5. Klicken Sie auf **Massenaktionen** und wählen Sie **Hostauflösung festlegen** oder **Bandauflösung festlegen**.

Das System zeigt den Bildschirm „Identifizieren“ an, der eine Liste aller Regeln enthält, die Geräte erfolgreich identifiziert haben.

6. Ändern Sie die Reihenfolge der Regeln in eine Reihenfolge, die Ihren Anforderungen entspricht.

   Die Reihenfolge der Regeln wird im Identifizierungsbildschirm geändert, jedoch nicht global.

7. Wählen Sie die Methode aus, die Ihren Anforderungen entspricht.

Data Infrastructure Insights führt den Hostauflösungsprozess in der Reihenfolge aus, in der die Methoden angezeigt werden, beginnend mit denen ganz oben.

Wenn zutreffende Regeln gefunden werden, werden die Regelnamen in der Spalte „Regeln“ angezeigt und als „manuell“ gekennzeichnet.

Verwandt:"Fibre Channel-Geräteauflösung" "IP-Geräteauflösung" "Festlegen der Geräteauflösungseinstellungen"

Fibre Channel-Geräteauflösung

Der Bildschirm „Fibre Channel-Identifizierung“ zeigt die WWN und WWPN von Fibre-Channel-Geräten an, deren Hosts nicht durch die automatische Geräteauflösung identifiziert wurden. Auf dem Bildschirm werden auch alle Geräte angezeigt, die durch manuelle Geräteauflösung aufgelöst wurden.

Geräte, die durch manuelle Auflösung aufgelöst wurden, weisen den Status *OK* auf und identifizieren die Regel, die zur Identifizierung des Geräts verwendet wurde. Fehlende Geräte haben den Status *Unidentifiziert*. Geräte, die ausdrücklich von der Identifizierung ausgeschlossen sind, haben den Status *Ausgeschlossen*. Die Gesamtabdeckung zur Identifizierung von Geräten ist auf dieser Seite aufgeführt.

Sie führen Massenaktionen durch, indem Sie auf der linken Seite des Fibre Channel-Identifizierungsbildschirms mehrere Geräte auswählen. Aktionen können auf einem einzelnen Gerät ausgeführt werden, indem Sie mit der Maus über ein Gerät fahren und die Schaltflächen „Identifizieren“ oder „Nicht identifizieren“ ganz rechts in der Liste auswählen.

Der Link „Gesamtabdeckung“ zeigt eine Liste der Anzahl der identifizierten Geräte/der für Ihre Konfiguration verfügbaren Geräte an:

- SRM-Alias
- Speicheralias
- Alias wechseln
- Zonen
- Benutzerdefiniert

Manuelles Hinzufügen eines Fibre Channel-Geräts

Sie können Data Infrastructure Insights manuell ein Fibre-Channel-Gerät hinzufügen, indem Sie die Funktion „Manuell hinzufügen“ verwenden, die auf der Registerkarte „Fibre-Channel-Identifizierung“ der Geräteauflösung verfügbar ist. Dieser Prozess kann zur Voridentifizierung eines Geräts verwendet werden, das voraussichtlich in der Zukunft entdeckt wird.

Bevor Sie beginnen

Um dem System erfolgreich eine Geräteidentifikation hinzuzufügen, müssen Sie die WWN- oder IP-Adresse und den Gerätenamen kennen.

Informationen zu diesem Vorgang

Sie können ein Host-, Speicher-, Band- oder unbekanntes Fibre-Channel-Gerät manuell hinzufügen.

Verfahren

1. Melden Sie sich bei der Data Infrastructure Insights -Webbenutzeroberfläche an
2. Klicken Sie auf **Verwalten > Geräteauflösung**
3. Klicken Sie auf die Registerkarte **Fibre Channel Identify**.
4. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Dialog **Gerät hinzufügen** wird angezeigt

5. Geben Sie die WWN- oder IP-Adresse und den Gerätenamen ein und wählen Sie den Gerätetyp aus.

   Das von Ihnen eingegebene Gerät wird der Geräteliste auf der Registerkarte „Fibre Channel-Identifizierung“ hinzugefügt. Die Regel wird als *Manuell* gekennzeichnet.

Importieren der Fibre Channel-Geräteidentifikation aus einer CSV-Datei

Sie können die Fibre-Channel-Geräteidentifikation manuell in die Data Infrastructure Insights -Geräteauflösung importieren, indem Sie eine Geräteliste in einer CSV-Datei verwenden.

1. Bevor Sie beginnen

Sie müssen über eine korrekt formatierte CSV-Datei verfügen, um Geräteidentifikationen direkt in die Geräteauflösung zu importieren. Die CSV-Datei für Fibre-Channel-Geräte erfordert die folgenden Informationen:

WWN	IP	Name	Typ

Die Datenfelder müssen in Anführungszeichen gesetzt werden, wie im folgenden Beispiel gezeigt.

```
"WWN","IP","Name","Type"
"WWN:2693","ADDRESS2693|IP2693","NAME-2693","HOST"
"WWN:997","ADDRESS997|IP997","NAME-997","HOST"
"WWN:1860","ADDRESS1860|IP1860","NAME-1860","HOST"
```

Als bewährte Methode wird empfohlen, zunächst die Fibre Channel Identify-Informationen in eine CSV-Datei zu exportieren, die gewünschten Änderungen in dieser Datei vorzunehmen und die Datei dann wieder in Fibre Channel Identify zu importieren. Dadurch wird sichergestellt, dass die erwarteten Spalten vorhanden und in der richtigen Reihenfolge sind.

So importieren Sie Fibre Channel-Identifikationsinformationen:

1. Melden Sie sich bei der Web-Benutzeroberfläche von Data Infrastructure Insights an.
2. Klicken Sie auf **Verwalten > Geräteauflösung**

3. Wählen Sie die Registerkarte **Fibre Channel Identify**.
4. Klicken Sie auf die Schaltfläche **Identifizieren > Aus Datei identifizieren**.
5. Navigieren Sie zu dem Ordner, der Ihre zu importierenden CSV-Dateien enthält, und wählen Sie die gewünschte Datei aus.

   Die von Ihnen eingegebenen Geräte werden der Geräteliste auf der Registerkarte „Fibre Channel-Identifizierung“ hinzugefügt. Die „Regel“ wird als „Manuell“ gekennzeichnet.

Exportieren von Fibre Channel-Gerätekennungen in eine CSV-Datei

Sie können vorhandene Fibre-Channel-Geräteidentifikationen aus der Geräteauflösungsfunktion von Data Infrastructure Insights in eine CSV-Datei exportieren. Möglicherweise möchten Sie eine Gerätekennung exportieren, damit Sie sie ändern und dann wieder in Data Infrastructure Insights importieren können, wo sie dann zum Identifizieren von Geräten verwendet wird, die denen ähneln, die ursprünglich mit der exportierten Kennung übereinstimmten.

Informationen zu diesem Vorgang

Dieses Szenario kann verwendet werden, wenn Geräte ähnliche Attribute haben, die in der CSV-Datei einfach bearbeitet und dann wieder in das System importiert werden können.

Wenn Sie eine Fibre Channel-Gerätekennung in eine CSV-Datei exportieren, enthält die Datei die folgenden Informationen in der angezeigten Reihenfolge:

WWN	IP	Name	Typ

Verfahren

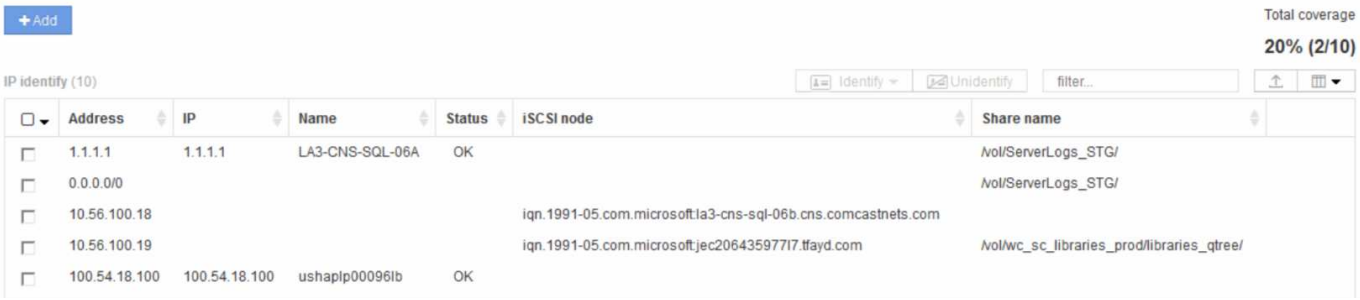
1. Melden Sie sich bei der Web-Benutzeroberfläche von Data Infrastructure Insights an.
2. Klicken Sie auf **Verwalten > Geräteauflösung**
3. Wählen Sie die Registerkarte **Fibre Channel Identify**.
4. Wählen Sie das oder die Fibre-Channel-Geräte aus, deren Identifikation Sie exportieren möchten.
5. Klicken Sie auf *Exportieren* Taste.

   Wählen Sie aus, ob die CSV-Datei geöffnet oder gespeichert werden soll.

Verwandt:"IP-Geräteauflösung" "Erstellen von Geräteauflösungsregeln" "Festlegen der Geräteauflösungseinstellungen"

IP-Geräteauflösung

Der Bildschirm „IP-Identifizierung“ zeigt alle iSCSI- und CIFS- oder NFS-Freigaben an, die durch automatische oder manuelle Geräteauflösung identifiziert wurden. Es werden auch nicht identifizierte Geräte angezeigt. Der Bildschirm enthält die IP-Adresse, den Namen, den Status, den iSCSI-Knoten und den Freigabenamen für Geräte. Außerdem wird der Prozentsatz der erfolgreich identifizierten Geräte angezeigt.



IP-Geräte manuell hinzufügen

Sie können Data Infrastructure Insights manuell ein IP-Gerät hinzufügen, indem Sie die Funktion zum manuellen Hinzufügen im Bildschirm „IP-Identifizierung“ verwenden.

Verfahren

1. Melden Sie sich bei der Data Infrastructure Insights Webbenutzeroberfläche an.
2. Klicken Sie auf **Verwalten > Geräteauflösung**
3. Klicken Sie auf die Registerkarte **IP-Adresse identifizieren**.
4. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Dialog „Gerät hinzufügen“ wird angezeigt

5. Geben Sie die Adresse, IP-Adresse und einen eindeutigen Gerätenamen ein.

Ergebnis

Das von Ihnen eingegebene Gerät wird der Geräteliste auf der Registerkarte „IP-Adresse identifizieren“ hinzugefügt.

Importieren der IP-Geräteidentifikation aus einer CSV-Datei

Sie können IP-Gerätekennungen manuell in die Funktion „Geräteauflösung“ importieren, indem Sie eine Liste von Gerätekennungen in einer CSV-Datei verwenden.

1. Bevor Sie beginnen

Sie müssen über eine korrekt formatierte CSV-Datei verfügen, um Geräteidentifikationen direkt in die Funktion „Geräteauflösung“ zu importieren. Die CSV-Datei für IP-Geräte erfordert die folgenden Informationen:

Adresse	IP	Name

Die Datenfelder müssen in Anführungszeichen gesetzt werden, wie im folgenden Beispiel gezeigt.

```
"Address","IP","Name"
"ADDRESS6447","IP6447","NAME-6447"
"ADDRESS3211","IP3211","NAME-3211"
"ADDRESS593","IP593","NAME-593"
```

Als bewährte Methode wird empfohlen, zunächst die IP-Adressidentifizierungsinformationen in eine CSV-Datei zu exportieren, die gewünschten Änderungen in dieser Datei vorzunehmen und die Datei dann wieder in IP Address Identify zu importieren. Dadurch wird sichergestellt, dass die erwarteten Spalten vorhanden und in der richtigen Reihenfolge sind.

Exportieren der IP-Geräteidentifikation in eine CSV-Datei

Sie können vorhandene IP-Geräteidentifikationen aus der Geräteauflösungsfunktion von Data Infrastructure Insights in eine CSV-Datei exportieren. Möglicherweise möchten Sie eine Gerätekennung exportieren, damit Sie sie ändern und dann wieder in Data Infrastructure Insights importieren können, wo sie dann zum Identifizieren von Geräten verwendet wird, die denen ähneln, die ursprünglich mit der exportierten Kennung übereinstimmten.

Informationen zu diesem Vorgang

1. Dieses Szenario kann verwendet werden, wenn Geräte ähnliche Attribute haben, die in der CSV-Datei einfach bearbeitet und dann wieder in das System importiert werden können.

Wenn Sie eine IP-Gerätekennung in eine CSV-Datei exportieren, enthält die Datei die folgenden Informationen in der angezeigten Reihenfolge:

Adresse	IP	Name

Verfahren

1. Melden Sie sich bei der Web-Benutzeroberfläche von Data Infrastructure Insights an.
2. Klicken Sie auf **Verwalten > Geräteauflösung**
3. Wählen Sie die Registerkarte **IP-Adresse identifizieren**.
4. Wählen Sie das oder die IP-Geräte aus, deren Identifikation Sie exportieren möchten.
5. Klicken Sie auf *Exportieren* Taste.

   Wählen Sie aus, ob die CSV-Datei geöffnet oder gespeichert werden soll.

Verwandt:"Fibre Channel-Geräteauflösung" "Erstellen von Geräteauflösungsregeln" "Festlegen der Geräteauflösungseinstellungen"

Einstelloptionen auf der Registerkarte „Einstellungen“

Auf der Registerkarte „Einstellungen für die Geräteauflösung“ können Sie einen Zeitplan für die automatische Auflösung erstellen, Speicher- und Bandanbieter angeben, die in die Identifizierung einbezogen oder davon ausgeschlossen werden sollen, und DNS-Suchoptionen festlegen.

Zeitplan für die automatische Auflösung

Ein Zeitplan für die automatische Auflösung kann angeben, wann die automatische Geräteauflösung ausgeführt wird:

Option	Beschreibung

Jeder	Verwenden Sie diese Option, um die automatische Geräteauflösung in Intervallen von Tagen, Stunden oder Minuten auszuführen.
Täglich	Verwenden Sie diese Option, um die automatische Geräteauflösung täglich zu einer bestimmten Zeit auszuführen.
Manuell	Verwenden Sie diese Option, um die automatische Geräteauflösung nur manuell auszuführen.
Bei jeder Umgebungsänderung	Verwenden Sie diese Option, um bei jeder Änderung der Umgebung eine automatische Geräteauflösung auszuführen.

Wenn Sie *Manuell* angeben, wird die nächtliche automatische Geräteauflösung deaktiviert.

DNS-Verarbeitungsoptionen

Mit den DNS-Verarbeitungsoptionen können Sie die folgenden Funktionen auswählen:

- Wenn die Verarbeitung der DNS-Suchergebnisse aktiviert ist, können Sie eine Liste mit DNS-Namen hinzufügen, die an aufgelöste Geräte angehängt werden sollen.
- Sie können „Automatische Auflösung von IPs“ auswählen, um die automatische Hostauflösung für iSCSI-Initiatoren und Hosts zu aktivieren, die per DNS-Lookup auf NFS-Freigaben zugreifen. Wenn dies nicht angegeben ist, wird nur eine FC-basierte Auflösung durchgeführt.
- Sie können Unterstriche in Hostnamen zulassen und in Ergebnissen einen „Verbunden mit“-Alias anstelle des Standard-Port-Alias verwenden.

Einbeziehung oder Ausschluss bestimmter Speicher- und Bandanbieter

Sie können bestimmte Speicher- und Bandanbieter zur automatischen Lösung ein- oder ausschließen. Möglicherweise möchten Sie bestimmte Anbieter ausschließen, wenn Sie beispielsweise wissen, dass ein bestimmter Host zu einem Legacy-Host wird und aus Ihrer neuen Umgebung ausgeschlossen werden sollte. Sie können auch Anbieter erneut hinzufügen, die Sie zuvor ausgeschlossen hatten, aber nicht mehr ausschließen möchten.

Geräteauflösungsregeln für Bänder funktionieren nur für WWNs, bei denen der Anbieter für dieses WWN in den Anbietereinstellungen auf *Nur als Band enthalten* eingestellt ist.

Siehe auch:"Beispiele für reguläre Ausdrücke"

Beispiele für reguläre Ausdrücke

Wenn Sie den Ansatz mit regulären Ausdrücken als Ihre Quellenbenennungsstrategie ausgewählt haben, können Sie die Beispiele für reguläre Ausdrücke als Leitfaden für Ihre eigenen Ausdrücke verwenden, die in den automatischen Auflösungsmethoden von Data Infrastructure Insights verwendet werden.

Formatieren regulärer Ausdrücke

Beim Erstellen regulärer Ausdrücke für die automatische Auflösung von Data Infrastructure Insights können Sie das Ausgabeformat konfigurieren, indem Sie Werte in ein Feld mit dem Namen *FORMAT* eingeben.

Die Standardeinstellung ist \1, was bedeutet, dass ein Zonenname, der mit dem regulären Ausdruck übereinstimmt, durch den Inhalt der ersten durch den regulären Ausdruck erstellten Variable ersetzt wird. In einem regulären Ausdruck werden Variablenwerte durch Klammeraussagen erstellt. Wenn mehrere Klammeraussagen vorkommen, werden die Variablen numerisch von links nach rechts referenziert. Die Variablen können im Ausgabeformat in beliebiger Reihenfolge verwendet werden. In die Ausgabe kann auch konstanter Text eingefügt werden, indem dieser zum Feld FORMAT hinzugefügt wird.

Beispielsweise könnten Sie für diese Zonenbenennungskonvention die folgenden Zonennamen haben:

```
 [Zone number]_[data center]_[hostname]_[device type]_[interface number]
* S123_Miami_hostname1_filer_FC1
* S14_Tampa_hostname2_switch_FC4
* S3991_Boston_hostname3_windows2K_FC0
* S44_Raleigh_hostname4_solaris_FC1
```

Und Sie möchten vielleicht, dass die Ausgabe das folgende Format hat:

```
 [hostname]-[data center]-[device type]
Dazu müssen Sie die Felder Hostname, Rechenzentrum und Gerätetyp in
Variablen erfassen und in der Ausgabe verwenden.  Der folgende reguläre
Ausdruck würde dies bewirken:
```

```
 .*?_([a-zA-Z0-9]+)_([a-zA-Z0-9]+)_([a-zA-Z0-9]+)_.*
Da es drei Klammern gibt, würden die Variablen \1, \2 und \3 ausgefüllt.
```

Sie können dann das folgende Format verwenden, um die Ausgabe in Ihrem bevorzugten Format zu erhalten:

```
 \2-\1-\3
Ihre Ausgabe würde wie folgt aussehen:
```

```
hostname1-Miami-filer
hostname2-Tampa-switch
hostname3-Boston-windows2K
hostname4-Raleigh-solaris
```

Die Bindestriche zwischen den Variablen stellen ein Beispiel für konstanten Text dar, der in die formatierte Ausgabe eingefügt wird.

Beispiele

Beispiel 1 mit Zonennamen

In diesem Beispiel verwenden Sie den regulären Ausdruck, um einen Hostnamen aus dem Zonennamen zu

extrahieren. Sie können einen regulären Ausdruck erstellen, wenn Sie über etwas Ähnliches wie die folgenden Zonennamen verfügen:

- S0032_myComputer1Name-HBA0
- S0434_myComputer1Name-HBA1
- S0432_myComputer1Name-HBA3

Der reguläre Ausdruck, den Sie zum Erfassen des Hostnamens verwenden könnten, wäre:

```
 S[0-9]+_([a-zA-Z0-9]*)[_-]HBA[0-9]
Das Ergebnis ist eine Übereinstimmung aller Zonen, die mit S beginnen und
auf die eine beliebige Kombination aus Ziffern folgt, gefolgt von einem
Unterstrich, dem alphanumerischen Hostnamen (myComputer1Name), einem
Unterstrich oder Bindestrich, den Großbuchstaben HBA und einer einzelnen
Ziffer (0-9).  In der Variable *\1* wird nur der Hostname gespeichert.
```

Der reguläre Ausdruck kann in seine Komponenten zerlegt werden:

- „S“ steht für den Zonennamen und leitet den Ausdruck ein. Dies entspricht nur einem „S“ am Anfang des Zonennamens.
- Die Zeichen [0-9] in Klammern geben an, dass auf „S“ eine Ziffer zwischen 0 und 9 (einschließlich) folgen muss.
- Das +-Zeichen gibt an, dass die Angabe in der vorhergehenden Klammer 1 oder mehrere Male vorkommen muss.
- Das _ (Unterstrich) bedeutet, dass auf die Ziffern nach S im Zonennamen unmittelbar nur ein Unterstrichzeichen folgen darf. In diesem Beispiel wird in der Zonenbenennungskonvention der Unterstrich verwendet, um den Zonennamen vom Hostnamen zu trennen.
- Nach dem erforderlichen Unterstrich zeigen die Klammern an, dass das darin enthaltene Muster in der Variable \1 gespeichert wird.
- Die eingeklammerten Zeichen [a-zA-Z0-9] geben an, dass es sich bei den übereinstimmenden Zeichen ausschließlich um Buchstaben (unabhängig von der Groß-/Kleinschreibung) und Zahlen handelt.
- Das * (Sternchen) nach den Klammern gibt an, dass die eingeklammerten Zeichen 0 oder mehr Mal vorkommen.
- Die eingeklammerten Zeichen [_-] (Unterstrich und Bindestrich) geben an, dass auf das alphanumerische Muster ein Unterstrich oder ein Bindestrich folgen muss.
- Die Buchstaben HBA im regulären Ausdruck geben an, dass genau diese Zeichenfolge im Zonennamen vorkommen muss.
- Der letzte Satz eingeklammerter Zeichen [0-9] entspricht einer einzelnen Ziffer von 0 bis einschließlich 9.

Beispiel 2

In diesem Beispiel wird bis zum ersten Unterstrich „*“ gesprungen, dann wird E und alles danach bis zum zweiten „*“ abgeglichen und dann alles danach übersprungen.

Zone: Z_E2FHDBS01_E1NETAPP

Hostname: E2FHDBS01

Regulärer Ausdruck: .*?(E.*?)*.*?

Beispiel 3

Die Klammern „( )“ um den letzten Abschnitt im regulären Ausdruck (unten) geben an, welcher Teil der Hostname ist. Wenn Sie VSAN3 als Hostnamen verwenden möchten, lautet dieser: _([a-zA-Z0-9]).*

Zone: A_VSAN3_SR48KENT_A_CX2578_SPA0

Hostname: SR48KENT

RegExp: _[a-zA-Z0-9]+_([a-zA-Z0-9]).*

Beispiel 4 zeigt ein komplizierteres Benennungsmuster

Sie können einen regulären Ausdruck erstellen, wenn Sie über etwas Ähnliches wie die folgenden Zonennamen verfügen:

- myComputerName123-HBA1_Symm1_FA3
- myComputerName123-HBA2_Symm1_FA5
- myComputerName123-HBA3_Symm1_FA7

Der reguläre Ausdruck, den Sie zum Erfassen dieser Daten verwenden könnten, wäre:

```
 ([a-zA-Z0-9]*)_.*
Die Variable \1 würde nach der Auswertung durch diesen Ausdruck nur
_myComputerName123_ enthalten.
```

Der reguläre Ausdruck kann in seine Komponenten zerlegt werden:

- Die Klammern zeigen an, dass das darin enthaltene Muster in der Variable \1 gespeichert wird.
- Die eingeklammerten Zeichen [a-zA-Z0-9] bedeuten, dass jeder Buchstabe (unabhängig von der Groß-/Kleinschreibung) oder jede Ziffer übereinstimmt.
- Das * (Sternchen) nach den Klammern gibt an, dass die eingeklammerten Zeichen 0 oder mehr Mal vorkommen.
- Das Zeichen _ (Unterstrich) im regulären Ausdruck bedeutet, dass der Zonenname unmittelbar nach der alphanumerischen Zeichenfolge, die mit den vorhergehenden Klammern übereinstimmt, einen Unterstrich haben muss.
- Der . (Punkt) entspricht einem beliebigen Zeichen (einem Platzhalter).
- Das * (Sternchen) zeigt an, dass der Platzhalter für den vorangehenden Punkt 0 oder mehr Mal vorkommen kann.

  Mit anderen Worten: Die Kombination .* steht für ein beliebiges Zeichen, beliebig oft.

Beispiel 5 mit Zonennamen ohne Muster

Sie können einen regulären Ausdruck erstellen, wenn Sie über etwas Ähnliches wie die folgenden Zonennamen verfügen:

- myComputerName_HBA1_Symm1_FA1
- myComputerName123_HBA1_Symm1_FA1

Der reguläre Ausdruck, den Sie zum Erfassen dieser Daten verwenden könnten, wäre:

```
 (.*?)_.*
Die Variable \1 würde _myComputerName_ (im ersten Zonennamenbeispiel) oder
_myComputerName123_ (im zweiten Zonennamenbeispiel) enthalten.  Dieser
reguläre Ausdruck würde also auf alles vor dem ersten Unterstrich passen.
```

Der reguläre Ausdruck kann in seine Komponenten zerlegt werden:

- Die Klammern zeigen an, dass das darin enthaltene Muster in der Variable \1 gespeichert wird.
- Der .* (Punkt Sternchen) passt zu jedem beliebigen Zeichen, beliebig oft.
- Das * (Sternchen) nach den Klammern gibt an, dass die eingeklammerten Zeichen 0 oder mehr Mal vorkommen.
- Das Zeichen ? macht die Übereinstimmung nicht gierig. Dadurch wird die Suche beim ersten Unterstrich beendet und nicht beim letzten.
- Die Zeichen _.* entsprechen dem ersten gefundenen Unterstrich und allen darauf folgenden Zeichen.

Beispiel 6 mit Computernamen mit einem Muster

Sie können einen regulären Ausdruck erstellen, wenn Sie über etwas Ähnliches wie die folgenden Zonennamen verfügen:

- Storage1_Switch1_myComputerName123A_A1_FC1
- Storage2_Switch2_myComputerName123B_A2_FC2
- Storage3_Switch3_myComputerName123T_A3_FC3

Der reguläre Ausdruck, den Sie zum Erfassen dieser Daten verwenden könnten, wäre:

```
 .*?_.*?_([a-zA-Z0-9]*[ABT])_.*
Da die Zonenbenennungskonvention eher einem Muster folgt, könnten wir den
obigen Ausdruck verwenden, der alle Instanzen eines Hostnamens (im
Beispiel myComputerName) abgleicht, der entweder mit A, B oder T endet,
und diesen Hostnamen in die Variable \1 einfügt.
```

Der reguläre Ausdruck kann in seine Komponenten zerlegt werden:

- Der .* (Punkt Sternchen) passt zu jedem beliebigen Zeichen, beliebig oft.
- Das Zeichen ? macht die Übereinstimmung nicht gierig. Dadurch wird die Suche beim ersten Unterstrich beendet und nicht beim letzten.
- Das Unterstrichzeichen entspricht dem ersten Unterstrich im Zonennamen.
- Daher entspricht die erste .*?-*Kombination den Zeichen Storage1* im ersten Zonennamenbeispiel.
- Die zweite .*?-*Kombination verhält sich wie die erste, entspricht aber Switch1* im ersten

Zonennamenbeispiel.

- Die Klammern zeigen an, dass das darin enthaltene Muster in der Variable \1 gespeichert wird.
- Die eingeklammerten Zeichen [a-zA-Z0-9] bedeuten, dass jeder Buchstabe (unabhängig von der Groß-/Kleinschreibung) oder jede Ziffer übereinstimmt.
- Das * (Sternchen) nach den Klammern gibt an, dass die eingeklammerten Zeichen 0 oder mehr Mal vorkommen.
- Die eingeklammerten Zeichen im regulären Ausdruck [ABT] entsprechen einem einzelnen Zeichen im Zonennamen, das A, B oder T sein muss.
- Der _ (Unterstrich) nach den Klammern gibt an, dass auf die Zeichenübereinstimmung [ABT] ein Unterstrich folgen muss.
- Der .* (Punkt Sternchen) passt zu jedem beliebigen Zeichen, beliebig oft.

Das Ergebnis wäre daher, dass die Variable \1 eine beliebige alphanumerische Zeichenfolge enthält, die:

- wurde durch eine Anzahl alphanumerischer Zeichen und zwei Unterstriche eingeleitet
- gefolgt von einem Unterstrich (und dann einer beliebigen Anzahl alphanumerischer Zeichen)
- hatte vor dem dritten Unterstrich ein letztes Zeichen von A, B oder T.

Beispiel 7

Zone: myComputerName123_HBA1_Symm1_FA1

Hostname: meinComputername123

Regulärer Ausdruck: ([a-zA-Z0-9]+)_.*

Beispiel 8

Dieses Beispiel findet alles vor dem ersten _.

Zone: MyComputerName_HBA1_Symm1_FA1

MyComputerName123_HBA1_Symm1_FA1

Hostname: MeinComputername

Regulärer Ausdruck: (.**?)_.**

Beispiel 9

Dieses Beispiel findet alles nach dem 1. _ und bis zum zweiten _.

Zone: Z_MeinComputername_Speichername

Hostname: MeinComputername

Regulärer Ausdruck: .***?(.?)***.*?

Beispiel 10

Dieses Beispiel extrahiert „MyComputerName123“ aus den Zonenbeispielen.

Zone: Storage1_Switch1_MyComputerName123A_A1_FC1

Storage2_Switch2_MyComputerName123B_A2_FC2

Storage3_Switch3_MyComputerName123T_A3_FC3

Hostname: MeinComputername123

RegExp: .**?.?**([a-zA-Z0-9]+)**[ABT]_.**

Beispiel 11

Zone: Storage1_Switch1_MyComputerName123A_A1_FC1

Hostname: MyComputerName123A

RegExp: .**?.?**([a-zA-z0-9]+).*?

Beispiel 12

Das ^ (Zirkumflex oder Caretzeichen) **in eckigen Klammern** negiert den Ausdruck. Beispielsweise bedeutet [^Ff] alles außer dem großen oder kleinen F und [^az] bedeutet alles außer den kleinen Buchstaben a bis z und im obigen Fall alles außer dem _. Die Formatanweisung fügt dem Ausgabehostnamen das „-“ hinzu.

Zone: mhs_apps44_d_A_10a0_0429

Hostname: mhs-apps44-d

Regulärer Ausdruck: ()_([AB]).*Format in Data Infrastructure Insights: \1-\2 ([^_])_ ()_([^_]).*Format in Data Infrastructure Insights: \1-\2-\3

Beispiel 13

In diesem Beispiel wird der Speicheralias durch „\“ abgegrenzt und der Ausdruck muss „\\“ verwenden, um zu definieren, dass in der Zeichenfolge tatsächlich „\“ verwendet werden und dass diese nicht Teil des Ausdrucks selbst sind.

Speicheralias: \Hosts\E2DOC01C1\E2DOC01N1

Hostname: E2DOC01N1

Regulärer Ausdruck: \\.**?\\.**?\\(.*?)

Beispiel 14

Dieses Beispiel extrahiert „PD-RV-W-AD-2“ aus den Zonenbeispielen.

Zone: PD_D-PD-RV-W-AD-2_01

Hostname: PD-RV-W-AD-2

Regulärer Ausdruck: -(.*-\d).*

Beispiel 15

Die Formateinstellung fügt in diesem Fall dem Hostnamen „US-BV-“ hinzu.

Zone: SRV_USBVM11_F1

Hostname: US-BV-M11

Regulärer Ausdruck: SRV_USBV([A-Za-z0-9]+)_F[12]

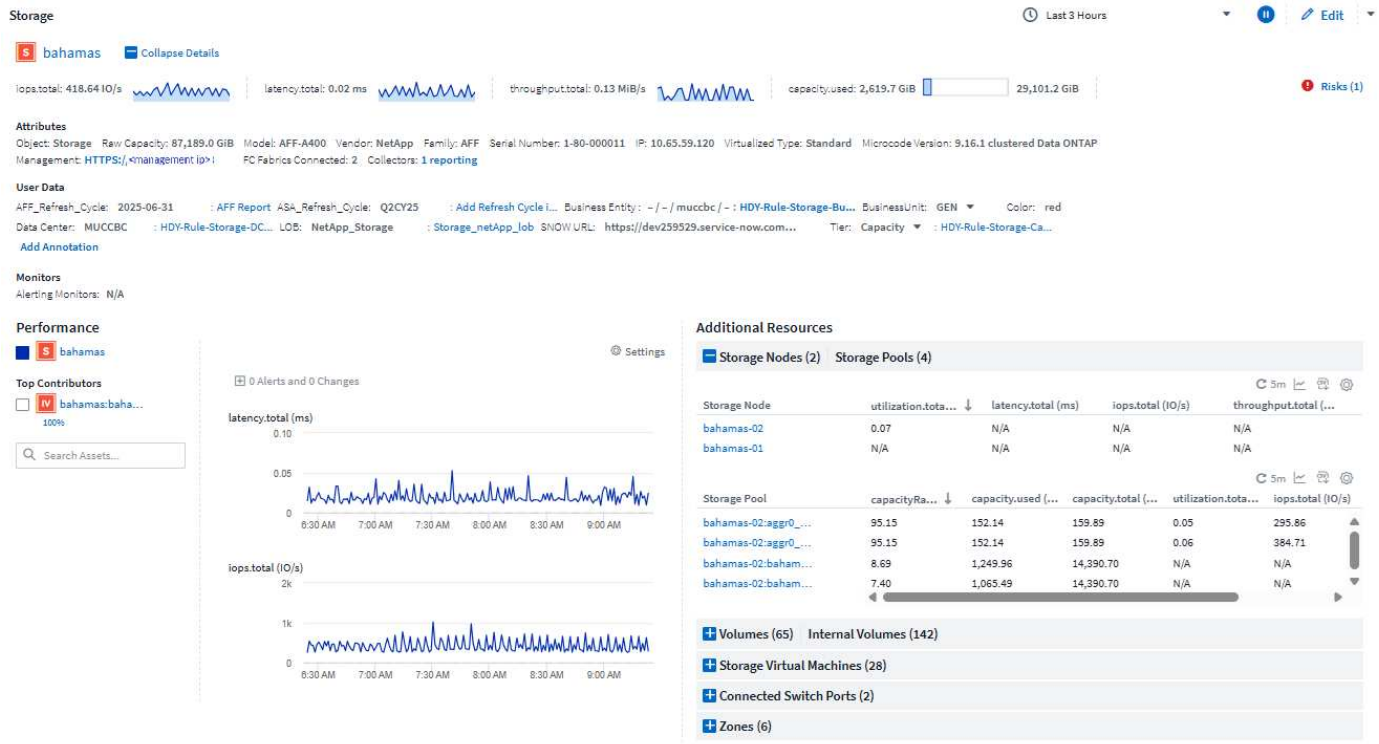
Format: US-BV-\1

Informationen zur Asset-Seite

Übersicht über die Asset-Seite

Asset-Landingpages fassen den aktuellen Status eines Assets zusammen und enthalten Links zu zusätzlichen Informationen über das Asset und die zugehörigen Assets.

Auf Zielseiten erhalten Sie eine Einzelseitenansicht des Objekts mit Informationen zu Zusammenfassung, Leistung und zugehörigen Ressourcen.



Zusammenfassung

Oben auf einer Zielseite befindet sich der erweiterbare Abschnitt „Zusammenfassung“, der mehrere Sparkline-Diagramme enthält, die aktuelle Datentrends für Dinge wie Durchsatz oder Latenz sowie Objektinformationen und -attribute und alle Monitore anzeigen, die möglicherweise Warnungen für das Objekt ausgeben.

Im Abschnitt „Zusammenfassung“ werden auch die dem Asset zugewiesenen Anmerkungen angezeigt und Sie können diese ändern.

Leistungsbereich

Im Abschnitt „Leistung“ werden Leistungsdaten für das Objekt angezeigt. Wählen Sie *Einstellungen*, um der

Anzeige zusätzliche Diagramme wie Durchsatz oder Kapazität hinzuzufügen, oder wählen Sie korrelierte oder beitragende Ressourcen aus, um deren Daten neben denen des Objekts darzustellen. Geräte, die möglicherweise Konflikte verursachen, werden auch im Abschnitt „Leistung“ aufgeführt. Die Daten in den Diagrammen werden automatisch aktualisiert, wenn Datensammler Abfragen durchführen und aktualisierte Daten erfasst werden.

Sie können dieMetriken Sie im Leistungsdiagramm für den ausgewählten Zeitraum anzeigen möchten. Klicken Sie auf das Dropdown-Menü „Einstellungen“ und wählen Sie aus den aufgelisteten Metriken aus.

Zusätzlich zu den Leistungsdaten werden auch alle Warnungen angezeigt, die innerhalb des ausgewählten Seitenzeitraums aktiv sind oder waren.

Sie können aus den folgenden Geräten auswählen, die im Abschnitt „Leistung“ aufgeführt sein können:

- Am stärksten korreliert

  Zeigt die Vermögenswerte an, die eine hohe Korrelation (Prozentsatz) mit einer oder mehreren Leistungskennzahlen zum Basisvermögenswert aufweisen.

- Top-Mitwirkende

  Zeigt die Vermögenswerte an, die (prozentual) zum Basisvermögen beitragen.

- Wichtigste Änderungen

  Vermögenswerte im Zusammenhang mit den jüngsten Änderungen.

- Workload-Konflikte

  Zeigt die Assets an, die sich auf andere gemeinsam genutzte Ressourcen wie Hosts, Netzwerke und Speicher auswirken oder von diesen beeinflusst werden. Diese werden manchmal als *gierige* und *verschlechterte* Ressourcen bezeichnet.

Abschnitt „Zusätzliche Ressourcen“

Im Abschnitt „Zusätzliche Ressourcen“ werden Datentabellen für Ressourcen angezeigt, die sich auf den aktuellen Objekttyp beziehen. Sie können diese Tabellen erweitern und reduzieren, um sich auf bestimmte Ressourcen zu konzentrieren. Wählen Sie das Zahnradsymbol aus, um vorübergehend zusätzliche Metriken oder Attribute in einer Tabelle anzuzeigen.

Benutzerdefinierte Widgets hinzufügen

Sie können jeder Asset-Seite Ihre eigenen Widgets hinzufügen. Von Ihnen hinzugefügte Widgets werden auf den Asset-Seiten für alle Objekte dieses Typs angezeigt. Wenn Sie beispielsweise einer Speicher-Asset-Seite ein benutzerdefiniertes Widget hinzufügen, wird dieses Widget auf den Asset-Seiten für alle Speicher-Assets angezeigt.

Benutzerdefinierte Widgets werden unten auf einer Zielseite unter den Abschnitten „Leistung“ und „Ressourcen“ platziert.

Arten von Asset-Seiten

Data Infrastructure Insights bietet Asset-Seiten für die folgenden Assets:

- Virtuelle Maschine
- Virtuelle Speichermaschine (SVM)
- Volumen
- Internes Volumen
- Host (einschließlich Hypervisor)
- Speicherpool
- Storage
- Datenspeicher
- Anwendung
- Speicherknoten
- Qtree
- Scheibe
- VMDK
- Hafen
- Schalten
- Stoff
- Gastgeber
- Zone

Ändern des Zeitbereichs der angezeigten Daten

Standardmäßig werden auf einer Asset-Seite die Daten der letzten drei Stunden angezeigt. Sie können den Zeitabschnitt der angezeigten Daten jedoch mithilfe einer Option ändern, die sich auf jeder Asset-Seite befindet, unabhängig vom Asset-Typ. Um den Zeitraum zu ändern, klicken Sie auf den angezeigten Zeitraum in der oberen Leiste und wählen Sie aus den folgenden Zeitsegmenten:

- Letzte 15 Minuten
- Letzte 30 Minuten
- Letzte 60 Minuten
- Letzte 2 Stunden
- Letzte 3 Stunden (dies ist die Standardeinstellung)
- Letzte 6 Stunden
- Letzte 12 Stunden
- Letzte 24 Stunden
- Letzte 2 Tage
- Letzte 3 Tage
- Letzte 7 Tage
- Letzte 14 Tage
- Letzte 30 Tage
- Benutzerdefinierter Zeitbereich

Mit dem benutzerdefinierten Zeitbereich können Sie bis zu 31 aufeinanderfolgende Tage auswählen. Sie können auch die Start- und Endzeit des Tages für diesen Bereich festlegen. Die Standardstartzeit ist 0:00 Uhr am ersten ausgewählten Tag und die Standardendzeit ist 23:59 Uhr am letzten ausgewählten Tag. Durch Klicken auf „Übernehmen“ wird der benutzerdefinierte Zeitbereich auf die Asset-Seite angewendet.

Die Informationen auf der Seite werden basierend auf dem ausgewählten Zeitraum automatisch aktualisiert. Die aktuelle Aktualisierungsrate wird in der oberen rechten Ecke des Abschnitts „Zusammenfassung“ sowie in allen relevanten Tabellen oder Widgets auf der Seite angezeigt.

Definitionen von Leistungsmetriken

Im Abschnitt „Leistung“ können basierend auf dem für das Asset ausgewählten Zeitraum mehrere Kennzahlen angezeigt werden. Jede Metrik wird in einem eigenen Leistungsdiagramm angezeigt. Sie können den Diagrammen Metriken und zugehörige Assets hinzufügen oder daraus entfernen, je nachdem, welche Daten Sie sehen möchten. Die zur Auswahl stehenden Metriken variieren je nach Asset-Typ.

Metrisch	Beschreibung
BB-Guthaben Null Rx, Tx	Gibt an, wie oft der Puffer-zu-Puffer-Guthabenzähler während des Abtastzeitraums auf Null gewechselt ist. Diese Metrik gibt an, wie oft der angeschlossene Port die Übertragung stoppen musste, weil dieser Port keine Credits mehr bereitstellen konnte.
BB Kredit Null Dauer Tx	Zeit in Millisekunden, während der das Sende-BB-Guthaben während des Abtastintervalls Null war.
Cache-Trefferquote (Gesamt, Lesen, Schreiben) %	Prozentsatz der Anfragen, die zu Cache-Treffern führen. Je höher die Anzahl der Treffer im Verhältnis zu den Zugriffen auf das Volume ist, desto besser ist die Leistung. Diese Spalte ist für Speicher-Arrays leer, die keine Cache-Trefferinformationen erfassen.
Cache-Auslastung (Gesamt) %	Gesamtprozentsatz der Cache-Anfragen, die zu Cache-Treffern führen

Rückwürfe der Klasse 3	Anzahl der beim Fibre Channel Class 3-Datentransport verworfenen Daten.
CPU-Auslastung (Gesamt) %	Menge der aktiv genutzten CPU-Ressourcen als Prozentsatz der insgesamt verfügbaren Ressourcen (über alle virtuellen CPUs).
CRC-Fehler	Anzahl der Frames mit ungültigen zyklischen Redundanzprüfungen (CRCs), die vom Port während des Abtastzeitraums erkannt wurden
Bildrate	Übertragungsbildrate in Bildern pro Sekunde (FPS)
Durchschnittliche Framegröße (Rx, Tx)	Verhältnis von Datenverkehr zu Framegröße. Mit dieser Kennzahl können Sie feststellen, ob sich im Gewebe Überkopfrahmen befinden.
Rahmengröße zu lang	Anzahl der zu langen Fibre-Channel-Datenübertragungsrahmen.
Rahmengröße zu klein	Anzahl der zu kurzen Fibre Channel-Datenübertragungsframes.
I/O-Dichte (Gesamt, Lesen, Schreiben)	Anzahl der IOPS geteilt durch die genutzte Kapazität (wie aus der letzten Bestandsabfrage der Datenquelle ermittelt) für das Volume, das interne Volume oder das Speicherelement. Gemessen in der Anzahl der E/A-Vorgänge pro Sekunde pro TB.
IOPS (Gesamt, Lesen, Schreiben)	Anzahl der Lese-/Schreib-E/A-Dienstanforderungen, die pro Zeiteinheit den E/A-Kanal oder einen Teil dieses Kanals durchlaufen (gemessen in E/A pro Sekunde)
IP-Durchsatz (Gesamt, Lesen, Schreiben)	Gesamt: Aggregierte Rate, mit der IP-Daten in Megabyte pro Sekunde gesendet und empfangen wurden.
Lesen: IP-Durchsatz (Empfangen):	Durchschnittliche Rate, mit der IP-Daten in Megabyte pro Sekunde empfangen wurden.
Schreiben: IP-Durchsatz (Übertragen):	Durchschnittliche Rate, mit der IP-Daten in Megabyte pro Sekunde übertragen wurden.
Latenz (Gesamt, Lesen, Schreiben)	Latenz (R&W): Rate, mit der Daten in einer festgelegten Zeitspanne von den virtuellen Maschinen gelesen oder auf diese geschrieben werden. Der Wert wird in Megabyte pro Sekunde gemessen.
Latenz:	Durchschnittliche Antwortzeit der virtuellen Maschinen in einem Datenspeicher.
Höchste Latenz:	Die höchste Antwortzeit der virtuellen Maschinen in einem Datenspeicher.
Verbindungsfehler	Anzahl der vom Port während des Stichprobenzeitraums erkannten Verbindungsfehler.

Link-Reset Rx, Tx	Anzahl der Zurücksetzungen der Empfangs- oder Sendeverbindung während des Abtastzeitraums. Diese Metrik stellt die Anzahl der Link-Resets dar, die vom angeschlossenen Port an diesen Port ausgegeben wurden.
Speicherauslastung (Gesamt) %	Schwellenwert für den vom Host verwendeten Speicher.
Teilweise R/W (Gesamt) %	Gesamtzahl der Male, die ein Lese-/Schreibvorgang eine Streifengrenze auf einem beliebigen Festplattenmodul in einem RAID 5-, RAID 1/0- oder RAID 0-LUN überschreitet. Im Allgemeinen sind Streifenüberschreitungen nicht vorteilhaft, da jede einen zusätzlichen E/A-Vorgang erfordert. Ein niedriger Prozentsatz weist auf eine effiziente Stripe-Elementgröße hin und ist ein Hinweis auf eine falsche Ausrichtung eines Volumes (oder einer NetApp LUN). Bei CLARiiON ist dieser Wert die Anzahl der Stripe-Übergänge geteilt durch die Gesamtzahl der IOPS.
Portfehler	Bericht über Portfehler über den Abtastzeitraum/angegebenen Zeitraum.
Signalverlustzähler	Anzahl der Signalverlustfehler. Wenn ein Signalverlustfehler auftritt, besteht keine elektrische Verbindung und es liegt ein physikalisches Problem vor.
Swapsatz (Gesamtsatz, Eingangssatz, Ausgangssatz)	Rate, mit der während des Stichprobenzeitraums Speicher von der Festplatte in den aktiven Speicher ein- und ausgelagert wird oder beides. Dieser Zähler gilt für virtuelle Maschinen.
Anzahl der Synchronisierungsverluste	Anzahl der Synchronisierungsverlustfehler. Wenn ein Synchronisierungsverlustfehler auftritt, kann die Hardware den Datenverkehr nicht verstehen oder sich darauf fixieren. Möglicherweise verwenden nicht alle Geräte dieselbe Datenrate oder die optische oder physische Verbindung ist von schlechter Qualität. Der Port muss nach jedem solchen Fehler neu synchronisiert werden, was sich auf die Systemleistung auswirkt. Gemessen in KB/Sek.
Durchsatz (Gesamt, Lesen, Schreiben)	Rate, mit der Daten als Antwort auf E/A-Dienstanforderungen in einer festgelegten Zeitspanne gesendet, empfangen oder beides werden (gemessen in MB pro Sekunde).
Timeout-Verwerfungsrahmen - Tx	Anzahl der durch Timeout verworfenen Sendeframes.
Verkehrsrate (Gesamt, Lesen, Schreiben)	Während des Stichprobenzeitraums gesendeter, empfangener oder beides empfangener Datenverkehr in Mebibyte pro Sekunde.
Verkehrsauslastung (Gesamt, Lesen, Schreiben)	Verhältnis des empfangenen/gesendeten/gesamten Datenverkehrs zur Empfangs-/Sende-/Gesamtkapazität während des Stichprobenzeitraums.

Auslastung (Gesamt, Lesen, Schreiben) %	Prozentsatz der verfügbaren Bandbreite, die für Übertragung (Tx) und Empfang (Rx) verwendet wird.
Ausstehendes Schreiben (Gesamt)	Anzahl der ausstehenden Schreib-E/A-Dienstanforderungen.

Filtern nach Objekten im Kontext

Wenn Sie ein Widget auf der Zielseite eines Assets konfigurieren, können Sie *Kontextfilter* festlegen, um nur Objekte anzuzeigen, die in direktem Zusammenhang mit dem aktuellen Asset stehen. Wenn Sie ein Widget hinzufügen, werden standardmäßig *alle* Objekte des ausgewählten Typs auf Ihrem Mandanten angezeigt. Mithilfe von Kontextfiltern können Sie nur die für Ihr aktuelles Asset relevanten Daten anzeigen.

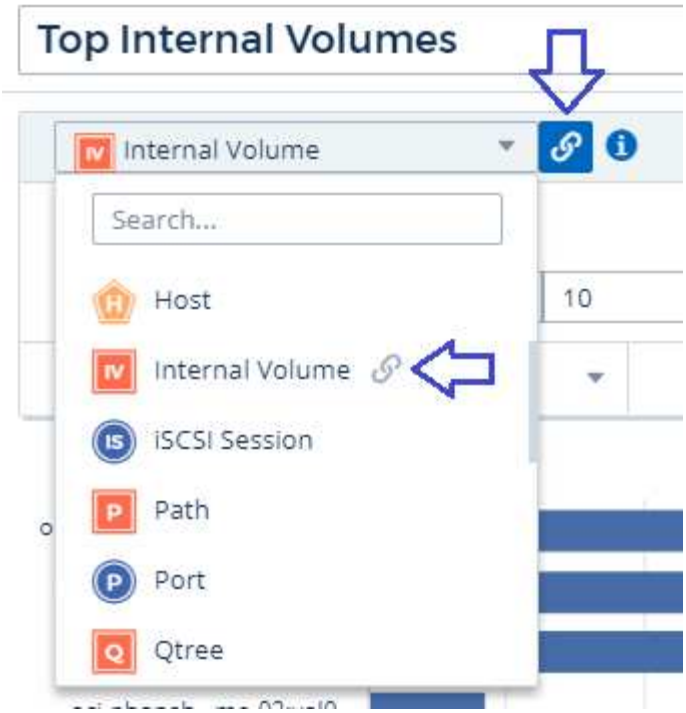
Auf den meisten Asset-Landingpages können Sie mithilfe von Widgets nach Objekten filtern, die mit dem aktuellen Asset in Zusammenhang stehen. In Filter-Dropdowns können Objekttypen, die ein Linksymbol anzeigen, im Kontext des aktuellen Assets gefiltert werden.

Sie können beispielsweise auf einer Speicher-Asset-Seite ein Balkendiagramm-Widget hinzufügen, um die höchsten IOPS auf internen Volumes nur auf diesem Speicher anzuzeigen. Wenn Sie ein Widget hinzufügen, werden standardmäßig *alle* internen Volumes Ihres Mandanten angezeigt.

Um nur interne Volumes auf dem aktuellen Speicher-Asset anzuzeigen, gehen Sie wie folgt vor:

Schritte

1. Öffnen Sie eine Asset-Seite für ein beliebiges **Speicher**-Asset.
2. Klicken Sie auf **Bearbeiten**, um die Asset-Seite im Bearbeitungsmodus zu öffnen.
3. Klicken Sie auf **Widget hinzufügen** und wählen Sie *Balkendiagramm*.
4. Wählen Sie **Internes Volumen** als Objekttyp aus, der im Balkendiagramm angezeigt werden soll. Beachten Sie, dass neben dem Objekttyp „internes Volume“ ein Linksymbol angezeigt wird. Das Symbol „Verknüpft“ ist standardmäßig aktiviert.



5. Wählen Sie *IOPS – Gesamt* und legen Sie alle gewünschten zusätzlichen Filter fest.
6. Reduzieren Sie das Feld **Roll Up**, indem Sie auf das [X] daneben klicken. Das Feld **Anzeigen** wird angezeigt.
7. Wählen Sie die Anzeige der Top 10.
8. Speichern Sie das Widget.

   Das Balkendiagramm zeigt nur die internen Volumes, die sich auf dem aktuellen Speicher-Asset befinden.

Das Widget wird auf den Asset-Seiten für alle Speicherobjekte angezeigt. Wenn der kontextbezogene Link im Widget aktiviert ist, zeigt das Balkendiagramm Daten für interne Volumes an, die sich nur auf das aktuell angezeigte Speicher-Asset beziehen.

Um die Verknüpfung der Objektdaten aufzuheben, bearbeiten Sie das Widget und klicken Sie auf das Verknüpfungssymbol neben dem Objekttyp. Der Link wird deaktiviert und das Diagramm zeigt Daten für *alle* Objekte Ihres Mandanten an.

Sie können auch**"spezielle Variablen in Widgets"** um anlagenbezogene Informationen auf Zielseiten anzuzeigen.

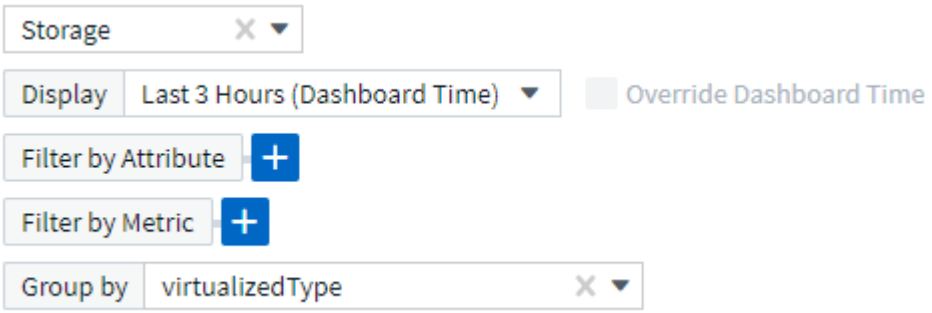
Speichervirtualisierung

Data Infrastructure Insights kann zwischen einem Speicherarray mit lokalem Speicher oder der Virtualisierung anderer Speicherarrays unterscheiden. Dadurch haben Sie die Möglichkeit, Kosten in Beziehung zu setzen und die Leistung vom Front-End bis zum Back-End Ihrer Infrastruktur zu unterscheiden.

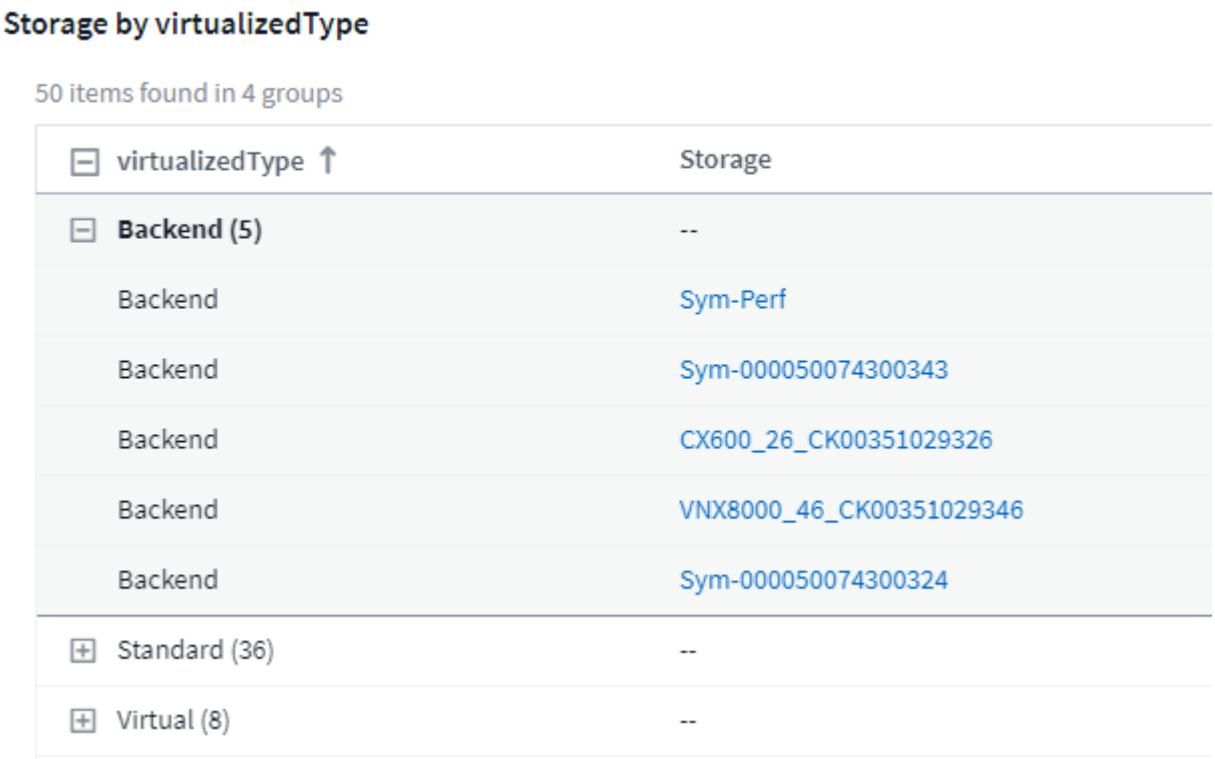
Virtualisierung in einem Tabellen-Widget

Eine der einfachsten Möglichkeiten, sich mit der Virtualisierung Ihres Speichers zu befassen, besteht darin, ein Dashboard-Tabellen-Widget zu erstellen, das den Typ „Virtualisiert“ anzeigt. Fügen Sie beim Erstellen der

Abfrage für das Widget einfach „virtualizedType“ zu Ihrer Gruppierung oder Ihrem Filter hinzu.

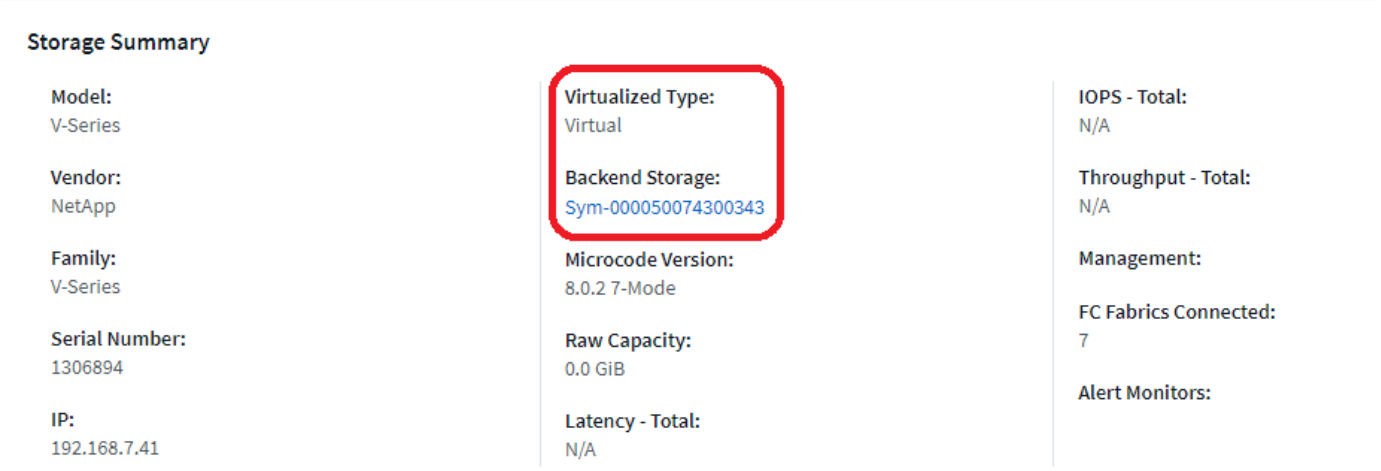


Das resultierende Tabellen-Widget zeigt Ihnen die *Standard*-, *Backend*- und *Virtual*-Speicher auf Ihrem Mandanten.



Landing Pages zeigen virtualisierte Informationen

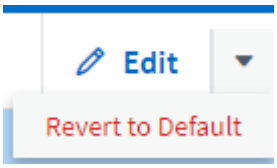
Auf der Zielseite zu Speicher, Volume, internem Volume oder Datenträger können Sie relevante Virtualisierungsinformationen sehen. Wenn Sie sich beispielsweise die Speicher-Landingpage unten ansehen, können Sie erkennen, dass es sich um einen virtuellen Speicher handelt und welches Backend-Speichersystem gilt. In allen relevanten Tabellen auf den Zielseiten werden gegebenenfalls auch Virtualisierungsinformationen angezeigt.



Vorhandene Landingpages und Dashboards

Beachten Sie, dass, wenn Sie derzeit benutzerdefinierte Zielseiten oder Dashboards auf Ihrem Mandanten haben, diese standardmäßig nicht automatisch alle Virtualisierungsinformationen anzeigen. Sie können jedoch jedes benutzerdefinierte Dashboard oder jede benutzerdefinierte Zielseite auf die Standardeinstellungen zurücksetzen (Sie müssen Ihre Anpassungen erneut implementieren) oder die entsprechenden Widgets ändern, um die gewünschten Virtualisierungsattribute oder -metriken einzuschließen.

„Auf Standard zurücksetzen“ ist in der oberen rechten Ecke eines benutzerdefinierten Dashboards oder Zielseitenbildschirms verfügbar.



Hinweise und Tipps zur Suche nach Assets und Warnungen

Zur Suche nach Daten oder Objekten in Ihrer überwachten Umgebung können mehrere Suchtechniken verwendet werden.

- **Platzhaltersuche**

  Sie können eine Platzhaltersuche mit mehreren Zeichen durchführen, indem Sie das Zeichen * verwenden. Beispielsweise würde *applic*n application* zurückgeben.

- **Bei der Suche verwendete Ausdrücke**

  Eine Phrase ist eine Gruppe von Wörtern, die von doppelten Anführungszeichen umgeben sind, beispielsweise „VNX LUN 5“. Sie können doppelte Anführungszeichen verwenden, um nach Dokumenten zu suchen, deren Namen oder Attribute Leerzeichen enthalten.

- **Boolesche Operatoren**

  Mithilfe der Booleschen Operatoren OR, AND und NOT können Sie mehrere Begriffe kombinieren, um eine komplexere Abfrage zu erstellen.

  ODER

Der ODER-Operator ist der Standard-Konjunktionsoperator.

Wenn zwischen zwei Begriffen kein Boolescher Operator steht, wird der ODER-Operator verwendet.

Der ODER-Operator verknüpft zwei Begriffe und findet ein passendes Dokument, wenn einer der Begriffe in einem Dokument vorhanden ist.

Beispielsweise sucht *storage OR netapp* nach Dokumenten, die entweder *storage* oder *netapp* enthalten.

Dokumente, die den meisten Begriffen entsprechen, erhalten hohe Punktzahlen.

UND

Mit dem UND-Operator können Sie nach Dokumenten suchen, in denen beide Suchbegriffe in einem einzigen Dokument vorkommen. Beispielsweise sucht *storage AND netapp* nach Dokumenten, die sowohl *storage* als auch *netapp* enthalten.

Sie können das Symbol **&&** anstelle des Wortes AND verwenden.

NICHT

Wenn Sie den Operator NOT verwenden, werden alle Dokumente, die den Begriff nach NOT enthalten, aus den Suchergebnissen ausgeschlossen. Beispielsweise sucht *storage NOT netapp* nach Dokumenten, die nur *storage* und nicht *netapp* enthalten.

Sie können das Symbol **!** anstelle des Wortes NOT verwenden.

Bei der Suche wird die Groß-/Kleinschreibung nicht berücksichtigt.

Suche mit indexierten Begriffen

Suchen, die mit mehr indexierten Begriffen übereinstimmen, führen zu höheren Punktzahlen.

Der Suchstring wird durch Leerzeichen in einzelne Suchbegriffe aufgeteilt. Beispielsweise wird die Suchzeichenfolge „storage aurora netapp“ in drei Schlüsselwörter aufgeteilt: „storage“, „aurora“ und „netapp“. Die Suche wird mit allen drei Begriffen durchgeführt. Die Dokumente, die den meisten dieser Begriffe entsprechen, erhalten die höchste Punktzahl. Je mehr Informationen Sie angeben, desto besser sind die Suchergebnisse. Sie können beispielsweise nach einem Speicher anhand seines Namens und Modells suchen.

Die Benutzeroberfläche zeigt die Suchergebnisse kategorienübergreifend an, mit den drei besten Ergebnissen pro Kategorie. Wenn Sie ein erwartetes Objekt nicht gefunden haben, können Sie weitere Begriffe in den Suchbegriff aufnehmen, um die Suchergebnisse zu verbessern.

Die folgende Tabelle enthält eine Liste indexierter Begriffe, die der Suchzeichenfolge hinzugefügt werden können.

Kategorie	Indizierte Begriffe
Storage	"Speicher" Name Anbieter Modell

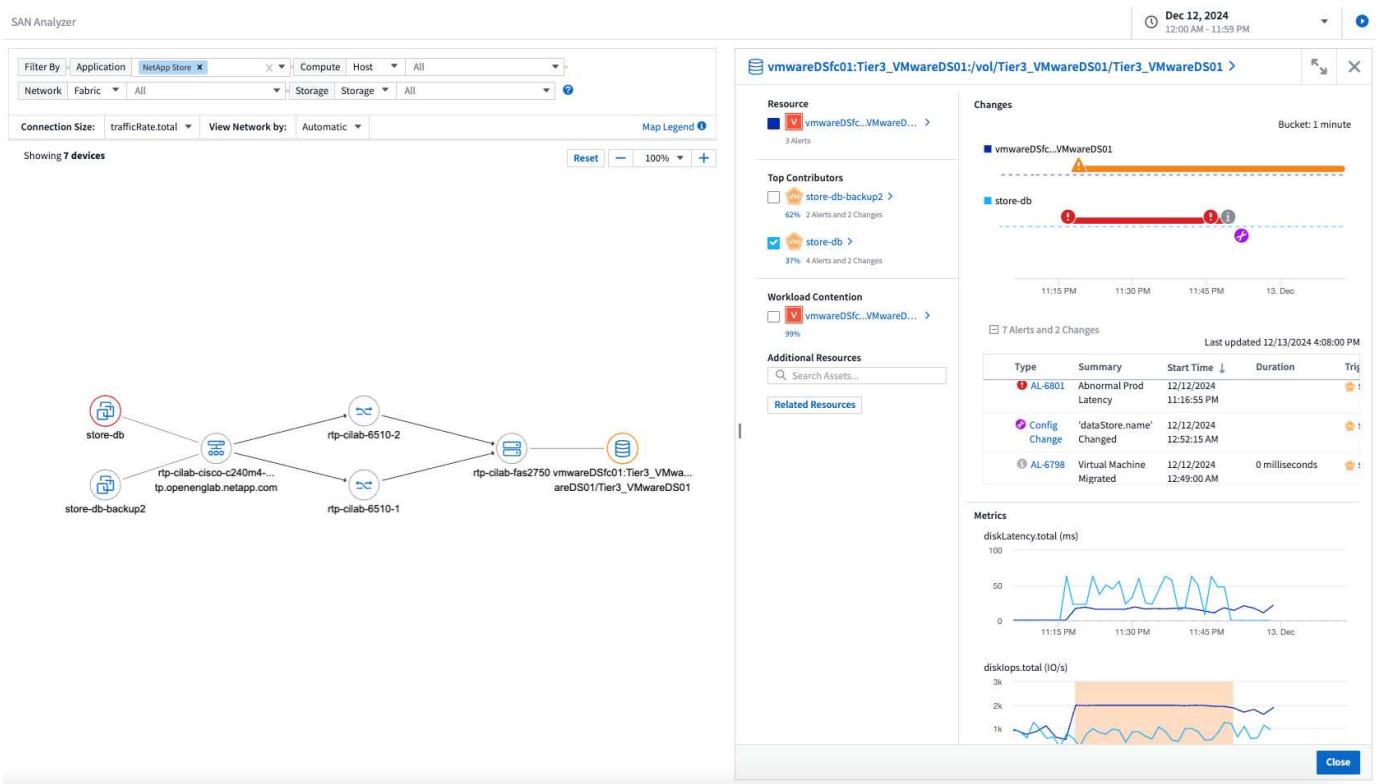
Kategorie	Indizierte Begriffe
Speicherpool	Name des „Speicherpools“ Name des Speichers IP-Adressen des Speichers Seriennummer des Speichers Speicheranbieter Speichermodell Namen aller zugehörigen internen Volumes Namen aller zugehörigen Datenträger
Internes Volumen	Name des „internen Datenträgers“ Name des Speichers IP-Adressen des Speichers Seriennummer des Speichers Speicheranbieter Speichermodell Name des Speicherpools Namen aller zugehörigen Freigaben Namen aller zugehörigen Anwendungen
Volumen	„Volume“-Name Bezeichnung Namen aller internen Volumes Name des Speicherpools Name des Speichers IP-Adressen des Speichers Seriennummer des Speichers Speicheranbieter Speichermodell
Speicherknoten	"storagenode" Name Name des Speichers IP-Adressen des Speichers Seriennummer des Speichers Speicheranbieter Speichermodell
Gastgeber	„Host“-Name IP-Adressen Namen aller zugehörigen Anwendungen
Datenspeicher	Name des „Datenspeichers“ Virtuelles Zentrum IP-Namen aller Datenträger Namen aller internen Datenträger
Virtuelle Maschinen	Name der „virtuellen Maschine“ DNS-Name IP-Adressen Name des Hosts IP-Adressen der Hostnamen aller Datenspeicher Namen aller zugehörigen Anwendungen
Switches (regulär und NPV)	"Switch" IP-Adresse WWN-Name Seriennummer Modell Domänen-ID Name des Fabric WWN des Fabric
Anwendung	"Anwendung" Name Mandant Geschäftsbereich Geschäftseinheit Projekt
Band	"Band" IP-Adresse Name Seriennummer Hersteller
Hafen	"Port" WWN-Name
Stoff	"Stoff" WWN-Name
Virtuelle Speichermaschine (SVM)	"storagevirtualmachine" Name UUID

Daten analysieren

SAN Analyzer – Übersicht

SAN spielt eine entscheidende Rolle bei der Bewältigung wichtiger Arbeitslasten, seine Komplexität kann jedoch zu erheblichen Ausfällen und Störungen für die Kunden führen. Mit dem **SAN Analyzer** von DII wird die SAN-Verwaltung einfacher und effizienter. Dieses

leistungsstarke Tool bietet End-to-End-Sichtbarkeit und bildet Abhängigkeiten von VM/Host über Netzwerk bis hin zu LUN und Speicher ab. Durch die Bereitstellung einer interaktiven Topologiekarte ermöglicht Ihnen SAN Analyzer, Probleme zu lokalisieren, Änderungen zu verstehen und das Verständnis des Datenflusses zu verbessern. Optimieren Sie die SAN-Verwaltung in komplexen IT-Umgebungen mit SAN Analyzer und erhöhen Sie Ihre Transparenz bei Block-Workloads.



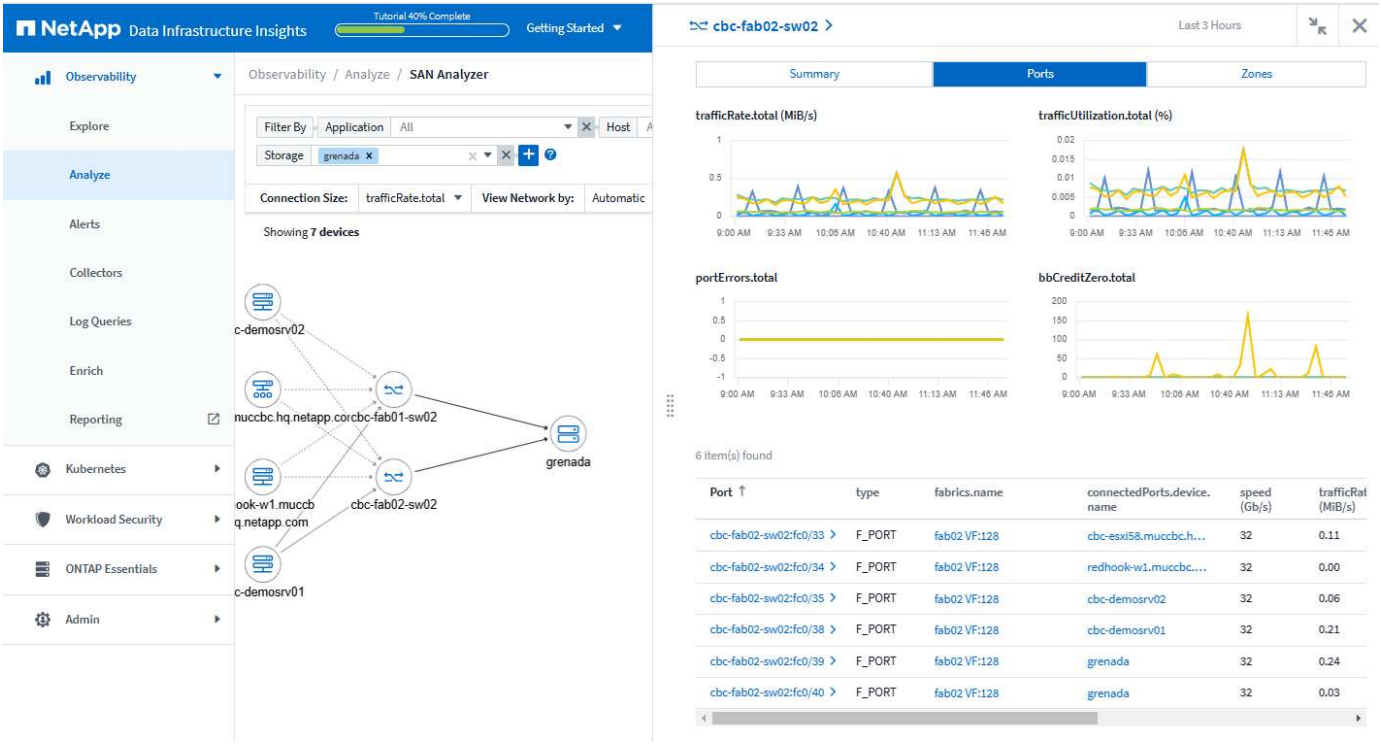
Untersuchen Sie die Verbindungen zwischen Ihren Assets

Wählen Sie **Beobachtbarkeit > Analysieren > SAN-Analysator**, um den SAN-Analysator anzuzeigen. Legen Sie einen Filter für Anwendung, Host, Fabric und/oder Speicher fest. Die Karte für die Objekte wird angezeigt und zeigt verbundene Objekte. Bewegen Sie den Mauszeiger über ein Objekt, um die Verkehrsmetriken für diese Verbindungen anzuzeigen.

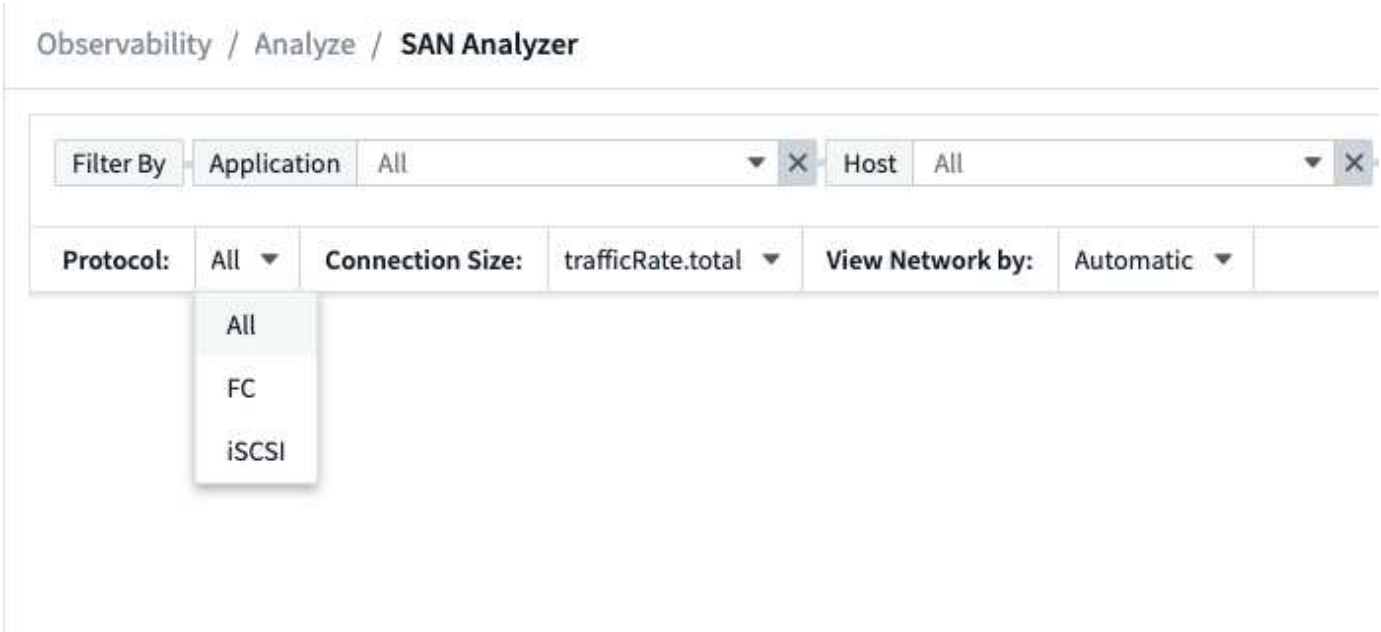
Die meisten SAN Analyzer-Filter (einschließlich derer, die Sie hinzufügen können) sind kontextbezogen. Wenn Sie in einem dieser Filter ein Objekt auswählen, werden die in den anderen Filter-Dropdowns angezeigten Auswahlmöglichkeiten im Kontext des bzw. der ausgewählten Objekte aktualisiert. Die einzigen Ausnahmen hiervon sind Anwendung, Port und Switch; diese Filter sind nicht kontextbezogen.

Durch Klicken auf ein Objekt oder eine Gruppe wird ein Slideout-Fenster geöffnet, das zusätzliche Details zum Objekt und seinen Verbindungen bietet. Das Slideout-Panel zeigt eine Zusammenfassung mit Details zum ausgewählten Objekt (z. B. IP, Hypervisor, Connected Fabrics usw., je nach Objekttyp) und Diagramme mit Metriken für das Objekt wie Latenz oder IOPS sowie gegebenenfalls Änderungen und Warnungen. Sie können bei Bedarf auch die Anzeige von Metriken für die am stärksten korrelierten Objekte in den Diagrammen auswählen.

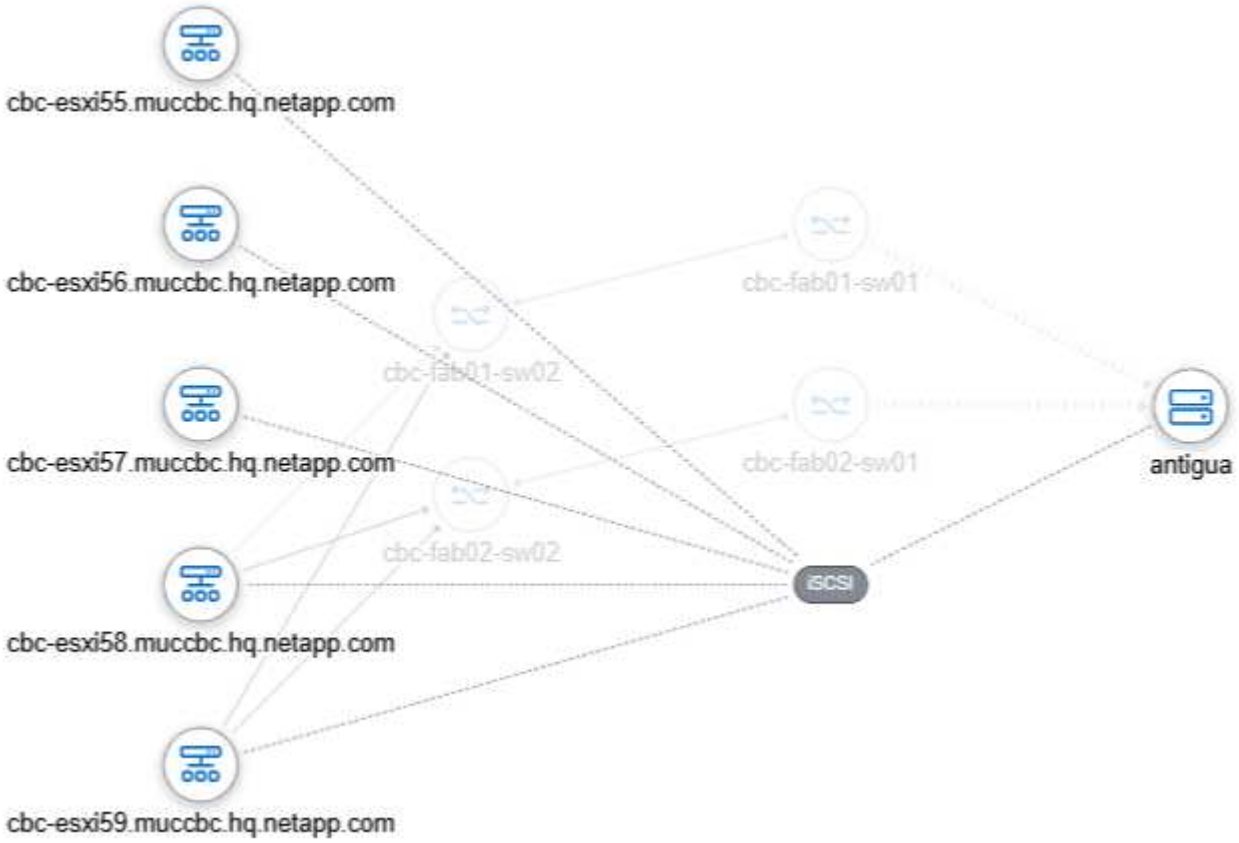
Zusätzlich zur Registerkarte „Zusammenfassung“ werden im Slideout-Bereich Registerkarten für Dinge wie Portdetails oder Zoneninformationen angezeigt, je nachdem, was für das ausgewählte Objekt zutrifft.



Wenn Ihre Umgebung über unterschiedliche Protokolle verfügt, können Sie nach iSCSI oder FC filtern:



Wenn Ihre Umgebung iSCSI-Geräte umfasst, werden durch Bewegen des Mauszeigers über das *iSCSI*-Objekt die Verbindungen hervorgehoben, die mit den entsprechenden iSCSI-Geräten in Zusammenhang stehen.



Tipps zur Fehlerbehebung

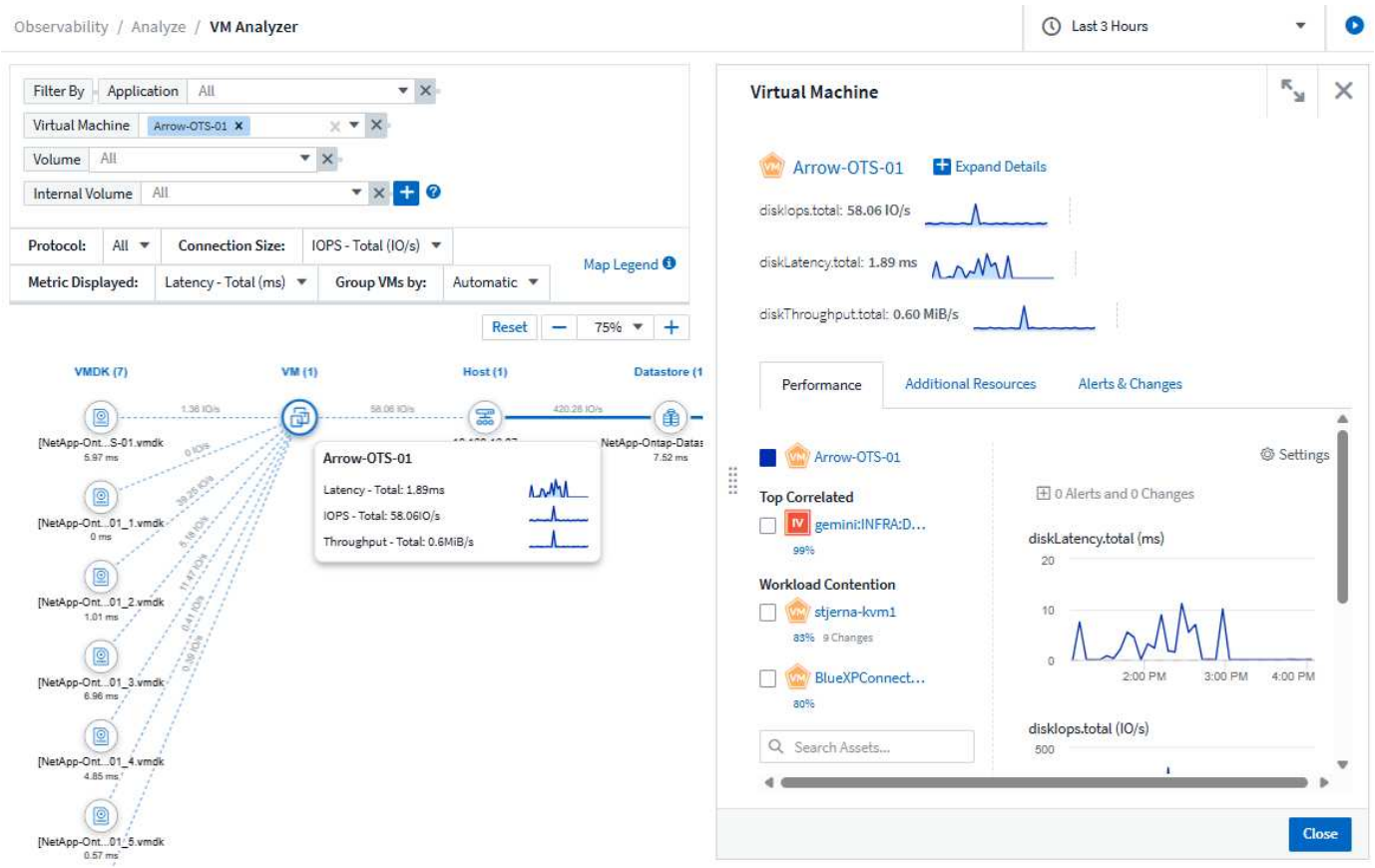
Wenn Probleme auftreten, können Sie Folgendes versuchen:

Problem:	Versuchen Sie Folgendes:
Ich sehe <0, =0 oder >0 in der Legende für Metriken wie *trafficUtilization* oder *trafficRate*.	Dies kann in sehr seltenen Fällen passieren, wenn die Metrikwerte weniger als zwei Dezimalstellen aufweisen, beispielsweise 0,000123. Eine Erweiterung des Zeitfensters kann dabei helfen, die Metrik effektiver zu analysieren.

VM Analyzer – Übersicht

Mit dem **VM Analyzer** von DII wird die Verwaltung Ihrer virtuellen Assets einfacher und effizienter. Dieses leistungsstarke Tool bietet End-to-End-Sichtbarkeit und ordnet Abhängigkeiten von VMDK/VM über Host und Datastore bis hin zu internem Volume/Volume und Speicher zu.

Durch die Bereitstellung einer interaktiven Topologiekarte ermöglicht Ihnen VM Analyzer, Probleme zu lokalisieren, Änderungen zu verstehen und das Verständnis des Datenflusses zu verbessern. Optimieren Sie die VM-Verwaltung und erhöhen Sie Ihre Transparenz bei virtuellen Workloads.



Untersuchen Sie die Verbindungen zwischen Ihren Assets

Wählen Sie **Beobachtbarkeit > Analysieren > VM-Analysator**, um den VM-Analysator anzuzeigen. Legen Sie einen Filter für Anwendung, virtuelle Maschine, Volume, internes Volume fest oder fügen Sie Ihre eigenen Filter hinzu. Die Karte für die Objekte wird angezeigt und zeigt verbundene Objekte. Bewegen Sie den Mauszeiger über ein Objekt, um die Verkehrsmetriken für diese Verbindungen anzuzeigen.

Die meisten VM Analyzer-Filter (einschließlich derer, die Sie hinzufügen können) sind kontextbezogen. Wenn Sie in einem dieser Filter ein Objekt auswählen, werden die in den anderen Filter-Dropdowns angezeigten Auswahlmöglichkeiten im Kontext mit dem bzw. den ausgewählten Objekten aktualisiert.

Durch Klicken auf ein Objekt oder eine Gruppe wird ein Slideout-Fenster geöffnet, das zusätzliche Details zum Objekt und seinen Verbindungen bietet. Das Slideout-Panel zeigt eine Zusammenfassung mit Details zum ausgewählten Objekt (z. B. Durchsatz oder Auslastung, je nach Objekttyp) sowie Diagramme mit Metriken für das Objekt wie Latenz oder IOPS. Über zusätzliche Registerkarten können Sie zugehörige zusätzliche

Ressourcen oder Änderungen und Warnungen erkunden. Sie können bei Bedarf auch die Anzeige von Metriken für die am stärksten korrelierten oder konkurrierenden Objekte in den Diagrammen auswählen.

Sehen Sie es in Aktion

Vereinfachte Fehlerbehebung mit VM Analyzer (Video), Fenster=Später lesen

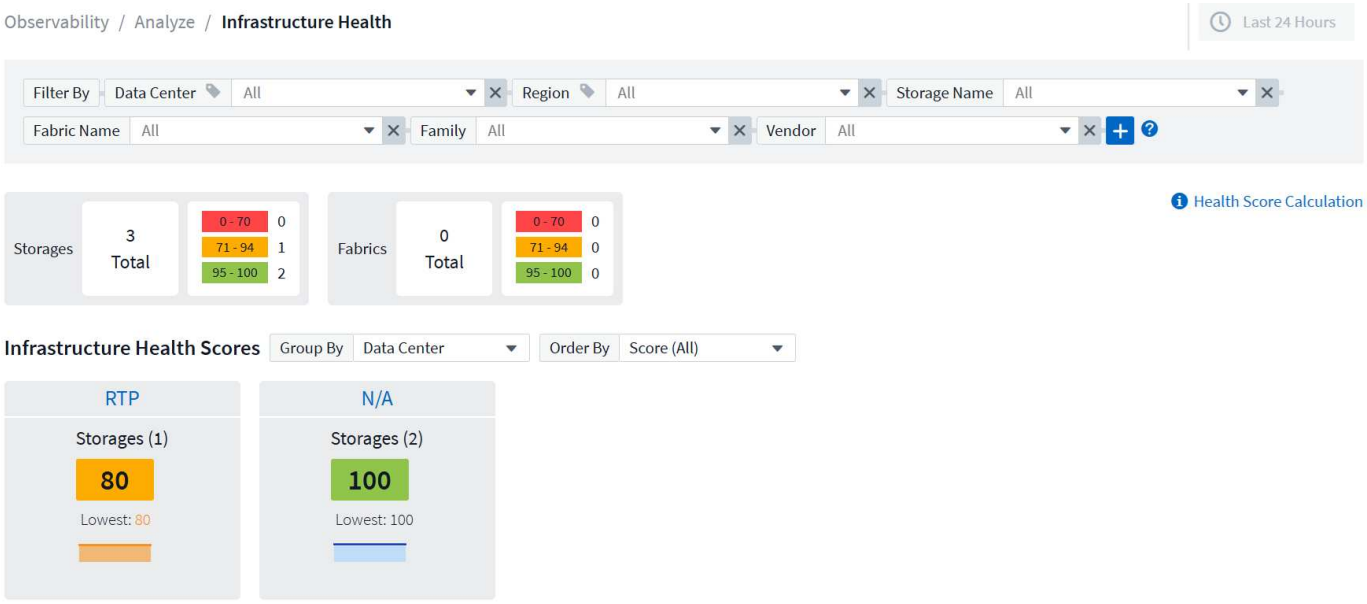
Überwachen des Infrastrukturzustands

Data Infrastructure Insights bietet eine umfassende Überwachung der Infrastrukturintegrität, die Leistung, Kapazität, Konfiguration und Komponentenstatus Ihrer Speicherumgebung verfolgt. Die Integritätswerte werden auf Grundlage von Monitorwarnungen in diesen Kategorien berechnet. So erhalten Sie einen einheitlichen Überblick über die Systemintegrität und können Probleme proaktiv lösen.

Das Dashboard „Infrastructure Health“

Die Überwachung des Infrastrukturzustands ist ein"Vorschau" Funktion und kann sich ändern.

Navigieren Sie zu **Beobachtbarkeit > Analysieren** und wählen Sie **Infrastrukturzustand** aus. Das Dashboard bietet einen Überblick über den Zustand Ihres Systems, basierend auf den unten erläuterten Alarmkategorien und Bewertungen des Monitors. Legen Sie oben Filter fest, um den Fokus Ihrer Untersuchung einzugrenzen.



Standardmäßig werden Integritätswerte nach Rechenzentrum gruppiert. Sie können die Gruppierung auswählen, die für Ihre Sitzung am besten geeignet ist.

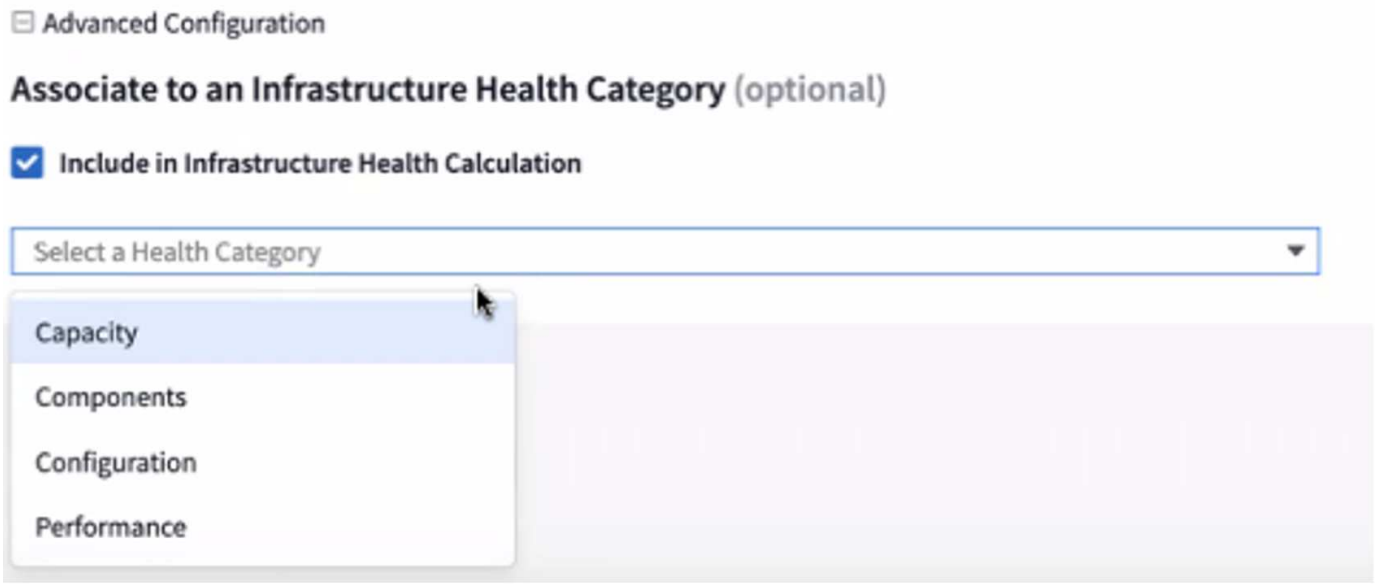
Konfigurieren Sie Monitore zur Überwachung der Infrastrukturintegrität

Die Integritätswerte werden durch Warnungen bestimmt, die für die Einbeziehung in die Berechnung der Systemintegrität konfiguriert sind.

Beim Erstellen eines Monitors für ein Infrastrukturobjekt können Sie auswählen, ob Warnungen vom Monitor in die Berechnungen einbezogen werden sollen. Erweitern Sie unten auf dem Bildschirm die erweiterte

Konfiguration und wählen Sie „In Infrastrukturzustandsberechnung einbeziehen“ aus. Wählen Sie eine Kategorie aus, auf die die Berechnung für den Monitor angewendet werden soll:

- **Komponentenzustand** – Lüfterausfall, Serviceprozessor offline usw.
- **Leistungszustand** – hohe Speicherknotenauslastung, anormale Spitze der Knotenlatenz usw.
- **Kapazitätszustand** – Speicherpoolkapazität fast voll, nicht genügend Speicherplatz für LUN-Snapshot usw.
- **Konfigurationsintegrität** – Cloud-Ebene nicht erreichbar, SnapMirror -Beziehung nicht synchron usw.



Gesundheitswerte erklärt

Die Punktzahlen werden auf einer Skala von 0 bis 100 angegeben, wobei 100 für volle Gesundheit steht. Überwachte Infrastrukturobjekte, bei denen derzeit oder in letzter Zeit Probleme aufgetreten sind, senken diesen Wert entsprechend den folgenden gewichteten Durchschnittswerten:

- Komponenten, Leistung oder Kapazität: jeweils 30 %
- Konfiguration: 10 %

Die Integritätswerte werden durch Warnungen beeinflusst, die von den Monitoren generiert werden, die Sie für die Berücksichtigung in der Berechnung der Infrastrukturintegrität konfiguriert haben. Dies geschieht auf folgende Weise:

- Kritische Warnungen senken den Gesundheitswert um das *volle* Kategoriegewicht
- Warnmeldungen senken die Punktzahl um die *Hälfte* des Kategoriegewichts.

Wenn für bestimmte Kategorien keine Meldungen vorliegen, wird der gewichtete Durchschnitt entsprechend angepasst.

Beispiel: 1 kritischer Alarm bei Komponenten (-30) und 1 Warnalarm bei Leistung (50 % von 30 = -15) ergeben einen Integritätswert von 55 (100 minus 45).

Wenn die Warnungen behoben werden, verschwinden diese Gesundheitsbewertungsminderungen allmählich und die Bewertung erholt sich innerhalb von zwei Stunden vollständig.

Berichterstattung

Übersicht über die Data Infrastructure Insights

Data Infrastructure Insights Reporting ist ein Business Intelligence-Tool, mit dem Sie vordefinierte Berichte anzeigen oder benutzerdefinierte Berichte erstellen können.

Die Berichtsfunktion ist in Data Infrastructure Insights verfügbar"Premium Edition" . Die Verfügbarkeit der Berichtsfunktion unterliegt einer Mindestspeicherkapazitätsanforderung. "Kontaktieren Sie Ihren NetApp Vertriebsmitarbeiter" für weitere Informationen.

Mit Data Infrastructure Insights -Berichten können Sie die folgenden Aufgaben ausführen:

- Ausführen eines vordefinierten Berichts
- Erstellen eines benutzerdefinierten Berichts
- Passen Sie das Format und die Übermittlungsmethode eines Berichts an
- Planen Sie die automatische Ausführung von Berichten
- E-Mail-Berichte
- Verwenden Sie Farben, um Schwellenwerte für Daten darzustellen

Data Infrastructure Insights Reporting kann benutzerdefinierte Berichte für Bereiche wie Chargeback, Verbrauchsanalyse und Prognose erstellen und bei der Beantwortung von Fragen wie den folgenden helfen:

- Welchen Bestand habe ich?
- Wo ist mein Inventar?
- Wer nutzt unsere Vermögenswerte?
- Wie hoch ist die Rückbuchung für zugewiesenen Speicher für eine Geschäftseinheit?
- Wie lange dauert es, bis ich zusätzliche Speicherkapazität benötige?
- Sind die Geschäftseinheiten auf die richtigen Speicherebenen ausgerichtet?
- Wie ändert sich die Speicherzuweisung im Laufe eines Monats, Quartals oder Jahres?

Zugriff auf Data Infrastructure Insights Reporting

Sie können auf die Data Infrastructure Insights -Berichterstellung zugreifen, indem Sie im Menü auf den Link **Berichte** klicken.

Sie werden zur Berichtsoberfläche weitergeleitet. Data Infrastructure Insights verwendet IBM Cognos Analytics für seine Berichts-Engine.

Was ist ETL?

Wenn Sie mit Reporting arbeiten, werden Sie die Begriffe „Data Warehouse“ und „ETL“ hören. ETL steht für „Extract, Transform, and Load“. Der ETL-Prozess ruft in Data Infrastructure Insights erfasste Daten ab und wandelt die Daten in ein Format um, das in der Berichterstattung verwendet werden kann. „Data Warehouse“ bezieht sich auf die gesammelten Daten, die für die Berichterstattung zur Verfügung stehen.

Der ETL-Prozess umfasst diese einzelnen Prozesse:

- **Extrahieren**: Nimmt Daten von Data Infrastructure Insights.
- **Transformieren**: Wendet Geschäftslogikregeln oder -funktionen auf die Daten an, während sie aus Data Infrastructure Insights extrahiert werden.
- **Laden**: Speichert die transformierten Daten zur Verwendung im Reporting im Data Warehouse.

Benutzerrollen für Data Infrastructure Insights Reporting

Wenn Sie über Data Infrastructure Insights Premium Edition mit Reporting verfügen, verfügt jeder Data Infrastructure Insights Benutzer auf Ihrem Mandanten auch über eine Single Sign-On-Anmeldung (SSO) bei der Reporting-Anwendung (d. h. Cognos). Klicken Sie einfach im Menü auf den Link **Berichte** und Sie werden automatisch bei Reporting angemeldet.

Ihre Benutzerrolle in Data Infrastructure Insights bestimmt Ihre Reporting-Benutzerrolle:

Rolle „Data Infrastructure Insights“	Berichtsrolle	Berichtsberechtigungen
Gast	Verbraucher	Kann Berichte anzeigen, planen und ausführen und persönliche Einstellungen wie Sprachen und Zeitzonen festlegen. Verbraucher können keine Berichte erstellen oder Verwaltungsaufgaben ausführen.
Benutzer	Autor	Kann alle Verbraucherfunktionen ausführen sowie Berichte und Dashboards erstellen und verwalten.
Administrator	Administrator	Kann alle Autorenfunktionen sowie alle Verwaltungsaufgaben ausführen, z. B. die Konfiguration von Berichten und das Herunterfahren und Neustarten von Berichtsaufgaben.

Die folgende Tabelle zeigt die für jede Berichterstellungsrolle verfügbaren Funktionen.

Funktion	Verbraucher	Autor	Administrator
Berichte auf der Registerkarte „Teaminhalte“ anzeigen	Ja	Ja	Ja
Ausführen von Berichten	Ja	Ja	Ja
Berichte planen	Ja	Ja	Ja
Externe Dateien hochladen	Nein	Ja	Ja
Jobs erstellen	Nein	Ja	Ja
Geschichten erstellen	Nein	Ja	Ja

Erstellen von Berichten	Nein	Ja	Ja
Erstellen von Paketen und Datenmodulen	Nein	Ja	Ja
Ausführen administrativer Aufgaben	Nein	Nein	Ja
HTML-Element hinzufügen/bearbeiten	Nein	Nein	Ja
Bericht mit HTML-Element ausführen	Ja	Ja	Ja
Benutzerdefiniertes SQL hinzufügen/bearbeiten	Nein	Nein	Ja
Ausführen von Berichten mit benutzerdefiniertem SQL	Ja	Ja	Ja

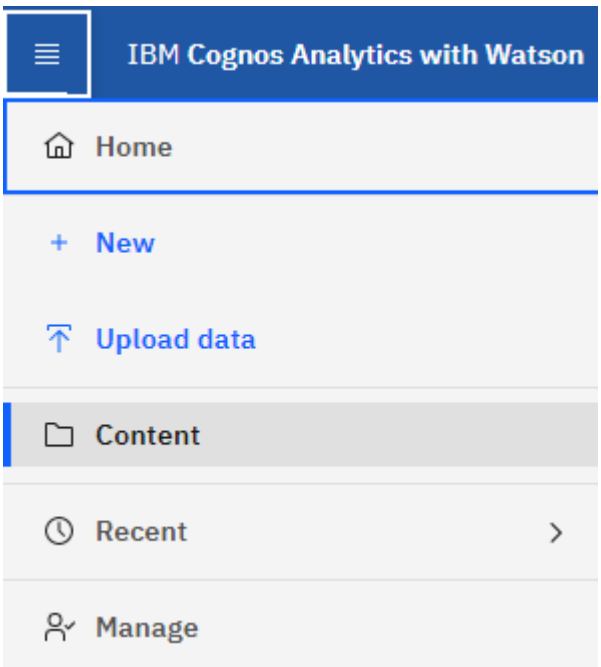
Festlegen von E-Mail-Einstellungen für Reporting (Cognos)

Wenn Sie Ihre E-Mail-Benutzereinstellungen in Data Infrastructure Insights Reporting (d. h. in der Cognos-Anwendung) ändern, sind diese Einstellungen *nur für die aktuelle Sitzung* aktiv. Wenn Sie sich bei Cognos ab- und wieder anmelden, werden Ihre E-Mail-Einstellungen zurückgesetzt.

Welche Schritte muss ich unternehmen, um meine vorhandene Umgebung für die Aktivierung von SSO vorzubereiten?

Um sicherzustellen, dass Ihre Berichte erhalten bleiben, migrieren Sie alle Berichte mit den folgenden Schritten von „Meine Inhalte“ zu „Teaminhalte“. Sie müssen dies tun, bevor Sie SSO auf Ihrem Mandanten aktivieren:

1. Navigieren Sie zu **Menü > Inhalt**



1. Erstellen Sie einen neuen Ordner in ***Team Content***
    a. Wenn mehrere Benutzer angelegt wurden, erstellen Sie bitte für jeden Benutzer einen eigenen Ordner, um das Überschreiben von Berichten mit doppelten Namen zu vermeiden.
2. Navigieren Sie zu *Meine Inhalte*
3. Wählen Sie alle Berichte aus, die Sie behalten möchten.
4. Wählen Sie in der oberen rechten Ecke des Menüs "Kopieren oder Verschieben"
5. Navigieren Sie zum neu erstellten Ordner in *Team Content*
6. Fügen Sie die Berichte mit den Schaltflächen „Kopieren nach“ oder „Verschieben nach“ in den neu erstellten Ordner ein
7. Sobald SSO für Cognos aktiviert ist, melden Sie sich bei Data Infrastructure Insights mit der E-Mail-Adresse an, die Sie zum Erstellen Ihres Kontos verwendet haben.
8. Navigieren Sie in Cognos zum Ordner „Team Content“ und kopieren oder verschieben Sie die zuvor gespeicherten Berichte zurück in „Meine Inhalte“.

Vordefinierte Berichte leicht gemacht

Data Infrastructure Insights Reporting umfasst vordefinierte Berichte, die eine Reihe gängiger Berichtsanforderungen erfüllen und wichtige Erkenntnisse liefern, die die Beteiligten benötigen, um fundierte Entscheidungen über ihre Speicherinfrastruktur zu treffen.

Die Berichtsfunktion ist in Data Infrastructure Insights verfügbar"Premium Edition" .

Sie können vordefinierte Berichte aus dem Data Infrastructure Insights Reporting Portal erstellen, sie per E-Mail an andere Benutzer senden und sie sogar ändern. Mehrere Berichte ermöglichen Ihnen das Filtern nach Gerät, Geschäftseinheit oder Ebene. Die Berichtstools verwenden IBM Cognos als Grundlage und bieten Ihnen zahlreiche Möglichkeiten zur Datenpräsentation.

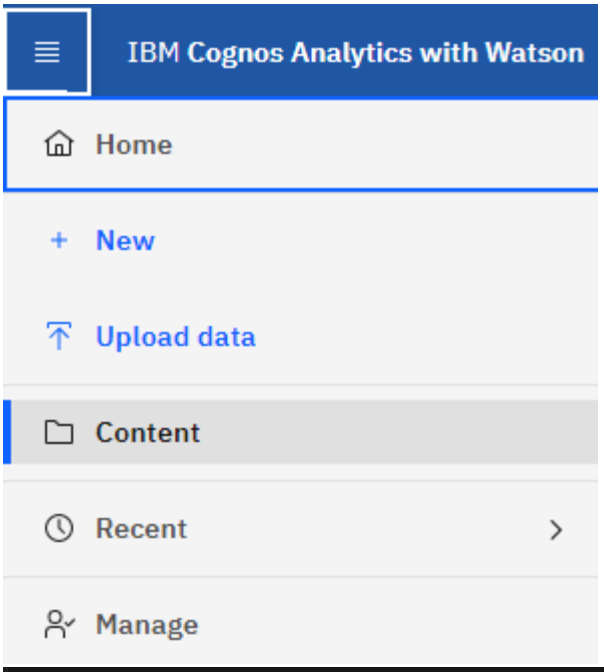
Die vordefinierten Berichte zeigen Ihre Daten zu Inventar, Speicherkapazität, Rückbuchung, Leistung, Speichereffizienz und Cloud-Kosten. Sie können diese vordefinierten Berichte ändern und Ihre Änderungen speichern.

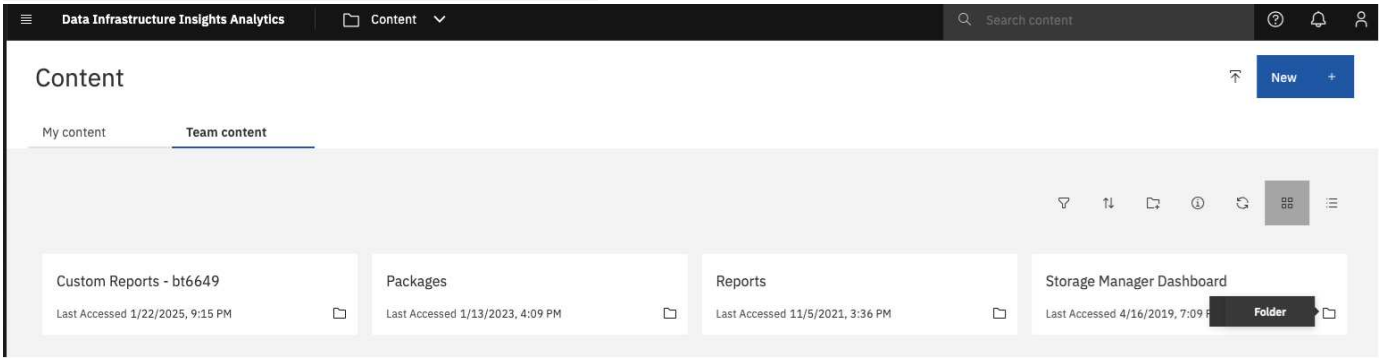
Sie können Berichte in verschiedenen Formaten erstellen, darunter HTML, PDF, CSV, XML und Excel.

Navigieren zu vordefinierten Berichten

Wenn Sie das Reporting-Portal öffnen, ist der Ordner „Team Content“ der Ausgangspunkt für die Auswahl der Art von Informationen, die Sie in den Data Infrastructure Insights -Berichten benötigen.

1. Wählen Sie im linken Navigationsbereich **Inhalt > Teaminhalt** aus.
2. Wählen Sie **Berichte**, um auf die vordefinierten Berichte zuzugreifen.





Verwenden vordefinierter Berichte zum Beantworten häufiger Fragen

Die folgenden vordefinierten Berichte sind unter **Teaminhalte > Berichte** verfügbar.

Kapazität und Leistung der Anwendungsdienstebene

Der Bericht zur Service-Level-Kapazität und -Leistung von Anwendungen bietet einen umfassenden Überblick über Ihre Anwendungen. Sie können diese Informationen für die Kapazitätsplanung oder einen Migrationsplan verwenden.

Rückbuchung

Der Chargeback-Bericht bietet Informationen zum Chargeback der Speicherkapazität und zur Verantwortlichkeit nach Hosts, Anwendungen und Geschäftseinheiten und enthält sowohl aktuelle als auch historische Daten.

Um eine Doppelzählung zu vermeiden, schließen Sie keine ESX-Server ein, überwachen Sie nur die VMs.

Datenquellen

Der Bericht „Datenquellen“ zeigt alle auf Ihrer Site installierten Datenquellen, den Status der Datenquelle (Erfolg/Fehler) und Statusmeldungen. Der Bericht enthält Informationen dazu, wo Sie mit der Fehlerbehebung bei Datenquellen beginnen können. Fehlerhafte Datenquellen beeinträchtigen die Genauigkeit der Berichterstattung und die allgemeine Benutzerfreundlichkeit des Produkts.

ESX vs. VM-Leistung

Der Bericht „ESX vs. VM-Leistung“ bietet einen Vergleich von ESX-Servern und VMs und zeigt durchschnittliche und Spitzen-IOPs, Durchsatz sowie Latenz und Auslastung für ESX-Server und VMs. Um eine Doppelzählung zu vermeiden, schließen Sie die ESX-Server aus und schließen Sie nur die VMs ein. Eine aktualisierte Version dieses Berichts ist im NetApp Storage Automation Store verfügbar.

Stoffübersicht

Der Fabric-Zusammenfassungsbericht identifiziert Switches und Switch-Informationen, einschließlich Portanzahl, Firmware-Versionen und Lizenzstatus. Der Bericht enthält keine NPV-Switch-Ports.

Host-HBAs

Der Host-HBA-Bericht bietet einen Überblick über die Hosts in der Umgebung und gibt den Anbieter, das Modell und die Firmware-Version der HBAs sowie die Firmware-Ebene der Switches an, mit denen sie verbunden sind. Dieser Bericht kann verwendet werden, um die Firmware-Kompatibilität zu analysieren, wenn ein Firmware-Upgrade für einen Switch oder einen HBA geplant wird.

Kapazität und Leistung des Host-Service-Levels

Der Bericht „Host Service Level Capacity and Performance“ bietet einen Überblick über die Speicherauslastung nach Host für Nur-Block-Anwendungen.

Host-Zusammenfassung

Der Host-Zusammenfassungsbericht bietet einen Überblick über die Speicherauslastung jedes ausgewählten Hosts mit Informationen zu Fibre Channel- und iSCSI-Hosts. Mit dem Bericht können Sie Ports und Pfade, die Fibre Channel- und ISCSI-Kapazität sowie die Anzahl der Verstöße vergleichen.

Lizenzdetails

Der Bericht „Lizenzdetails“ zeigt die Menge der Ressourcen an, für die Sie über eine Lizenz verfügen, und zwar für alle Sites mit aktiven Lizenzen. Der Bericht zeigt auch eine Zusammenfassung der tatsächlichen Menge aller Sites mit aktiven Lizenzen. Die Summierung kann Überschneidungen von Speicher-Arrays enthalten, die von mehreren Servern verwaltet werden.

Zugeordnete, aber nicht maskierte Volumes

Der Bericht „Zugeordnete, aber nicht maskierte Volumes“ listet die Volumes auf, deren logische Gerätenummer (LUN) für die Verwendung durch einen bestimmten Host zugeordnet wurde, für diesen Host jedoch nicht maskiert ist. In einigen Fällen kann es sich dabei um stillgelegte LUNs handeln, die demaskiert wurden. Auf nicht maskierte Volumes kann von jedem Host aus zugegriffen werden, wodurch sie anfällig für Datenbeschädigungen sind.

NetApp Kapazität und Performance

Der NetApp Kapazitäts- und Leistungsbericht bietet globale Daten zur zugewiesenen, genutzten und zugesagten Kapazität mit Trend- und Leistungsdaten zur NetApp -Kapazität.

Scorecard

Der Scorecard-Bericht bietet eine Zusammenfassung und den allgemeinen Status aller von Data Infrastructure Insights erworbenen Assets. Der Status wird durch grüne, gelbe und rote Flaggen angezeigt:

- Grün zeigt den Normalzustand an
- Gelb weist auf ein potenzielles Problem in der Umgebung hin
- Rot weist auf ein Problem hin, das Aufmerksamkeit erfordert

Alle Felder im Bericht werden im mit dem Bericht bereitgestellten Datenwörterbuch beschrieben.

Speicherübersicht

Der Speicherzusammenfassungsbericht bietet eine globale Zusammenfassung der verwendeten und ungenutzten Kapazitätsdaten für Roh- und zugewiesene Speicherpools und Volumes. Dieser Bericht bietet einen Überblick über alle erkannten Speicher.

VM-Kapazität und -Leistung

Beschreibt die Umgebung der virtuellen Maschine (VM) und ihre Kapazitätsnutzung. Um bestimmte Daten anzuzeigen, beispielsweise wann VMs heruntergefahren wurden, müssen VM-Tools aktiviert sein.

VM-Pfade

Der Bericht „VM-Pfade“ liefert Daten zur Speicherkapazität und Leistungsmetriken für die virtuelle Maschine, die auf dem Host ausgeführt wird, die Hosts, die auf die freigegebenen Volumes zugreifen, den aktiven Zugriffspfad und die Kapazitätszuweisung und -nutzung.

HDS-Kapazität nach Thin Pool

Der Bericht „HDS-Kapazität nach Thin Pool“ zeigt die Menge der nutzbaren Kapazität eines Thin Provisioning-Speicherpools.

NetApp -Kapazität nach Aggregat

Der Bericht „NetApp -Kapazität nach Aggregat“ zeigt den gesamten Rohspeicherplatz, den gesamten, den genutzten, den verfügbaren und den zugesicherten Speicherplatz der Aggregate an.

Symmetrix-Kapazität durch Thick Array

Der Bericht „Symmetrix-Kapazität nach Thick-Array“ zeigt Rohkapazität, nutzbare Kapazität, freie Kapazität, zugeordnete, maskierte und gesamte freie Kapazität.

Symmetrix-Kapazität nach Thin Pool

Der Bericht „Symmetrix-Kapazität nach Thin Pool“ zeigt Rohkapazität, nutzbare Kapazität, genutzte Kapazität, freie Kapazität, genutzten Prozentsatz, abonnierte Kapazität und Abonnementrate.

XIV Kapazität nach Array

Der XIV-Kapazitätsbericht nach Array zeigt die verwendete und ungenutzte Kapazität für das Array.

XIV Kapazität nach Pool

Der XIV-Kapazitätsbericht nach Pool zeigt die genutzte und ungenutzte Kapazität für Speicherpools.

Storage Manager-Dashboard

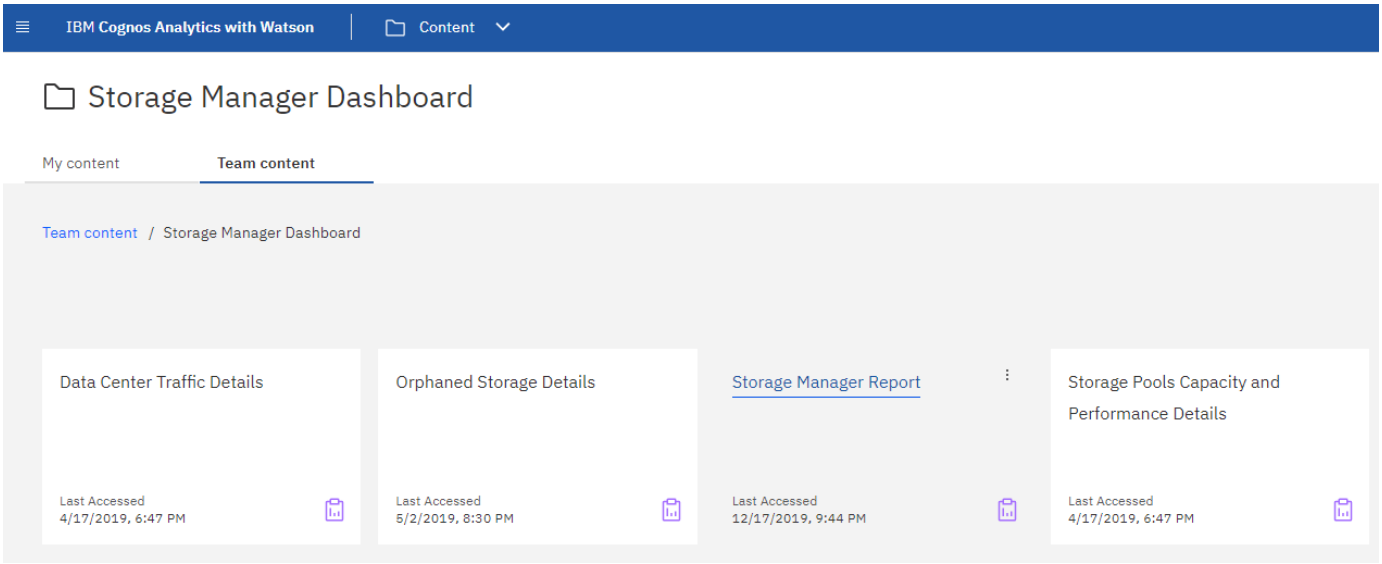
Das Storage Manager Dashboard bietet Ihnen eine zentrale Visualisierung, mit der Sie

die Ressourcennutzung im Zeitverlauf mit den akzeptablen Bereichen und den Aktivitätstagen der vorherigen Tage vergleichen und gegenüberstellen können. Indem nur die wichtigsten Leistungskennzahlen für Ihre Speicherdienste angezeigt werden, können Sie Entscheidungen zur Wartung Ihrer Rechenzentren treffen.

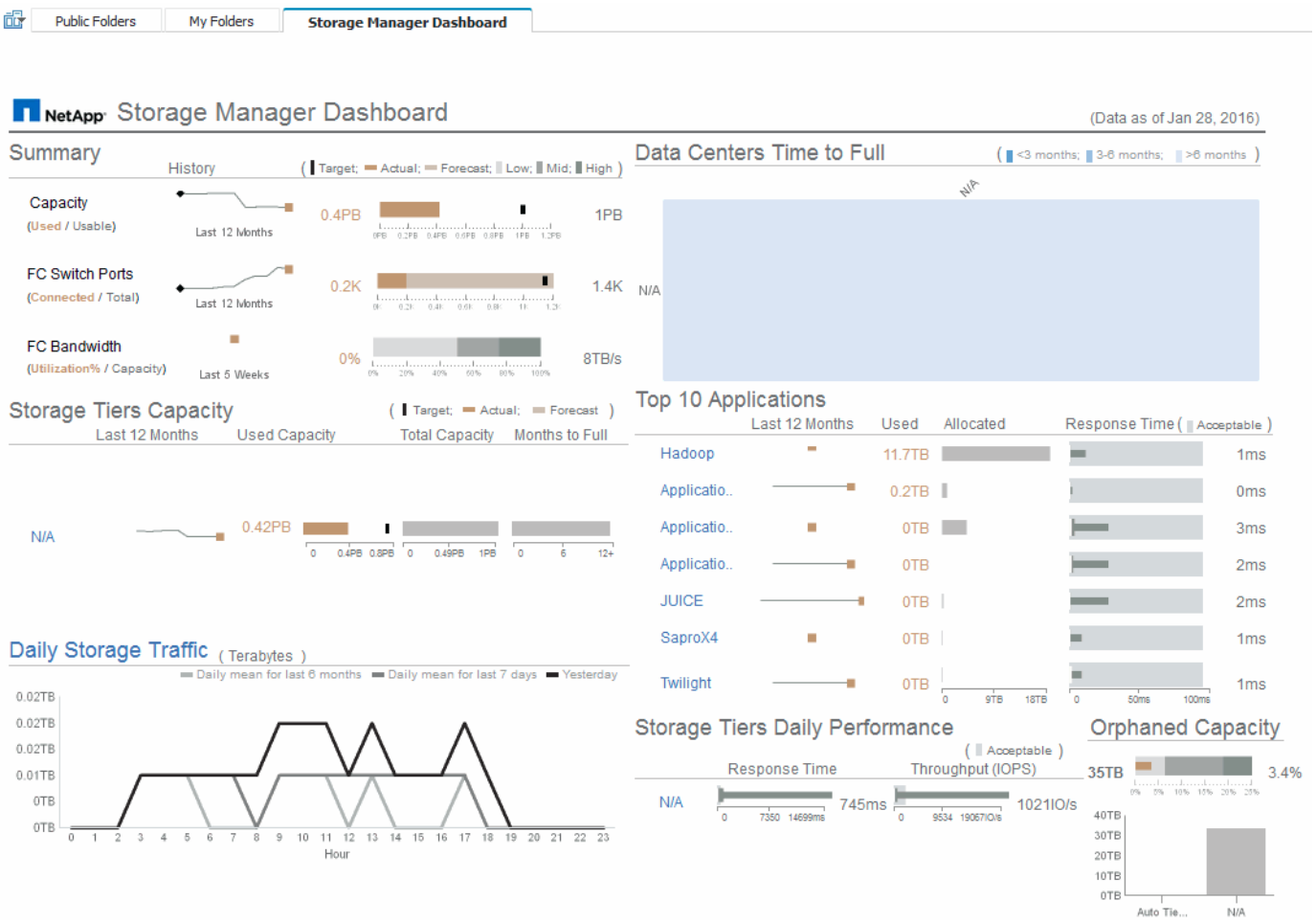
Die Berichtsfunktion ist in Data Infrastructure Insights verfügbar"Premium Edition" .

Zusammenfassung

Wenn Sie unter „Teaminhalte“ das „Storage Manager Dashboard“ auswählen, erhalten Sie mehrere Berichte mit Informationen zu Ihrem Datenverkehr und Speicher.



Für eine Übersicht auf einen Blick besteht der **Storage Manager-Bericht** aus sieben Komponenten, die Kontextinformationen zu vielen Aspekten Ihrer Speicherumgebung enthalten. Sie können die Aspekte Ihrer Speicherdienste genauer untersuchen, um eine eingehende Analyse des Abschnitts durchzuführen, der Sie am meisten interessiert.



Diese Komponente zeigt die verwendete Speicherkapazität im Vergleich zur nutzbaren Speicherkapazität, die Gesamtzahl der Switch-Ports im Vergleich zur Anzahl der verbundenen Switch-Ports und die Gesamtauslastung der verbundenen Switch-Ports im Vergleich zur Gesamtbandbreite sowie die Entwicklung dieser Werte im Zeitverlauf. Sie können die tatsächliche Nutzung im Vergleich zu den niedrigen, mittleren und hohen Bereichen anzeigen. So können Sie die Nutzung zwischen Prognosen und Ihren gewünschten tatsächlichen Werten auf der Grundlage eines Ziels vergleichen und gegenüberstellen. Für Kapazität und Switch-Ports können Sie dieses Ziel konfigurieren. Die Prognose basiert auf einer Extrapolation der aktuellen Wachstumsrate und des von Ihnen festgelegten Datums. Wenn die prognostizierte genutzte Kapazität, die auf dem Prognosedatum für die zukünftige Nutzung basiert, das Ziel überschreitet, wird neben „Kapazität“ eine Warnung (durchgezogener roter Kreis) angezeigt.

Speicherebenenkapazität

Diese Komponente zeigt die genutzte Kapazität der Stufe im Vergleich zur der Stufe zugewiesenen Kapazität. Dies gibt an, wie die genutzte Kapazität über einen Zeitraum von 12 Monaten zunimmt oder abnimmt und wie viele Monate bis zur vollständigen Auslastung verbleiben. Die Kapazitätsauslastung wird mit den angegebenen Werten für die tatsächliche Auslastung, die Auslastungsprognose und ein von Ihnen konfigurierbares Kapazitätsziel angezeigt. Wenn die prognostizierte genutzte Kapazität, die auf dem Prognosedatum für die zukünftige Nutzung basiert, die Zielkapazität überschreitet, wird neben einer Stufe eine Warnung (durchgezogener roter Kreis) angezeigt.

Sie können auf eine beliebige Ebene klicken, um den Bericht „Kapazitäts- und Leistungsdetails der Speicherpools“ anzuzeigen. Darin werden freie und genutzte Kapazitäten, die Anzahl der Tage bis zur vollständigen Belegung sowie Leistungsdetails (IOPS und Reaktionszeit) für alle Pools in der ausgewählten Ebene angezeigt. Sie können in diesem Bericht auch auf einen beliebigen Speicher- oder Speicherpoolnamen klicken, um die Asset-Seite mit einer Zusammenfassung des aktuellen Status dieser Ressource anzuzeigen.

Täglicher Speicherverkehr

Diese Komponente zeigt die Leistung der Umgebung und ob es im Vergleich zu den letzten sechs Monaten zu starkem Wachstum, Änderungen oder potenziellen Problemen kommt. Außerdem wird der durchschnittliche Verkehr im Vergleich zum Verkehr der letzten sieben Tage und des Vortages angezeigt. Sie können alle Anomalien in der Leistung der Infrastruktur visualisieren, da Informationen bereitgestellt werden, die sowohl zyklische (letzte sieben Tage) als auch saisonale Schwankungen (letzte sechs Monate) hervorheben.

Sie können auf den Titel (Täglicher Speicherverkehr) klicken, um den Bericht „Speicherverkehrsdetails“ anzuzeigen, der die Heatmap des stündlichen Speicherverkehrs des vorherigen Tages für jedes Speichersystem zeigt. Klicken Sie in diesem Bericht auf einen beliebigen Speichernamen, um die Asset-Seite mit einer Zusammenfassung des aktuellen Status dieser Ressource anzuzeigen.

Zeit bis zur Auslastung von Rechenzentren

Diese Komponente zeigt alle Rechenzentren im Vergleich zu allen Ebenen und wie viel Kapazität in jedem Rechenzentrum für jede Speicherebene basierend auf den prognostizierten Wachstumsraten verbleibt. Die Kapazitätsstufe wird in Blau angezeigt. Je dunkler die Farbe, desto weniger Zeit bleibt der Stufe am Standort, bevor sie voll ist.

Sie können auf einen Abschnitt einer Ebene klicken, um den Bericht „Tage bis zur vollständigen Belegung der Speicherpools“ anzuzeigen. Darin werden die Gesamtkapazität, die freie Kapazität und die Anzahl der Tage bis zur vollständigen Belegung für alle Pools in der ausgewählten Ebene und im Rechenzentrum angezeigt. Klicken Sie in diesem Bericht auf einen beliebigen Speicher- oder Speicherpoolnamen, um die Asset-Seite mit einer Zusammenfassung des aktuellen Status dieser Ressource anzuzeigen.

Top 10 Anwendungen

Diese Komponente zeigt die Top 10-Anwendungen basierend auf der verwendeten Kapazität. Unabhängig davon, wie die Ebene die Daten organisiert, zeigt dieser Bereich die aktuell genutzte Kapazität und den Anteil der Infrastruktur an. Sie können die Bandbreite der Benutzererfahrung der letzten sieben Tage visualisieren, um zu sehen, ob die Verbraucher akzeptable (oder, noch wichtiger, inakzeptable) Reaktionszeiten erlebt haben.

In diesem Bereich werden auch Trends angezeigt, die darauf hinweisen, ob die Anwendungen ihre Leistungs-Servicelevelziele (SLO) erfüllen. Sie können die minimale Antwortzeit der vorherigen Woche, das erste Quartil, das dritte Quartil und die maximale Antwortzeit anzeigen, wobei ein Median gegenüber einem akzeptablen SLO angezeigt wird, das Sie konfigurieren können. Wenn die mittlere Antwortzeit für eine Anwendung außerhalb des akzeptablen SLO-Bereichs liegt, wird neben der Anwendung eine Warnung (durchgezogener roter Kreis) angezeigt. Sie können auf eine Anwendung klicken, um die Asset-Seite mit einer Zusammenfassung des aktuellen Status dieser Ressource anzuzeigen.

Tägliche Leistung der Speicherebenen

Diese Komponente zeigt eine Zusammenfassung der Leistung der Ebene hinsichtlich Reaktionszeit und IOPS für die letzten sieben Tage. Diese Leistung wird mit einem SLO verglichen, das Sie konfigurieren können. So können Sie erkennen, ob die Möglichkeit besteht, Ebenen zu konsolidieren, die von diesen Ebenen bereitgestellten Arbeitslasten neu auszurichten oder Probleme mit bestimmten Ebenen zu identifizieren. Wenn die mittlere Antwortzeit oder der mittlere IOPS außerhalb des akzeptablen SLO-Bereichs liegt, wird neben einer Stufe eine Warnung (durchgezogener roter Kreis) angezeigt.

Sie können auf einen Tier-Namen klicken, um den Bericht „Kapazitäts- und Leistungsdetails der Speicherpools“ anzuzeigen. Darin werden freie und genutzte Kapazitäten, die Anzahl der Tage bis zur vollständigen Befüllung sowie Leistungsdetails (IOPS und Reaktionszeit) für alle Pools im ausgewählten Tier angezeigt. Klicken Sie in diesem Bericht auf einen beliebigen Speicher oder Speicherpool, um die Asset-Seite

mit einer Zusammenfassung des aktuellen Status dieser Ressource anzuzeigen.

Verwaiste Kapazität

Diese Komponente zeigt die gesamte verwaiste Kapazität und die verwaiste Kapazität nach Ebene an, vergleicht sie mit akzeptablen Bereichen für die gesamte nutzbare Kapazität und zeigt die tatsächlich verwaiste Kapazität an. Verwaiste Kapazität wird durch Konfiguration und Leistung definiert. Durch Konfiguration verwaister Speicher beschreibt eine Situation, in der einem Host Speicher zugewiesen ist. Die Konfiguration wurde jedoch nicht ordnungsgemäß durchgeführt und der Host kann nicht auf den Speicher zugreifen. Von „verwaist durch Leistung“ spricht man, wenn der Speicher korrekt für den Zugriff durch einen Host konfiguriert ist. Es gab jedoch keinen Speicherverkehr.

Der horizontale gestapelte Balken zeigt die akzeptablen Bereiche. Je dunkler das Grau, desto inakzeptabler ist die Situation. Die tatsächliche Situation wird durch den schmalen bronzenen Balken dargestellt, der die tatsächlich verwaiste Kapazität anzeigt.

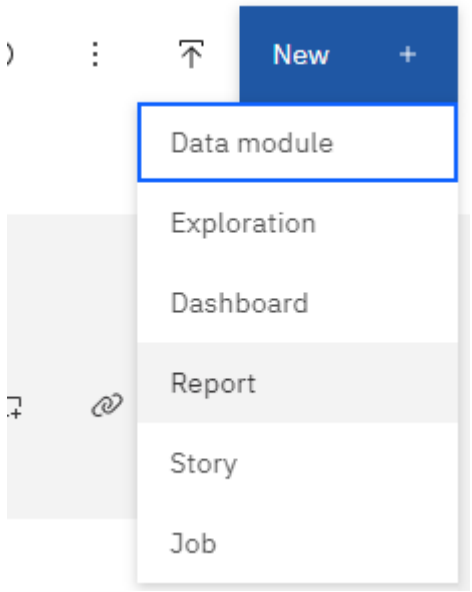
Sie können auf eine Ebene klicken, um den Bericht „Verwaiste Speicherdetails“ anzuzeigen. Darin sind alle Volumes aufgeführt, die aufgrund ihrer Konfiguration und Leistung für die ausgewählte Ebene als verwaist identifiziert wurden. Klicken Sie in diesem Bericht auf einen beliebigen Speicher, Speicherpool oder Datenträger, um die Asset-Seite mit einer Zusammenfassung des aktuellen Status dieser Ressource anzuzeigen.

Erstellen eines Berichts (Beispiel)

Verwenden Sie die Schritte in diesem Beispiel, um einen einfachen Bericht über die physische Kapazität von Speicher und Speicherpools in mehreren Rechenzentren zu erstellen.

Schritte

1. Navigieren Sie zu **Menü > Inhalt > Teaminhalt > Berichte**
2. Wählen Sie oben rechts auf dem Bildschirm **[Neu +]**
3. Wählen Sie **Bericht**



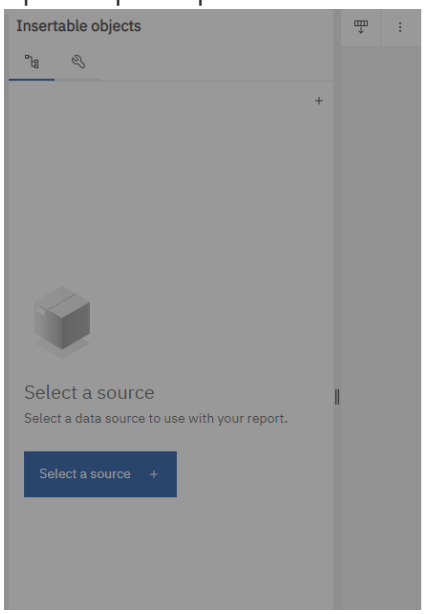
4. Wählen Sie auf der Registerkarte **Vorlagen** *Leer*

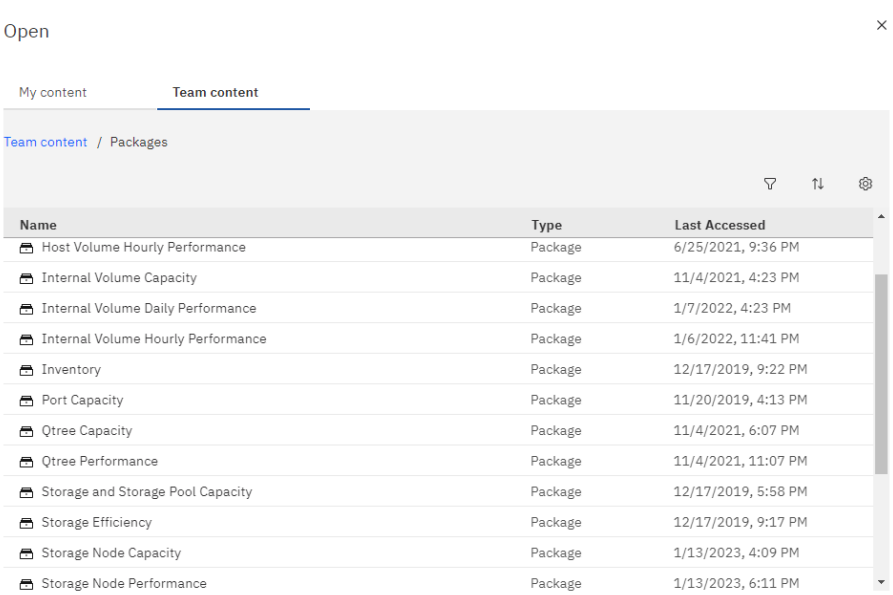
Die Registerkarten Quelle und Daten werden angezeigt

5. Öffnen **Quelle auswählen +**
6. Öffnen Sie unter **Teaminhalte Pakete**

   Es wird eine Liste der verfügbaren Pakete angezeigt.

7. Wählen Sie *Speicher und Speicherpoolkapazität*





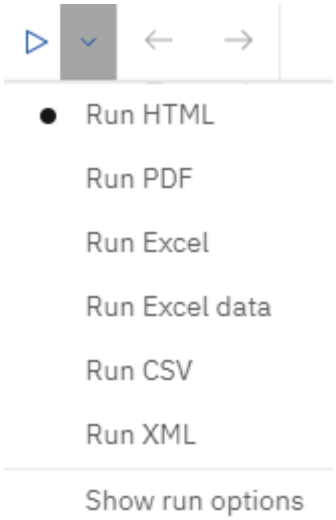
8. Wählen Sie **Öffnen**

   Die verfügbaren Stile für Ihren Bericht werden angezeigt.

9. Wählen Sie **Liste**

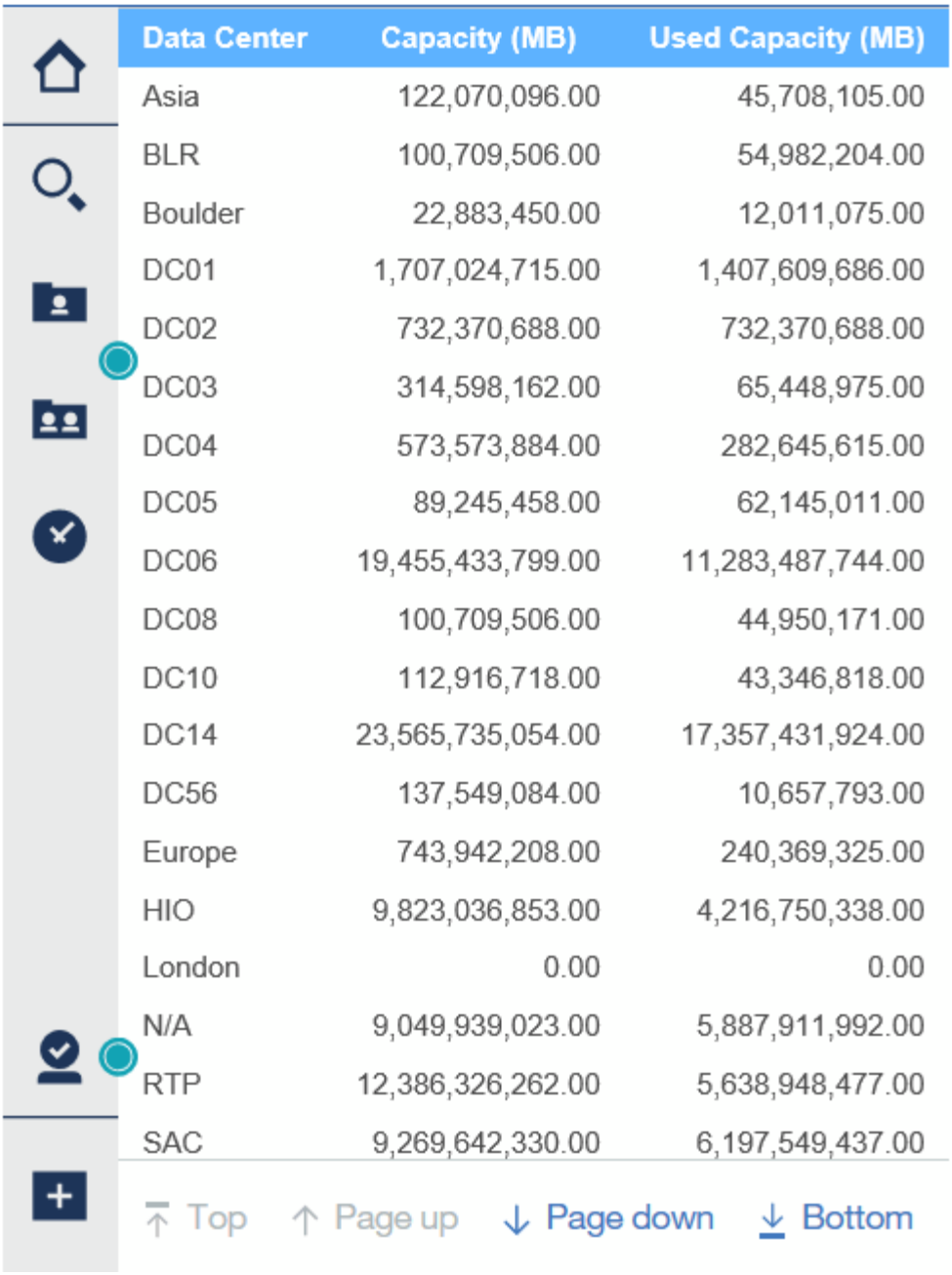
   Fügen Sie passende Namen für Liste und Abfrage hinzu

10. Wählen Sie **OK**
11. Erweitern Sie *Physische Kapazität*
12. Erweitern Sie auf die unterste Ebene des *Rechenzentrums*
13. Ziehen Sie „Data Center“ in die Berichtspalette.
14. Erweitern Sie *Kapazität (MB)*
15. Ziehen Sie *Kapazität (MB)* in die Berichtspalette.
16. Ziehen Sie „Verwendete Kapazität (MB)“ in die Berichtspalette.
17. Führen Sie den Bericht aus, indem Sie im Menü **Ausführen** einen Ausgabetyp auswählen.



Ergebnis

Es wird ein Bericht ähnlich dem folgenden erstellt:



Data Center	Capacity (MB)	Used Capacity (MB)
Asia	122,070,096.00	45,708,105.00
BLR	100,709,506.00	54,982,204.00
Boulder	22,883,450.00	12,011,075.00
DC01	1,707,024,715.00	1,407,609,686.00
DC02	732,370,688.00	732,370,688.00
DC03	314,598,162.00	65,448,975.00
DC04	573,573,884.00	282,645,615.00
DC05	89,245,458.00	62,145,011.00
DC06	19,455,433,799.00	11,283,487,744.00
DC08	100,709,506.00	44,950,171.00
DC10	112,916,718.00	43,346,818.00
DC14	23,565,735,054.00	17,357,431,924.00
DC56	137,549,084.00	10,657,793.00
Europe	743,942,208.00	240,369,325.00
HIO	9,823,036,853.00	4,216,750,338.00
London	0.00	0.00
N/A	9,049,939,023.00	5,887,911,992.00
RTP	12,386,326,262.00	5,638,948,477.00
SAC	9,269,642,330.00	6,197,549,437.00

Berichte verwalten

Sie können das Ausgabeformat und die Bereitstellung eines Berichts anpassen, Berichtseigenschaften oder Zeitpläne festlegen und Berichte per E-Mail versenden.

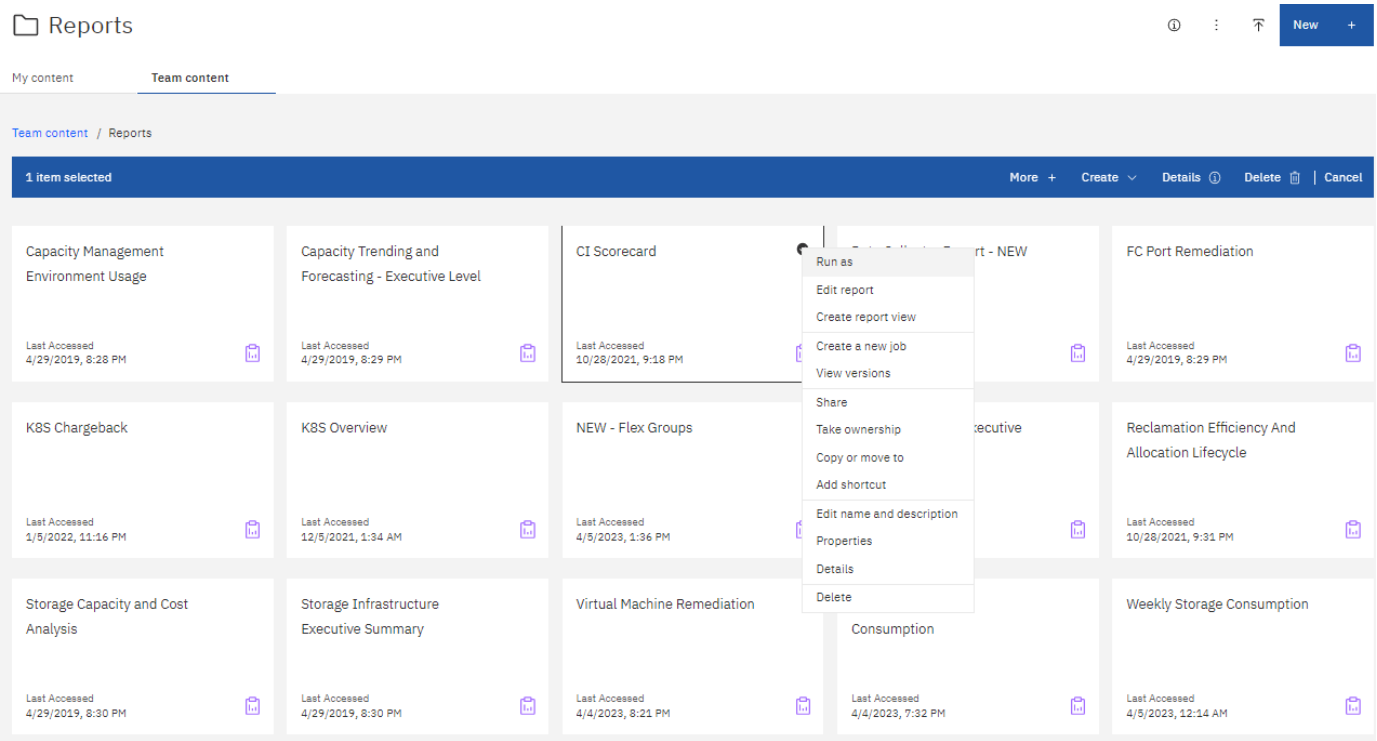
Die Berichtsfunktion ist in Data Infrastructure Insights verfügbar"Premium Edition" .

Bevor Sie Änderungen an den Berichtsberechtigungen oder der Sicherheit vornehmen, müssen Sie die Berichte „Meine Inhalte“ in den Ordner „Teaminhalte“ kopieren, um sicherzustellen, dass die Berichte gespeichert werden.

Anpassen des Ausgabeformats und der Bereitstellung eines Berichts

Sie können das Format und die Übermittlungsmethode von Berichten anpassen.

1. Gehen Sie im Data Infrastructure Insights Reporting Portal zu **Menü > Inhalt > Mein Inhalt/Teaminhalt**. Bewegen Sie die Maus über den Bericht, den Sie anpassen möchten, und öffnen Sie das Menü mit den drei Punkten.

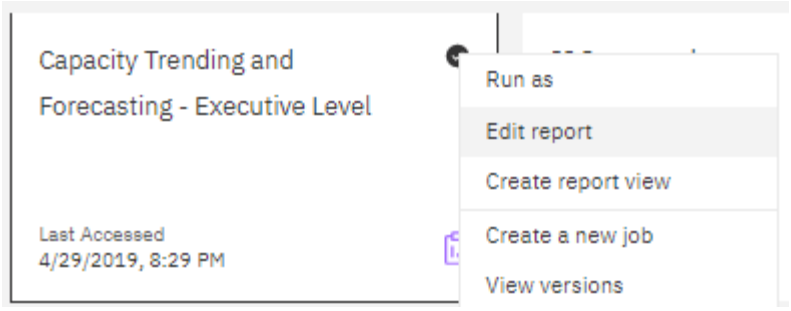


1. Klicken Sie auf **Eigenschaften > Zeitplan**
2. Sie können die folgenden Optionen festlegen:
   - **Planen** Sie, wann Berichte ausgeführt werden sollen.
   - Wählen Sie **Optionen** für Berichtsformat und -übermittlung (Speichern, Drucken, E-Mail) und Sprachen für den Bericht.
3. Klicken Sie auf **Speichern**, um den Bericht mit den von Ihnen getroffenen Auswahlen zu erstellen.

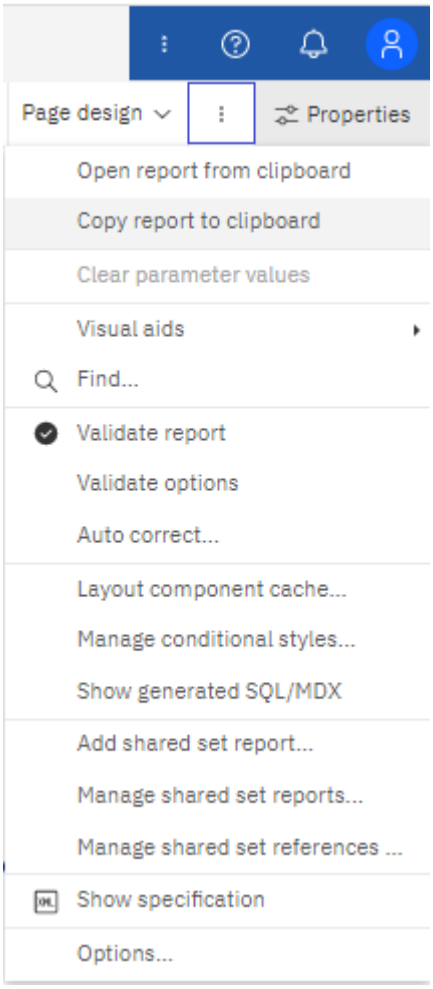
Kopieren eines Berichts in die Zwischenablage

Verwenden Sie diesen Vorgang, um einen Bericht in die Zwischenablage zu kopieren.

1. Wählen Sie einen Bericht zum Kopieren aus (**Menü > Inhalt > Mein Inhalt oder Teaminhalt**)
2. Wählen Sie *Bericht bearbeiten* aus dem Dropdown-Menü des Berichts



3. Öffnen Sie oben rechts auf dem Bildschirm das Menü mit den drei Punkten neben „Eigenschaften“.
4. Wählen Sie **Bericht in die Zwischenablage kopieren**.



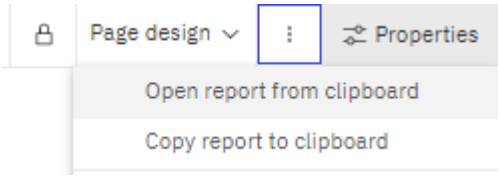
Öffnen von Berichten aus der Zwischenablage

Sie können eine Berichtsspezifikation öffnen, die zuvor in die Zwischenablage kopiert wurde.

Informationen zu diesem Vorgang: Erstellen Sie zunächst einen neuen Bericht oder öffnen Sie einen vorhandenen Bericht, den Sie durch den kopierten Bericht ersetzen möchten. Die folgenden Schritte gelten für einen neuen Bericht.

1. Wählen Sie **Menü > +Neu > Bericht** und erstellen Sie einen leeren Bericht.
2. Öffnen Sie oben rechts auf dem Bildschirm das Menü mit den drei Punkten neben „Eigenschaften“.

3. Wählen Sie **Bericht aus Zwischenablage öffnen**.



1. Fügen Sie den kopierten Code in das Fenster ein und wählen Sie **OK**.
2. Wählen Sie das Diskettensymbol, um den Bericht zu speichern.
3. Wählen Sie, wo der Bericht gespeichert werden soll (*Meine Inhalte*, *Teaminhalte* oder erstellen Sie einen neuen Ordner).
4. Geben Sie dem neuen Bericht einen aussagekräftigen Namen und wählen Sie **Speichern**.

Bearbeiten eines vorhandenen Berichts

Beachten Sie, dass beim Bearbeiten von Dateien an ihrem Standardspeicherort das Risiko besteht, dass diese Berichte bei der nächsten Aktualisierung des Berichtskatalogs überschrieben werden. Es wird empfohlen, den bearbeiteten Bericht unter einem neuen Namen oder an einem anderen als dem Standardspeicherort zu speichern.

Fehlerbehebung

Hier finden Sie Vorschläge zur Behebung von Problemen mit dem Reporting.

Problem:	**Versuchen Sie Folgendes:**
Wenn Sie einen Bericht zum Senden per E-Mail planen, wird der Name des angemeldeten Benutzers bereits in das Feld „An“ der E-Mail eingetragen. Der Name hat jedoch die Form „Vorname Nachname“ (Vorname, Leerzeichen, Nachname). Da es sich hierbei nicht um eine gültige E-Mail-Adresse handelt, kann die E-Mail beim Ausführen des geplanten Berichts nicht gesendet werden.	Wenn Sie den Bericht per E-Mail versenden möchten, löschen Sie den voreingestellten Namen und geben Sie im Feld „An“ eine gültige, richtig formatierte E-Mail-Adresse ein.
Mein geplanter Bericht wird per E-Mail versendet, aber auf den Bericht kann nicht zugegriffen werden, wenn er aus dem Ordner „Meine Inhalte“ stammt.	Um dies zu vermeiden, muss der Bericht oder die Berichtsansicht im Ordner „Teaminhalte > Benutzerdefinierte Berichte – xxxxxx“ gespeichert und der Zeitplan aus dieser gespeicherten Version erstellt werden. Der Ordner „Benutzerdefinierte Berichte – xxxxxx“ ist für alle Benutzer des Mandanten sichtbar.
Beim Speichern eines Jobs wird im Ordner möglicherweise „Teaminhalte“ mit der Inhaltsliste aus „Benutzerdefinierte Berichte – xxxxxx“ angezeigt. Sie können den Job hier jedoch nicht speichern, da Cognos davon ausgeht, dass dies der Ordner „Teaminhalte“ ist, für den Sie keinen Schreibzugriff haben.	Die Problemumgehung besteht darin, einen neuen Ordner mit einem eindeutigen Namen (z. B. „NewFolder“) zu erstellen und dort zu speichern oder in „Meine Inhalte“ zu speichern und dann nach „Benutzerdefinierte Berichte – xxxxxx“ zu kopieren/verschieben.

Erstellen benutzerdefinierter Berichte

Mit den Berichterstellungstools können Sie benutzerdefinierte Berichte erstellen. Nachdem Sie Berichte erstellt haben, können Sie diese speichern und regelmäßig ausführen. Die Ergebnisse der Berichte können automatisch per E-Mail an Sie selbst und andere gesendet werden.

Die Berichtsfunktion ist in Data Infrastructure Insights verfügbar"Premium Edition" .

Die Beispiele in diesem Abschnitt zeigen den folgenden Prozess, der für alle Data Infrastructure Insights Reporting-Datenmodelle verwendet werden kann:

- Identifizieren einer Frage, die mit einem Bericht beantwortet werden soll
- Ermittlung der zur Unterstützung der Ergebnisse erforderlichen Daten
- Auswählen von Datenelementen für den Bericht

Bevor Sie Ihren benutzerdefinierten Bericht entwerfen, müssen Sie einige vorbereitende Aufgaben erledigen. Wenn Sie diese nicht ausfüllen, können die Berichte ungenau oder unvollständig sein.

Wenn Sie beispielsweise den Geräteidentifizierungsprozess nicht abschließen, sind Ihre Kapazitätsberichte nicht genau. Oder wenn Sie die Festlegung von Anmerkungen (wie Ebenen, Geschäftseinheiten und Rechenzentren) nicht abschließen, werden in Ihren benutzerdefinierten Berichten die Daten Ihrer Domäne möglicherweise nicht genau wiedergegeben oder für einige Datenpunkte wird „N/A“ angezeigt.

Bevor Sie Ihre Berichte entwerfen, führen Sie die folgenden Aufgaben aus:

- Konfigurieren Sie alle"Datensammler" richtig.
- Geben Sie Anmerkungen (wie Ebenen, Rechenzentren und Geschäftseinheiten) zu Geräten und Ressourcen Ihres Mandanten ein. Es ist von Vorteil, vor der Berichterstellung stabile Anmerkungen zu haben, da Data Infrastructure Insights Reporting historische Informationen sammelt.

Berichterstellungsprozess

Der Prozess der Erstellung benutzerdefinierter (auch „Ad-hoc“-)Berichte umfasst mehrere Aufgaben:

- Planen Sie die Ergebnisse Ihres Berichts.
- Identifizieren Sie Daten, die Ihre Ergebnisse unterstützen.
- Wählen Sie das Datenmodell (z. B. Chargeback-Datenmodell, Inventar-Datenmodell usw.) aus, das die Daten enthält.
- Wählen Sie Datenelemente für den Bericht aus.
- Formatieren, sortieren und filtern Sie Berichtsergebnisse optional.

Planen der Ergebnisse Ihres benutzerdefinierten Berichts

Bevor Sie die Tools zur Berichterstellung öffnen, möchten Sie möglicherweise die Ergebnisse planen, die Sie mit dem Bericht erzielen möchten. Mit Berichterstellungstools können Sie Berichte einfach erstellen und benötigen dafür möglicherweise nicht viel Planung. Es ist jedoch ratsam, sich beim Berichtsanforderer über die Berichtsanforderungen zu informieren.

- Identifizieren Sie die genaue Frage, die Sie beantworten möchten. Beispiel:

    - Wie viel Kapazität habe ich noch?
    - Wie hoch sind die Rückbuchungskosten pro Geschäftseinheit?
    - Wie hoch ist die Kapazität pro Ebene, um sicherzustellen, dass die Geschäftseinheiten auf der richtigen Speicherebene ausgerichtet sind?
    - Wie kann ich den Strom- und Kühlbedarf prognostizieren? (Fügen Sie benutzerdefinierte Metadaten hinzu, indem Sie den Ressourcen Anmerkungen hinzufügen.)
- Identifizieren Sie die Datenelemente, die Sie zur Unterstützung der Antwort benötigen.
- Identifizieren Sie die Beziehungen zwischen Daten, die Sie in der Antwort sehen möchten. Bauen Sie in Ihrer Frage keine unlogischen Zusammenhänge ein, wie zum Beispiel: „Ich möchte die Ports sehen, die mit der Kapazität in Zusammenhang stehen.“
- Identifizieren Sie alle für die Daten erforderlichen Berechnungen.
- Bestimmen Sie, welche Filtertypen erforderlich sind, um die Ergebnisse einzugrenzen.
- Bestimmen Sie, ob Sie aktuelle oder historische Daten verwenden müssen.
- Stellen Sie fest, ob Sie Zugriffsrechte für Berichte festlegen müssen, um die Daten auf bestimmte Zielgruppen zu beschränken.
- Legen Sie fest, wie der Bericht verteilt wird. Soll es beispielsweise nach einem festgelegten Zeitplan per E-Mail versendet oder in den Ordnerbereich „Teaminhalte“ aufgenommen werden?
- Bestimmen Sie, wer den Bericht pflegen soll. Dies kann sich auf die Komplexität des Designs auswirken.
- Erstellen Sie ein Modell des Berichts.

Tipps zum Gestalten von Berichten

Beim Entwerfen von Berichten können Ihnen einige Tipps hilfreich sein.

- Bestimmen Sie, ob Sie aktuelle oder historische Daten verwenden müssen.

  Die meisten Berichte müssen nur über die neuesten in Data Infrastructure Insights verfügbaren Daten berichten.

- Data Infrastructure Insights Reporting bietet historische Informationen zu Kapazität und Leistung, jedoch nicht zum Inventar.
- Jeder sieht alle Daten. Möglicherweise müssen Sie die Daten jedoch auf bestimmte Zielgruppen beschränken.

  Um die Informationen für verschiedene Benutzer zu segmentieren, können Sie Berichte erstellen und Zugriffsberechtigungen dafür festlegen.

Berichtsdatenmodelle

Data Infrastructure Insights umfasst mehrere Datenmodelle, aus denen Sie entweder vordefinierte Berichte auswählen oder Ihren eigenen benutzerdefinierten Bericht erstellen können.

Jedes Datenmodell enthält einen einfachen Data Mart und einen erweiterten Data Mart:

- Der einfache Data Mart bietet schnellen Zugriff auf die am häufigsten verwendeten Datenelemente und enthält nur den letzten Snapshot der Data Warehouse-Daten; historische Daten sind nicht enthalten.
- Der erweiterte Data Mart bietet alle im einfachen Data Mart verfügbaren Werte und Details und umfasst den Zugriff auf historische Datenwerte.

Kapazitätsdatenmodelle

Ermöglicht Ihnen, Fragen zur Speicherkapazität, Dateisystemauslastung, internen Volumekapazität, Portkapazität, Qtree-Kapazität und Kapazität virtueller Maschinen (VM) zu beantworten. Das Kapazitätsdatenmodell ist ein Container für mehrere Kapazitätsdatenmodelle. Mit diesem Datenmodell können Sie Berichte erstellen, die verschiedene Arten von Fragen beantworten:

Datenmodell für Speicher und Speicherpoolkapazität

Ermöglicht Ihnen, Fragen zur Ressourcenplanung der Speicherkapazität zu beantworten, einschließlich Speicher und Speicherpools, und umfasst sowohl physische als auch virtuelle Speicherpooldaten. Dieses einfache Datenmodell kann Ihnen dabei helfen, Fragen zur Kapazität auf der Etage und zur Kapazitätsnutzung von Speicherpools nach Ebene und Rechenzentrum im Zeitverlauf zu beantworten. Wenn Sie mit der Kapazitätsberichterstattung noch nicht vertraut sind, sollten Sie mit diesem Datenmodell beginnen, da es sich um ein einfacheres, zielgerichteteres Datenmodell handelt. Mithilfe dieses Datenmodells können Sie Fragen wie die folgenden beantworten:

- Wann wird voraussichtlich die Kapazitätsschwelle von 80 % meines physischen Speichers erreicht?
- Wie groß ist die physische Speicherkapazität eines Arrays für eine bestimmte Ebene?
- Wie hoch ist meine Speicherkapazität nach Hersteller und Familie sowie nach Rechenzentrum?
- Wie ist der Trend zur Speicherauslastung eines Arrays für alle Ebenen?
- Welches sind meine Top 10 Speichersysteme mit der höchsten Auslastung?
- Wie ist der Trend zur Speicherauslastung der Speicherpools?
- Wie viel Kapazität ist bereits vergeben?
- Welche Kapazität steht zur Zuteilung zur Verfügung?

Datenmodell zur Dateisystemnutzung

Dieses Datenmodell bietet Einblick in die Kapazitätsauslastung durch Hosts auf Dateisystemebene. Administratoren können die zugewiesene und verwendete Kapazität pro Dateisystem ermitteln, den Typ des Dateisystems bestimmen und Trendstatistiken nach Dateisystemtyp identifizieren. Mit diesem Datenmodell können Sie folgende Fragen beantworten:

- Wie groß ist das Dateisystem?
- Wo werden die Daten gespeichert und wie wird darauf zugegriffen, beispielsweise lokal oder SAN?
- Was sind die historischen Trends bei der Dateisystemkapazität? Welchen zukünftigen Bedarf können wir auf dieser Grundlage voraussehen?

Datenmodell für die interne Volumekapazität

Ermöglicht Ihnen, Fragen zur genutzten Kapazität des internen Volumes, zur zugewiesenen Kapazität und zur Kapazitätsnutzung im Zeitverlauf zu beantworten:

- Welche internen Volumes haben eine Auslastung, die über einem vordefinierten Schwellenwert liegt?
- Welche internen Volumina laufen aufgrund eines Trends Gefahr, ihre Kapazitäten zu erreichen? 8 Wie hoch ist die genutzte Kapazität im Vergleich zur zugewiesenen Kapazität auf unseren internen Datenträgern?

Datenmodell für die Portkapazität

Ermöglicht Ihnen, Fragen zur Switch-Port-Konnektivität, zum Port-Status und zur Port-Geschwindigkeit im Zeitverlauf zu beantworten. Sie können Fragen wie die folgenden beantworten, um die Anschaffung neuer Switches zu planen: Wie kann ich eine Port-Verbrauchsprognose erstellen, die die Ressourcenverfügbarkeit (Portverfügbarkeit) vorhersagt (je nach Rechenzentrum, Switch-Anbieter und Portgeschwindigkeit)?

- Welche Ports werden voraussichtlich nicht mehr über ausreichende Kapazitäten verfügen, was die Datengeschwindigkeit, das Rechenzentrum, den Anbieter und die Anzahl der Host- und Speicherports betrifft?
- Wie entwickeln sich die Kapazitäten der Switch-Ports im Laufe der Zeit?
- Wie hoch sind die Portgeschwindigkeiten?
- Welche Art von Portkapazität wird benötigt und welcher Organisation steht ein bestimmter Porttyp oder Anbieter bald nicht mehr zur Verfügung?
- Wann ist der optimale Zeitpunkt, diese Kapazität zu erwerben und bereitzustellen?

Qtree-Kapazitätsdatenmodell

Ermöglicht Ihnen, die Qtree-Auslastung (mit Daten wie genutzte Kapazität im Vergleich zur zugewiesenen Kapazität) im Zeitverlauf zu verfolgen. Sie können die Informationen nach verschiedenen Dimensionen anzeigen, beispielsweise nach Geschäftseinheit, Anwendung, Ebene und Servicelevel. Mit diesem Datenmodell können Sie folgende Fragen beantworten:

- Wie hoch ist die genutzte Kapazität für Qtrees im Vergleich zu den pro Anwendung oder Geschäftseinheit festgelegten Grenzwerten?
- Wie entwickeln sich unsere genutzten und freien Kapazitäten, damit wir eine Kapazitätsplanung durchführen können?
- Welche Geschäftseinheiten nutzen die größte Kapazität?
- Welche Anwendungen verbrauchen die meiste Kapazität?

VM-Kapazitätsdatenmodell

Ermöglicht Ihnen, Berichte über Ihre virtuelle Umgebung und deren Kapazitätsauslastung zu erstellen. Mit diesem Datenmodell können Sie über Änderungen der Kapazitätsnutzung im Zeitverlauf für VMs und Datenspeicher berichten. Das Datenmodell bietet auch Thin Provisioning- und Chargeback-Daten für virtuelle Maschinen.

- Wie kann ich die Kapazitätsrückbelastung basierend auf der für VMs und Datenspeicher bereitgestellten Kapazität ermitteln?
- Welche Kapazität wird von VMs nicht genutzt und welcher ungenutzte Anteil ist frei, verwaist oder anderweitig?
- Was müssen wir aufgrund der Konsumtrends kaufen?
- Welche Einsparungen bei der Speichereffizienz erziele ich durch den Einsatz von Storage Thin Provisioning- und Deduplizierungstechnologien?

Kapazitäten im VM-Kapazitätsdatenmodell werden von virtuellen Datenträgern (VMDKs) übernommen. Dies bedeutet, dass die bereitgestellte Größe einer VM unter Verwendung des VM-Kapazitätsdatenmodells der Größe ihrer virtuellen Datenträger entspricht. Dies unterscheidet sich von der bereitgestellten Kapazität in der Ansicht „Virtuelle Maschinen“ in Data Infrastructure Insights, die die bereitgestellte Größe für die VM selbst anzeigt.

Datenmodell „Volume Capacity“

Ermöglicht Ihnen, alle Aspekte der Volumes auf Ihrem Mandanten zu analysieren und Daten nach Anbieter, Modell, Ebene, Servicelevel und Rechenzentrum zu organisieren.

Sie können die Kapazität im Zusammenhang mit verwaisten Volumes, ungenutzten Volumes und Schutzvolumes (für die Replikation verwendet) anzeigen. Sie können auch verschiedene Volume-Technologien (iSCSI oder FC) sehen und virtuelle Volumes mit nicht-virtuellen Volumes hinsichtlich Array-Virtualisierungsproblemen vergleichen.

Mit diesem Datenmodell können Sie Fragen wie die folgenden beantworten:

- Welche Volumes haben eine Auslastung, die über einem vordefinierten Schwellenwert liegt?
- Wie ist der Trend in meinem Rechenzentrum hinsichtlich der Kapazität verwaister Datenträger?
- Wie viel meiner Rechenzentrumskapazität ist virtualisiert oder Thin Provisioning-basiert?
- Wie viel meiner Rechenzentrumskapazität muss für die Replikation reserviert werden?

Chargeback-Datenmodell

Ermöglicht Ihnen, Fragen zur verwendeten Kapazität und zur zugewiesenen Kapazität von Speicherressourcen (Volumes, interne Volumes und Qtrees) zu beantworten. Dieses Datenmodell bietet Informationen zur Speicherkapazitätsrückbelastung und Verantwortlichkeit nach Hosts, Anwendungen und Geschäftseinheiten und umfasst sowohl aktuelle als auch historische Daten. Berichtsdaten können nach Servicelevel und Speicherebene kategorisiert werden.

Sie können dieses Datenmodell verwenden, um Rückbuchungsberichte zu erstellen, indem Sie die von einer Geschäftseinheit genutzte Kapazität ermitteln. Mit diesem Datenmodell können Sie einheitliche Berichte für mehrere Protokolle erstellen (einschließlich NAS, SAN, FC und iSCSI).

- Bei Speichern ohne interne Volumes zeigen Chargeback-Berichte die Rückbuchung nach Volumes an.
- Für Speicher mit internen Volumes:
  - Wenn Geschäftseinheiten Volumen zugewiesen sind, zeigen Rückbuchungsberichte die Rückbuchung nach Volumen an.
  - Wenn Geschäftseinheiten nicht Volumes, sondern Qtrees zugewiesen sind, zeigen Chargeback-Berichte Chargebacks nach Qtrees an.
  - Wenn Geschäftseinheiten keinen Volumes und keinen Qtrees zugewiesen sind, zeigen Chargeback-Berichte das interne Volume an.
  - Die Entscheidung, ob Chargeback nach Volume, Qtree oder internem Volume angezeigt wird, wird für jedes interne Volume einzeln getroffen. Daher ist es möglich, dass verschiedene interne Volumes im selben Speicherpool Chargebacks auf unterschiedlichen Ebenen anzeigen.

Kapazitätsfakten werden nach einem Standardzeitintervall gelöscht. Einzelheiten finden Sie unter Data Warehouse-Prozesse.

Berichte, die das Chargeback-Datenmodell verwenden, zeigen möglicherweise andere Werte an als Berichte, die das Speicherkapazitäts-Datenmodell verwenden.

- Bei Speicher-Arrays, die keine NetApp Speichersysteme sind, sind die Daten aus beiden Datenmodellen identisch.
- Bei NetApp und Celerra-Speichersystemen basiert das Chargeback-Datenmodell auf einer einzelnen Ebene (aus Volumes, internen Volumes oder Qtrees) zur Berechnung der Gebühren, während das Storage

Capacity-Datenmodell auf mehreren Ebenen (aus Volumes und internen Volumes) zur Berechnung der Gebühren basiert.

Inventardatenmodell

Ermöglicht Ihnen, Fragen zu Inventarressourcen zu beantworten, darunter Hosts, Speichersysteme, Switches, Festplatten, Bänder, Qtrees, Kontingente, virtuelle Maschinen und Server sowie generische Geräte. Das Inventory-Datenmodell umfasst mehrere Submarts, mit denen Sie Informationen zu Replikationen, FC-Pfaden, iSCSI-Pfaden, NFS-Pfaden und Verstößen anzeigen können. Das Inventardatenmodell enthält keine historischen Daten. Fragen, die Sie mit diesen Daten beantworten können

- Welche Vermögenswerte habe ich und wo sind sie?
- Wer nutzt die Vermögenswerte?
- Welche Arten von Geräten habe ich und was sind die Komponenten dieser Geräte?
- Wie viele Hosts pro Betriebssystem habe ich und wie viele Ports sind auf diesen Hosts vorhanden?
- Welche Speicher-Arrays pro Anbieter sind in jedem Rechenzentrum vorhanden?
- Wie viele Switches pro Anbieter habe ich in jedem Rechenzentrum?
- Wie viele Ports sind nicht lizenziert?
- Welche Bänder von welchem Anbieter verwenden wir und wie viele Ports sind auf jedem Band vorhanden? Werden alle generischen Geräte identifiziert, bevor wir mit der Arbeit an den Berichten beginnen?
- Wie lauten die Pfade zwischen Hosts und Speichervolumes oder Bändern?
- Welche Pfade gibt es zwischen generischen Geräten und Speichervolumes oder Bändern?
- Wie viele Verstöße jedes Typs habe ich pro Rechenzentrum?
- Was sind für jedes replizierte Volume die Quell- und Zielvolumes?
- Gibt es Firmware-Inkompatibilitäten oder nicht übereinstimmende Portgeschwindigkeiten zwischen Fibre Channel-Host-HBAs und Switches?

Leistungsdatenmodell

Ermöglicht Ihnen, Fragen zur Leistung von Volumes, Anwendungsvolumes, internen Volumes, Switches, Anwendungen, VMs, VMDKs, ESX im Vergleich zu VM, Hosts und Anwendungsknoten zu beantworten. Viele davon melden stündliche Daten, tägliche Daten oder beides. Mithilfe dieses Datenmodells können Sie Berichte erstellen, die verschiedene Arten von Fragen zum Leistungsmanagement beantworten:

- Welche Volumes oder internen Volumes wurden während eines bestimmten Zeitraums nicht verwendet oder nicht aufgerufen?
- Können wir eine mögliche Fehlkonfiguration des Speichers für eine Anwendung (unbenutzt) genau bestimmen?
- Wie war das allgemeine Zugriffsverhaltensmuster für eine Anwendung?
- Werden die abgestuften Volumes einer bestimmten Anwendung entsprechend zugewiesen?
- Könnten wir für eine derzeit laufende Anwendung günstigeren Speicher verwenden, ohne dass dies Auswirkungen auf die Anwendungsleistung hat?
- Welche Anwendungen führen zu mehr Zugriffen auf den aktuell konfigurierten Speicher?

Wenn Sie die Switch-Leistungstabellen verwenden, können Sie die folgenden Informationen erhalten:

- Ist mein Host-Verkehr über verbundene Ports ausgeglichen?

- Welche Switches oder Ports weisen eine hohe Fehleranzahl auf?
- Welche Switches werden basierend auf der Portleistung am häufigsten verwendet?
- Welche Switches werden auf Grundlage der Portleistung nicht ausreichend genutzt?
- Wie hoch ist der Trenddurchsatz des Hosts basierend auf der Portleistung?
- Wie hoch war die Leistungsauslastung für die letzten X Tage für einen bestimmten Host, ein bestimmtes Speichersystem, ein bestimmtes Band oder einen bestimmten Switch?
- Welche Geräte erzeugen Verkehr auf einem bestimmten Switch (z. B. welche Geräte sind für die Nutzung eines stark ausgelasteten Switches verantwortlich)?
- Wie hoch ist der Durchsatz für eine bestimmte Geschäftseinheit in unserer Umgebung?

Wenn Sie die Festplattenleistungstabellen verwenden, können Sie die folgenden Informationen erhalten:

- Wie hoch ist der Durchsatz für einen bestimmten Speicherpool basierend auf den Daten zur Festplattenleistung?
- Welcher Speicherpool wird am häufigsten genutzt?
- Wie hoch ist die durchschnittliche Festplattenauslastung für einen bestimmten Speicher?
- Wie ist der Nutzungstrend für ein Speichersystem oder einen Speicherpool basierend auf den Daten zur Festplattenleistung?
- Wie ist die Entwicklung der Datenträgernutzung für einen bestimmten Speicherpool?

Wenn Sie VM- und VMDK-Leistungstabellen verwenden, können Sie die folgenden Informationen erhalten:

- Erbringt meine virtuelle Umgebung die optimale Leistung?
- Welche VMDKs melden die höchsten Arbeitslasten?
- Wie kann ich die von VMDs, die verschiedenen Datenspeichern zugeordnet sind, gemeldete Leistung nutzen, um Entscheidungen über die Neuklassifizierung zu treffen?

Das Leistungsdatenmodell enthält Informationen, die Ihnen dabei helfen, die Eignung von Ebenen, Speicherfehlkonfigurationen für Anwendungen und die letzten Zugriffszeiten von Volumes und internen Volumes zu bestimmen. Dieses Datenmodell stellt Daten wie Antwortzeiten, IOPs, Durchsatz, Anzahl ausstehender Schreibvorgänge und Zugriffsstatus bereit.

Datenmodell zur Speichereffizienz

Ermöglicht Ihnen, den Speichereffizienzwert und das Speicherpotenzial im Laufe der Zeit zu verfolgen. In diesem Datenmodell werden nicht nur Messungen der bereitgestellten Kapazität gespeichert, sondern auch die Menge, die verwendet oder verbraucht wird (die physikalische Messung). Wenn beispielsweise Thin Provisioning aktiviert ist, zeigt Data Infrastructure Insights an, wie viel Kapazität vom Gerät genutzt wird. Sie können dieses Modell auch verwenden, um die Effizienz bei aktivierter Deduplizierung zu bestimmen. Mithilfe des Datamarts zur Speichereffizienz können Sie verschiedene Fragen beantworten:

- Wie hoch sind unsere Einsparungen bei der Speichereffizienz durch die Implementierung von Thin Provisioning- und Deduplizierungstechnologien?
- Wie hoch sind die Speichereinsparungen in den Rechenzentren?
- Wann müssen wir auf der Grundlage historischer Kapazitätstrends zusätzlichen Speicher kaufen?
- Welche Kapazitätssteigerung würde es geben, wenn wir Technologien wie Thin Provisioning und Deduplizierung aktivieren würden?

- Bin ich jetzt hinsichtlich der Speicherkapazität gefährdet?

Fakten- und Dimensionstabellen des Datenmodells

Jedes Datenmodell enthält sowohl Fakten- als auch Dimensionstabellen.

- Faktentabellen: Enthalten gemessene Daten, beispielsweise Menge, Roh- und Nutzkapazität. Enthalten Fremdschlüssel zu Dimensionstabellen.
- Dimensionstabellen: Enthalten beschreibende Informationen zu Fakten, beispielsweise Rechenzentren und Geschäftseinheiten. Eine Dimension ist eine Struktur, die häufig aus Hierarchien besteht und Daten kategorisiert. Dimensionsattribute helfen bei der Beschreibung der Dimensionswerte.

Mithilfe unterschiedlicher oder mehrerer Dimensionsattribute (die in den Berichten als Spalten angezeigt werden) erstellen Sie Berichte, die auf Daten für jede im Datenmodell beschriebene Dimension zugreifen.

In Datenmodellelementen verwendete Farben

Die Farben der Datenmodellelemente haben unterschiedliche Bedeutungen.

- Gelbe Assets: Stellen Messungen dar.
- Nicht gelbe Vermögenswerte: Stellen Attribute dar. Diese Werte werden nicht aggregiert.

Verwenden mehrerer Datenmodelle in einem Bericht

Normalerweise verwenden Sie ein Datenmodell pro Bericht. Sie können jedoch einen Bericht schreiben, der Daten aus mehreren Datenmodellen kombiniert.

Um einen Bericht zu schreiben, der Daten aus mehreren Datenmodellen kombiniert, wählen Sie eines der Datenmodelle als Basis aus und schreiben Sie dann SQL-Abfragen, um auf die Daten aus den zusätzlichen Data Marts zuzugreifen. Mit der SQL-Join-Funktion können Sie die Daten aus den verschiedenen Abfragen in einer einzigen Abfrage kombinieren, die Sie zum Schreiben des Berichts verwenden können.

Angenommen, Sie möchten die aktuelle Kapazität für jedes Speicherarray und benutzerdefinierte Anmerkungen zu den Arrays erfassen. Sie könnten den Bericht mithilfe des Datenmodells „Speicherkapazität“ erstellen. Sie könnten die Elemente aus den Tabellen „Aktuelle Kapazität“ und „Dimension“ verwenden und eine separate SQL-Abfrage hinzufügen, um auf die Anmerkungsinformationen im Inventardatenmodell zuzugreifen. Schließlich können Sie die Daten kombinieren, indem Sie die Inventarspeicherdaten mithilfe des Speichernamens und der Verknüpfungskriterien mit der Speicherdimensionstabelle verknüpfen.

Zugriff auf die Berichtsdatenbank über die API

Die leistungsstarke API von Data Infrastructure Insights ermöglicht es Benutzern, die Data Infrastructure Insights Reporting-Datenbank direkt abzufragen, ohne die Cognos Reporting-Umgebung zu durchlaufen.

Diese Dokumentation bezieht sich auf die Data Infrastructure Insights -Berichtsfunktion, die in der Data Infrastructure Insights Premium Edition verfügbar ist.

Odata

Die Data Infrastructure Insights Reporting API folgt dem"OData v4" (Open Data Protocol)-Standard für die Abfrage der Reporting-Datenbank. Weitere Informationen und weitere Informationen finden Sie unter"dieses Tutorial" auf OData.

Alle Anfragen beginnen mit der URL *https://< Data Infrastructure Insights URL>/rest/v1/dwh-management/odata*

Generieren eines API-Schlüssels

Lesen Sie mehr über"APIs für Data Infrastructure Insights" .

Gehen Sie wie folgt vor, um einen API-Schlüssel zu generieren:

- Melden Sie sich bei Ihrer Data Infrastructure Insights Umgebung an und wählen Sie **Admin > API-Zugriff**.
- Klicken Sie auf „+ API-Zugriffstoken“.
- Geben Sie einen Namen und eine Beschreibung ein.
- Wählen Sie als Typ „Data Warehouse“ aus.
- Legen Sie die Berechtigungen auf Lesen/Schreiben fest.
- Legen Sie ein gewünschtes Ablaufdatum fest.
- Klicken Sie auf „Speichern“, kopieren Sie dann den Schlüssel und speichern Sie ihn an einem sicheren Ort. Auf den vollständigen Schlüssel können Sie später nicht mehr zugreifen.

APIkeys sind gut für*Sync* oder *Async* .

Direkte Abfrage von Tabellen

Mit dem vorhandenen API-Schlüssel sind nun direkte Abfragen der Reporting-Datenbank möglich. Lange URLs können zu Anzeigezwecken auf https://…/odata/ vereinfacht werden, anstatt auf die vollständige Version https://< Data Infrastructure Insights URL>/rest/v1/dwh-management/odata/

Versuchen Sie es mit einfachen Abfragen wie

- https://< URL der Data Infrastructure Insights >/rest/v1/dwh-management/odata/dwh_custom
- https://< URL der Data Infrastructure Insights >/rest/v1/dwh-management/odata/dwh_inventory
- https://< URL der Data Infrastructure Insights >/rest/v1/dwh-management/odata/dwh_inventory/storage
- https://< URL der Data Infrastructure Insights >/rest/v1/dwh-management/odata/dwh_inventory/disk
- https://…/odata/dwh_custom/custom_queries

REST-API-Beispiele

Die URL für alle Aufrufe lautet *https://< Data Infrastructure Insights URL>/rest/v1/dwh-management/odata*.

- GET /{schema}/** – Ruft Daten aus der Berichtsdatenbank ab.

Format: *https://< Data Infrastructure Insights -URL>/rest/v1/dwh-management/odata/<schema_name>/<query>*

Beispiel:

```
 https://<domain>/rest/v1/dwh-
management/odata/dwh_inventory/fabric?$count=true&$orderby=name
Ergebnis:
```

```
{
   "@odata.context": "$metadata#fabric",
   "@odata.count": 2,
   "value": [
       {
           "id": 851,
           "identifier": "10:00:50:EB:1A:40:3B:44",
           "wwn": "10:00:50:EB:1A:40:3B:44",
           "name": "10:00:50:EB:1A:40:3B:44",
           "vsanEnabled": "0",
           "vsanId": null,
           "zoningEnabled": "0",
           "url": "https://<domain>/web/#/assets/fabrics/941716"
       },
       {
           "id": 852,
           "identifier": "10:00:50:EB:1A:40:44:0C",
           "wwn": "10:00:50:EB:1A:40:44:0C",
           "name": "10:00:50:EB:1A:40:44:0C",
           "vsanEnabled": "0",
           "vsanId": null,
           "zoningEnabled": "0",
           "url": "https://<domain>/web/#/assets/fabrics/941836"
        }
    ]
}
```


Hilfreiche Hinweise

Beachten Sie beim Arbeiten mit Reporting-API-Abfragen Folgendes.

- Die Abfragenutzlast muss eine gültige JSON-Zeichenfolge sein
- Die Abfragenutzlast muss in einer einzigen Zeile enthalten sein
- Doppelte Anführungszeichen müssen maskiert werden, d. h. \"
- Tabs werden als \t unterstützt
- Vermeiden Sie Kommentare
- Tabellennamen in Kleinbuchstaben werden unterstützt

Zusätzlich:

- 2 Header sind erforderlich:
  - Name „X-CloudInsights-ApiKey“
  - Attributwert „<apikey>“

Ihr API-Schlüssel ist spezifisch für Ihre Data Infrastructure Insights Umgebung.

Synchron oder asynchron?

Standardmäßig wird ein API-Befehl im *synchronen* Modus ausgeführt, d. h. Sie senden die Anfrage und die Antwort wird sofort zurückgegeben. Manchmal kann die Ausführung einer Abfrage jedoch sehr lange dauern, was zu einer Zeitüberschreitung der Anforderung führen kann. Um dies zu umgehen, können Sie eine Anfrage *asynchron* ausführen. Im asynchronen Modus gibt die Anfrage eine URL zurück, über die die Ausführung überwacht werden kann. Die URL gibt das Ergebnis zurück, wenn es fertig ist.

Um eine Abfrage im asynchronen Modus auszuführen, fügen Sie den Header hinzu **`Prefer: respond-async`** auf die Anfrage. Bei erfolgreicher Ausführung enthält die Antwort die folgenden Header:

```
Status Code: 202 (which means ACCEPTED)
preference-applied: respond-async
location: https://<Data Infrastructure Insights URL>/rest/v1/dwh-
management/odata/dwh_custom/asyncStatus/<token>
```

Bei der Abfrage der Standort-URL werden dieselben Header zurückgegeben, wenn die Antwort noch nicht bereit ist, oder der Status 200, wenn die Antwort bereit ist. Der Antwortinhalt ist vom Typ Text und enthält den HTTP-Status der ursprünglichen Abfrage und einige Metadaten, gefolgt von den Ergebnissen der ursprünglichen Abfrage.

```
HTTP/1.1 200 OK
 OData-Version: 4.0
 Content-Type: application/json;odata.metadata=minimal
 oDataResponseSizeCounted: true

 { <JSON_RESPONSE> }
```

Um eine Liste aller asynchronen Abfragen und deren Bereitschaft anzuzeigen, verwenden Sie den folgenden Befehl:

```
 GET https://<Data Infrastructure Insights URL>/rest/v1/dwh-
management/odata/dwh_custom/asyncList
Die Antwort hat das folgende Format:
```

```
{
   "queries" : [
       {
           "Query": "https://<Data Infrastructure Insights
URL>/rest/v1/dwh-
management/odata/dwh_custom/heavy_left_join3?$count=true",
           "Location": "https://<Data Infrastructure Insights
URL>/rest/v1/dwh-management/odata/dwh_custom/asyncStatus/<token>",
           "Finished": false
       }
   ]
}
```

So werden historische Daten für die Berichterstellung aufbewahrt

Data Infrastructure Insights speichert historische Daten zur Verwendung in Berichten basierend auf den Data Marts und der Granularität der Daten, wie in der folgenden Tabelle gezeigt.

Datamart	Messobjekt	Granularität	Aufbewahrungsfrist
Performance-Märkte	Volumes und interne Volumes	Stündlich	14 Tage
Performance-Märkte	Volumes und interne Volumes	Täglich	13 Monate
Performance-Märkte	Anwendung	Stündlich	13 Monate
Performance-Märkte	Gastgeber	Stündlich	13 Monate
Performance-Märkte	Switch-Leistung für Port	Stündlich	35 Tage
Performance-Märkte	Switch-Leistung für Host, Speicher und Band	Stündlich	13 Monate
Performance-Märkte	Speicherknoten	Stündlich	14 Tage
Performance-Märkte	Speicherknoten	Täglich	13 Monate
Performance-Märkte	VM-Leistung	Stündlich	14 Tage
Performance-Märkte	VM-Leistung	Täglich	13 Monate
Performance-Märkte	Hypervisor-Leistung	Stündlich	35 Tage
Performance-Märkte	Hypervisor-Leistung	Täglich	13 Monate
Performance-Märkte	VMDK-Leistung	Stündlich	35 Tage
Performance-Märkte	VMDK-Leistung	Täglich	13 Monate
Performance-Märkte	Festplattenleistung	Stündlich	14 Tage
Performance-Märkte	Festplattenleistung	Täglich	13 Monate

Kapazitätsmärkte	Alle (außer Einzelbände)	Täglich	13 Monate
Kapazitätsmärkte	Alle (außer Einzelbände)	Monatsvertreter	14 Monate und darüber hinaus
Inventarmärkte	Einzelbände	Aktueller Stand	1 Tag (oder bis zum nächsten ETL)

Schemadiagramme für die Data Infrastructure Insights -Berichterstattung

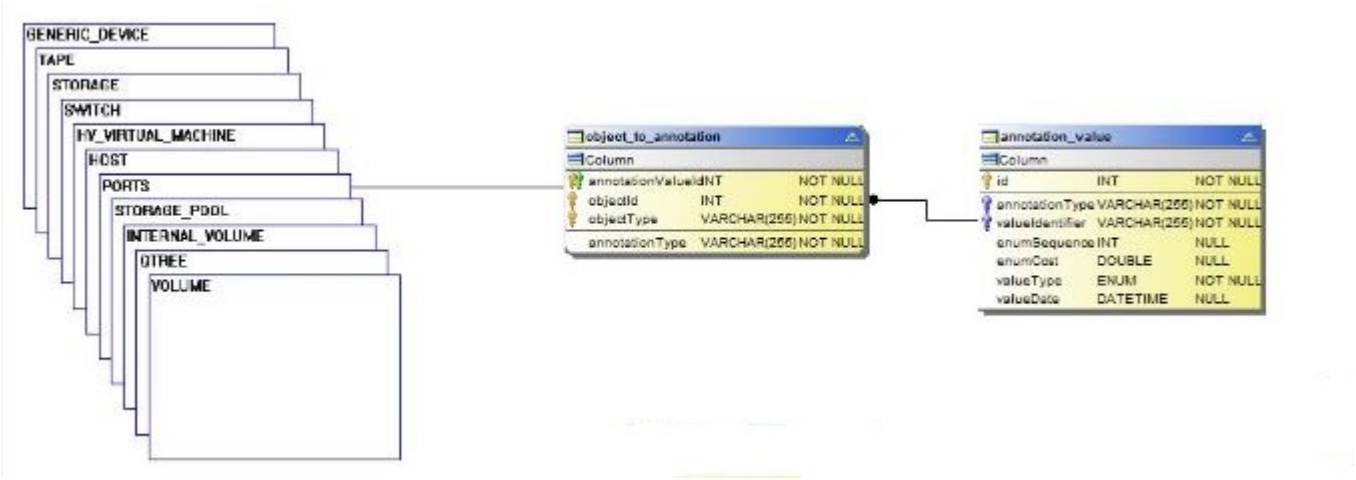
Dieses Dokument enthält Schemadiagramme für die Berichtsdatenbank.

Die Berichtsfunktion ist in Data Infrastructure Insights verfügbar"Premium Edition" .

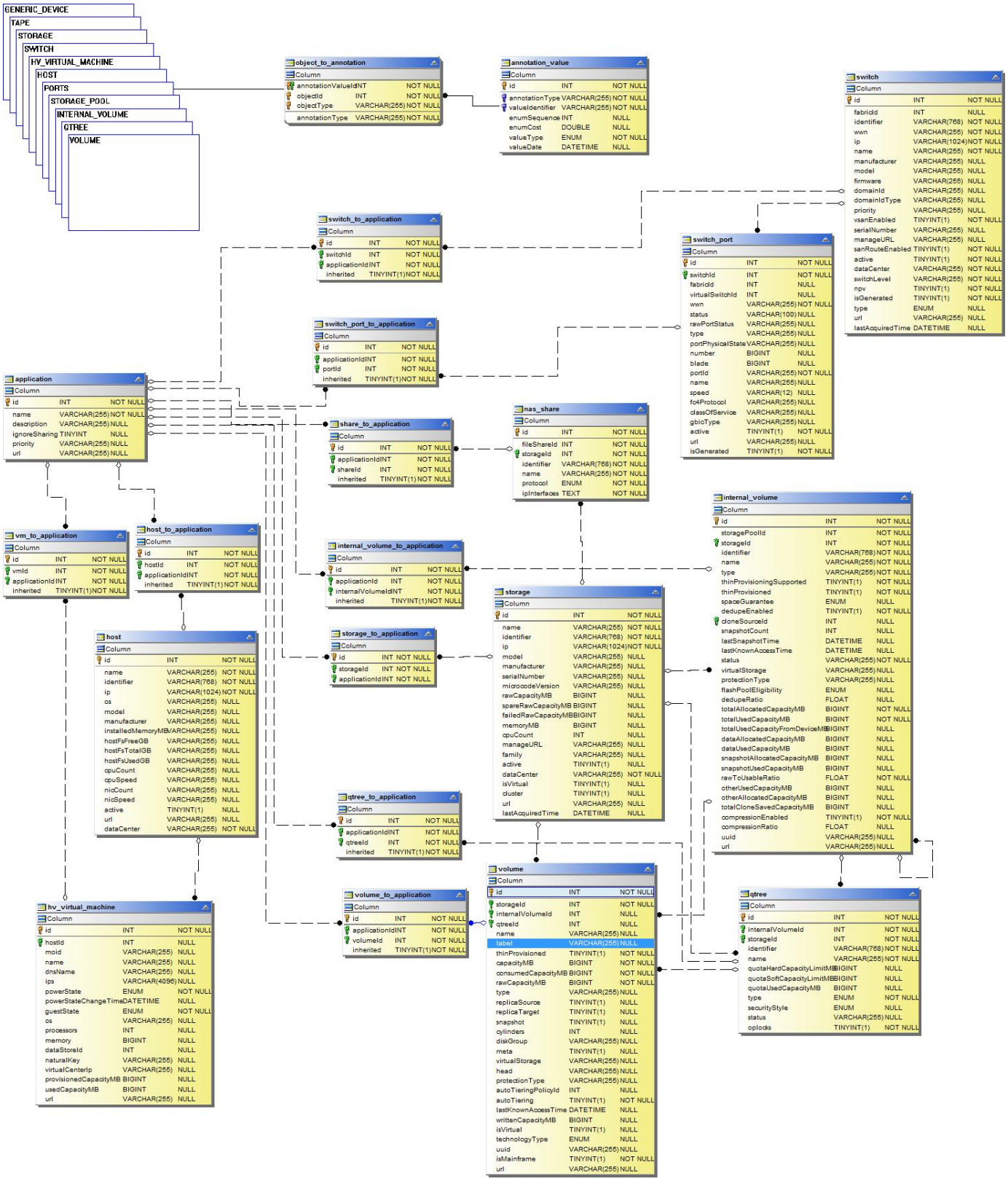
Inventar-Datamart

Die folgenden Bilder beschreiben den Inventar-Datamart.

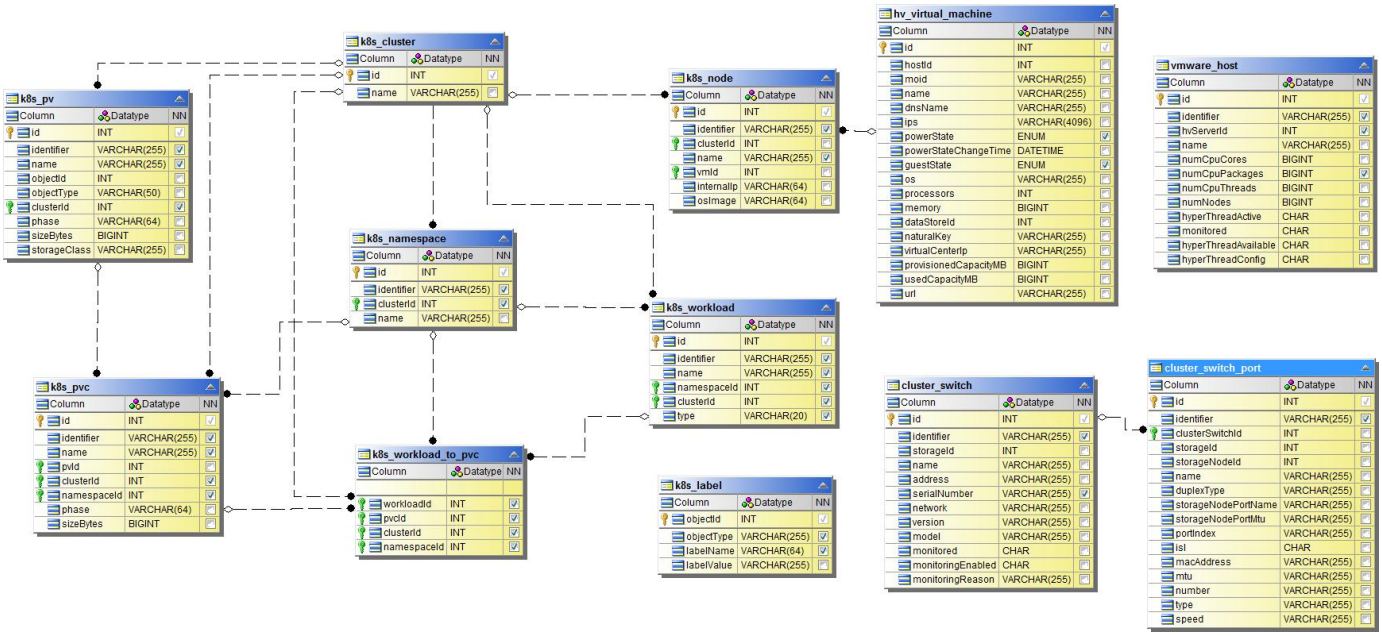
Anmerkungen



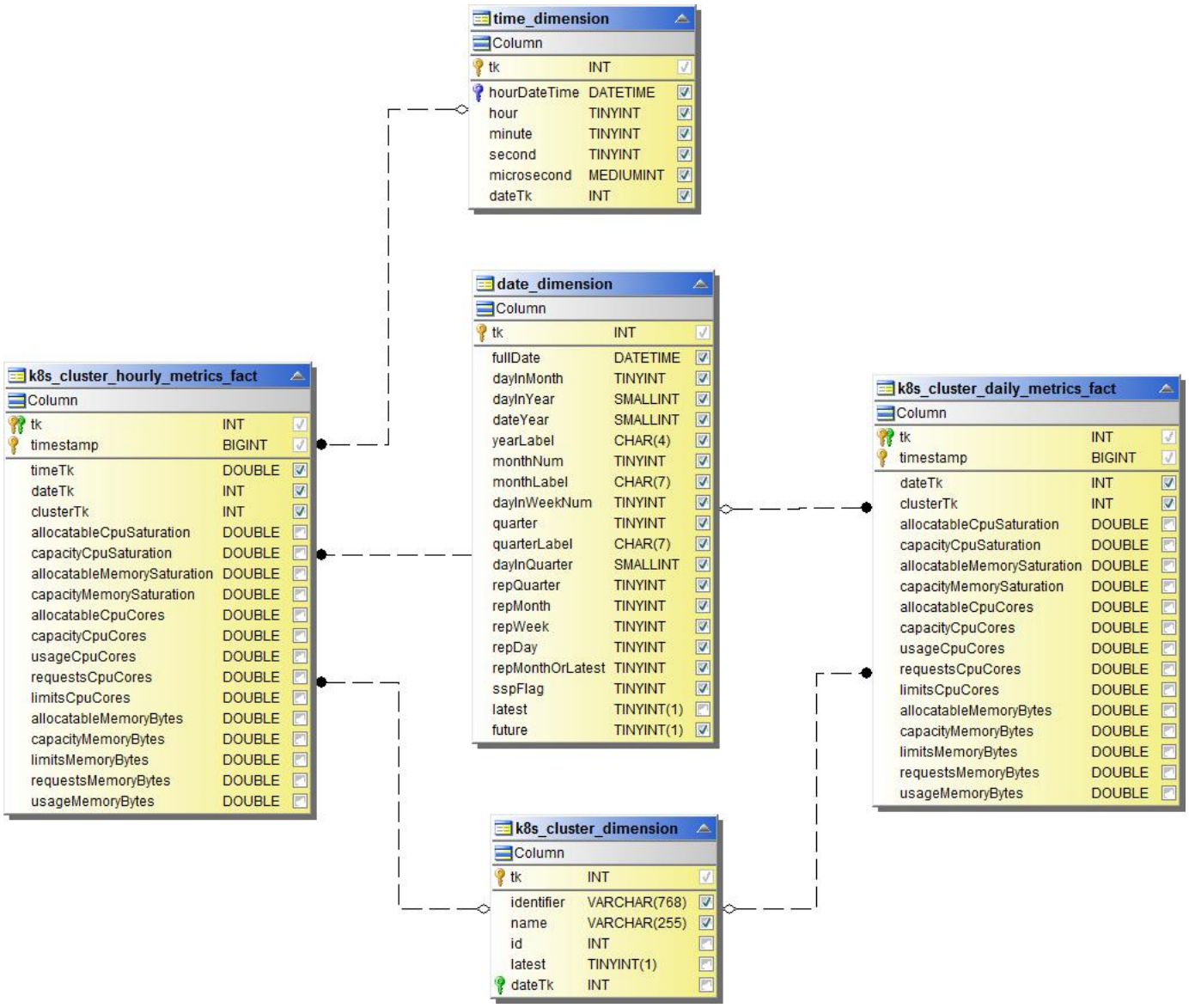
Anwendungen



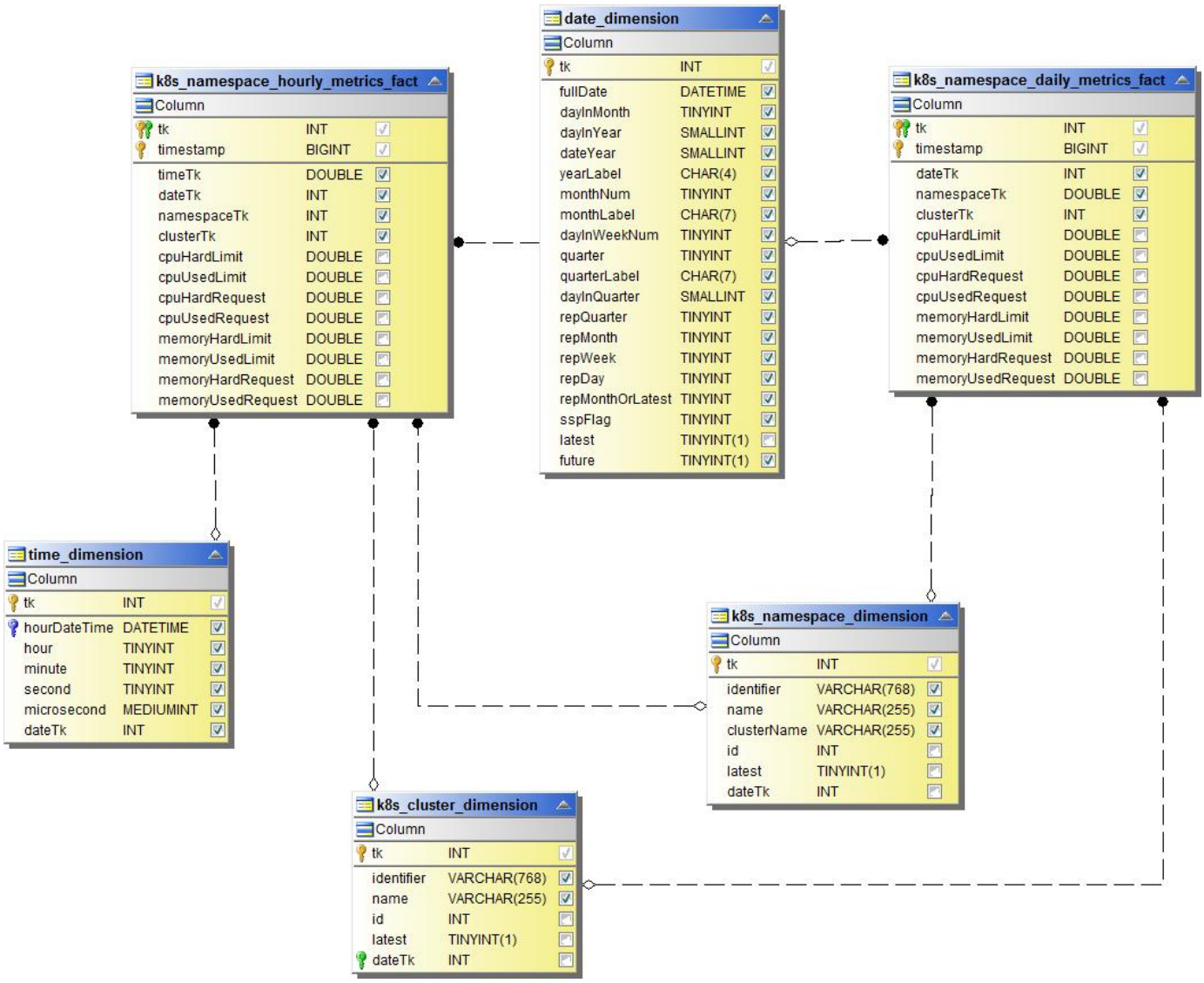
Kubernetes-Metriken



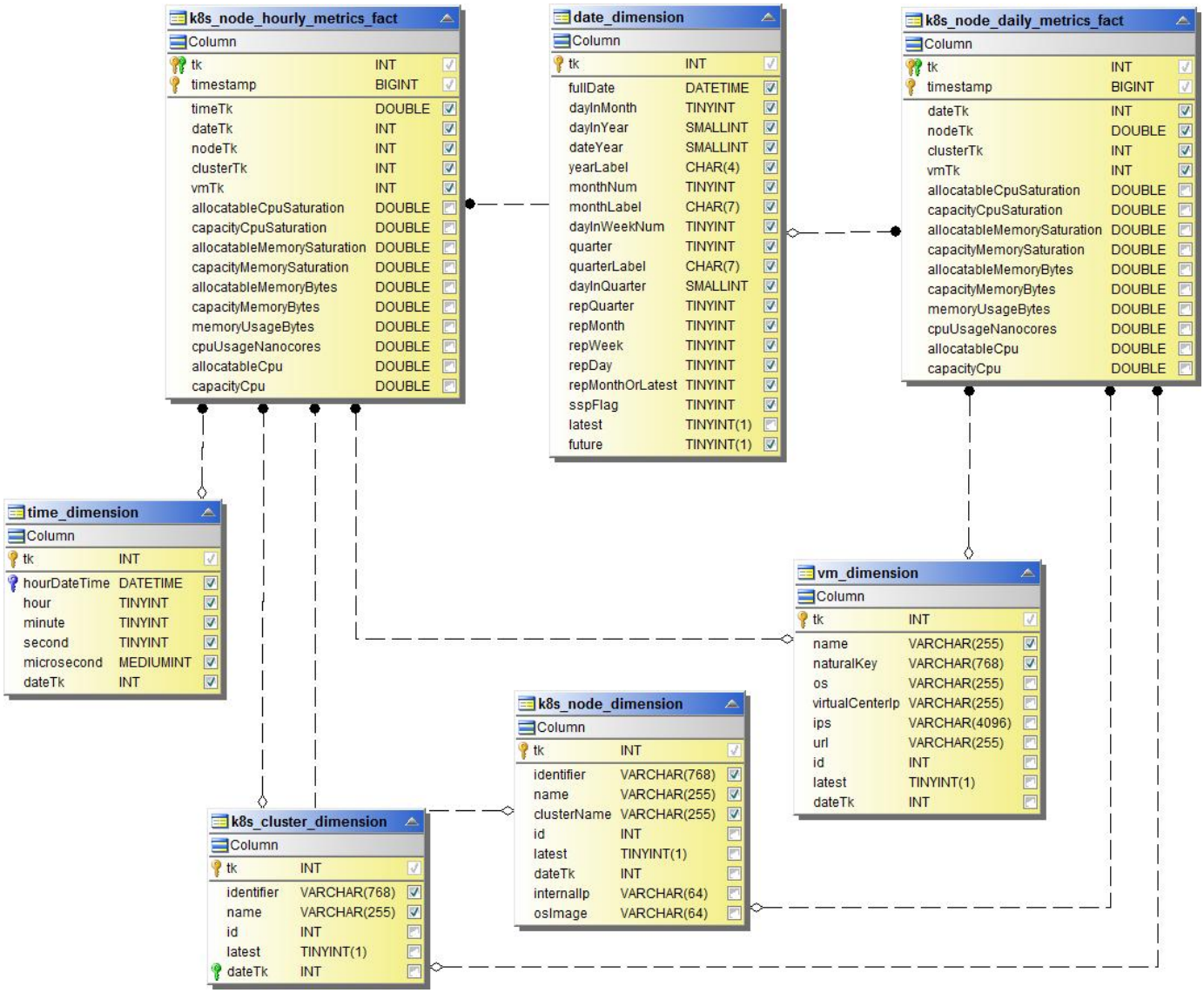
Kubernetes-Clustermetriken – Fakten



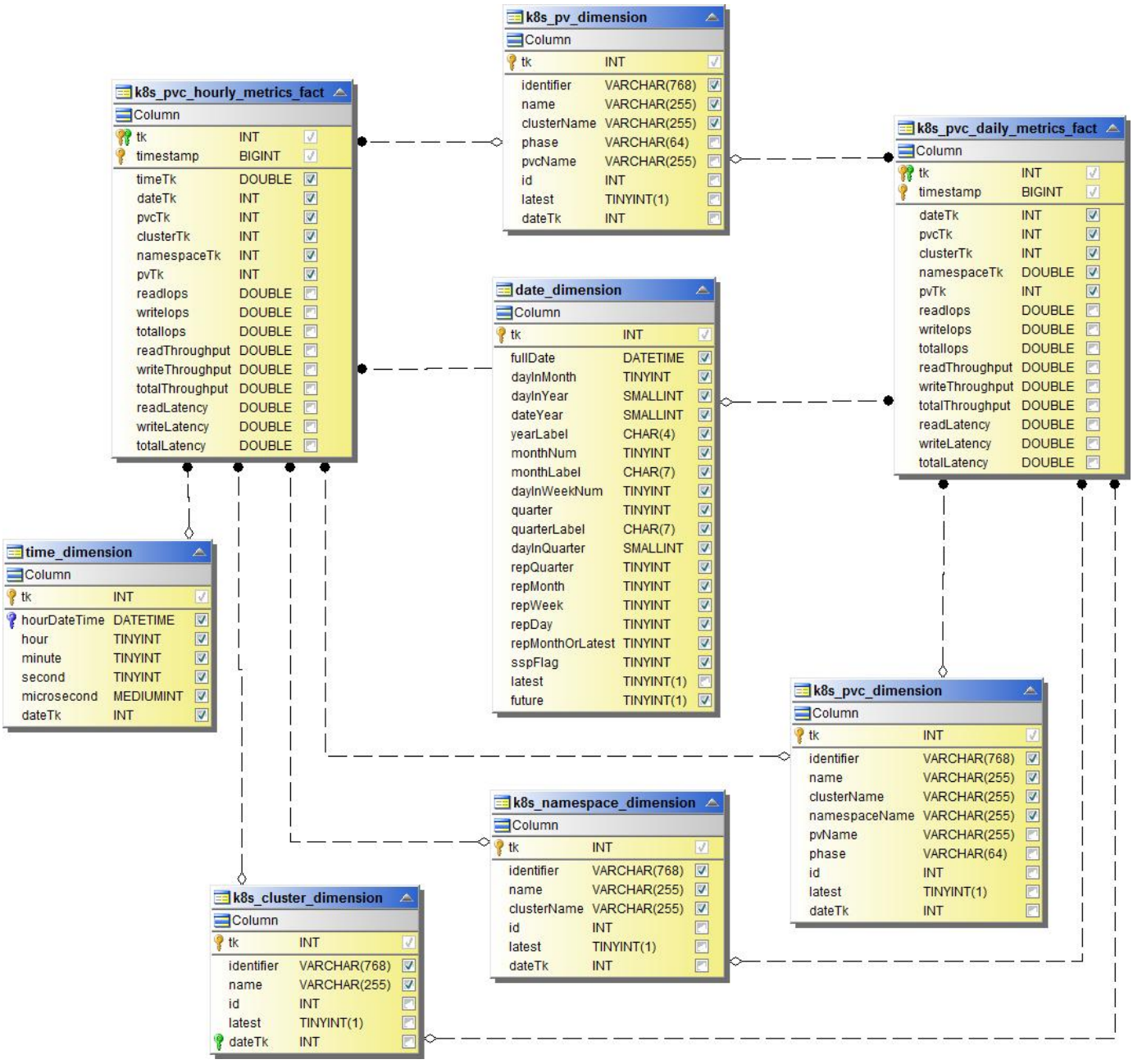
Kubernetes-Namespace-Metriken – Fakten



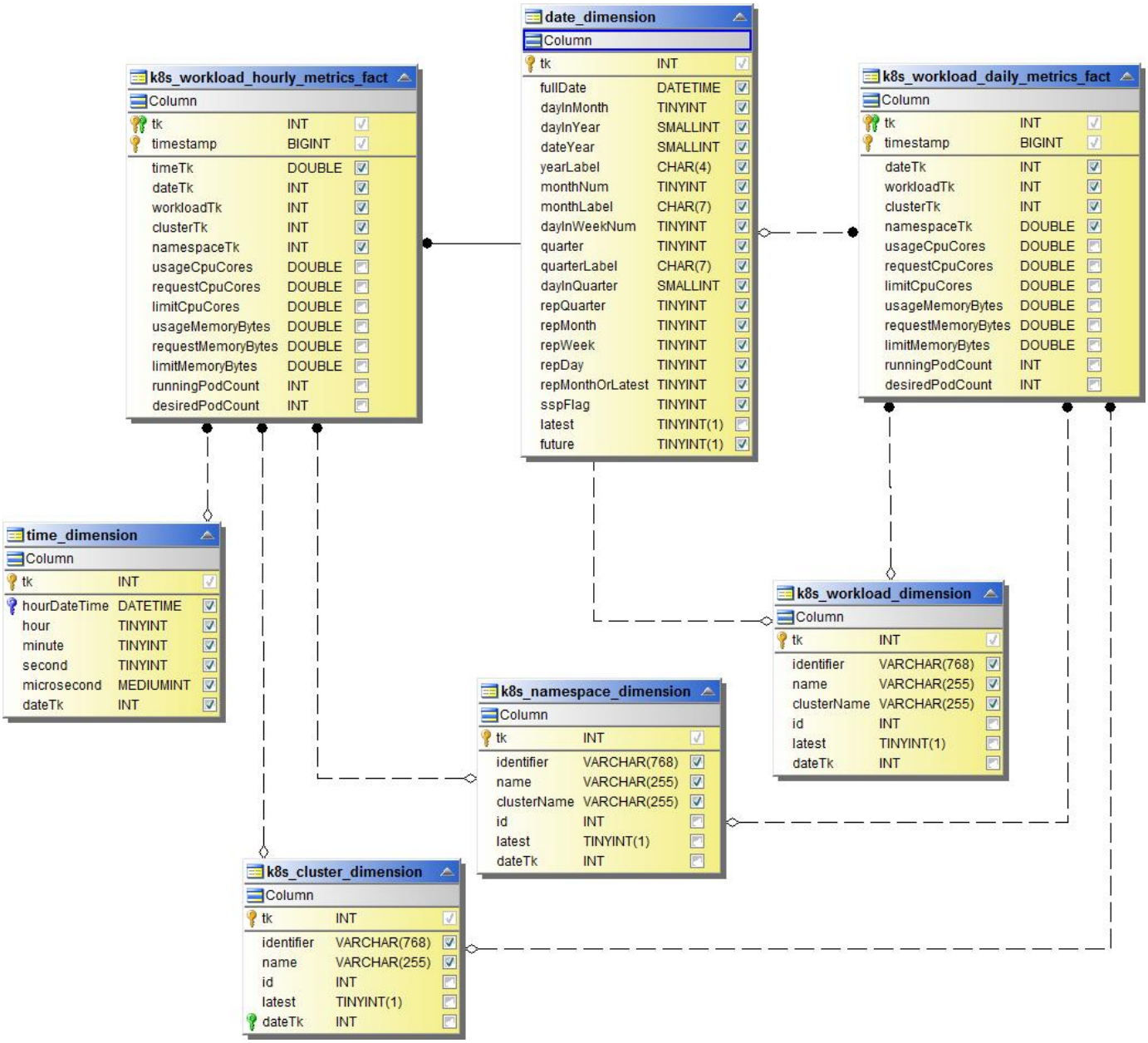
Kubernetes-Knotenmetriken – Fakten



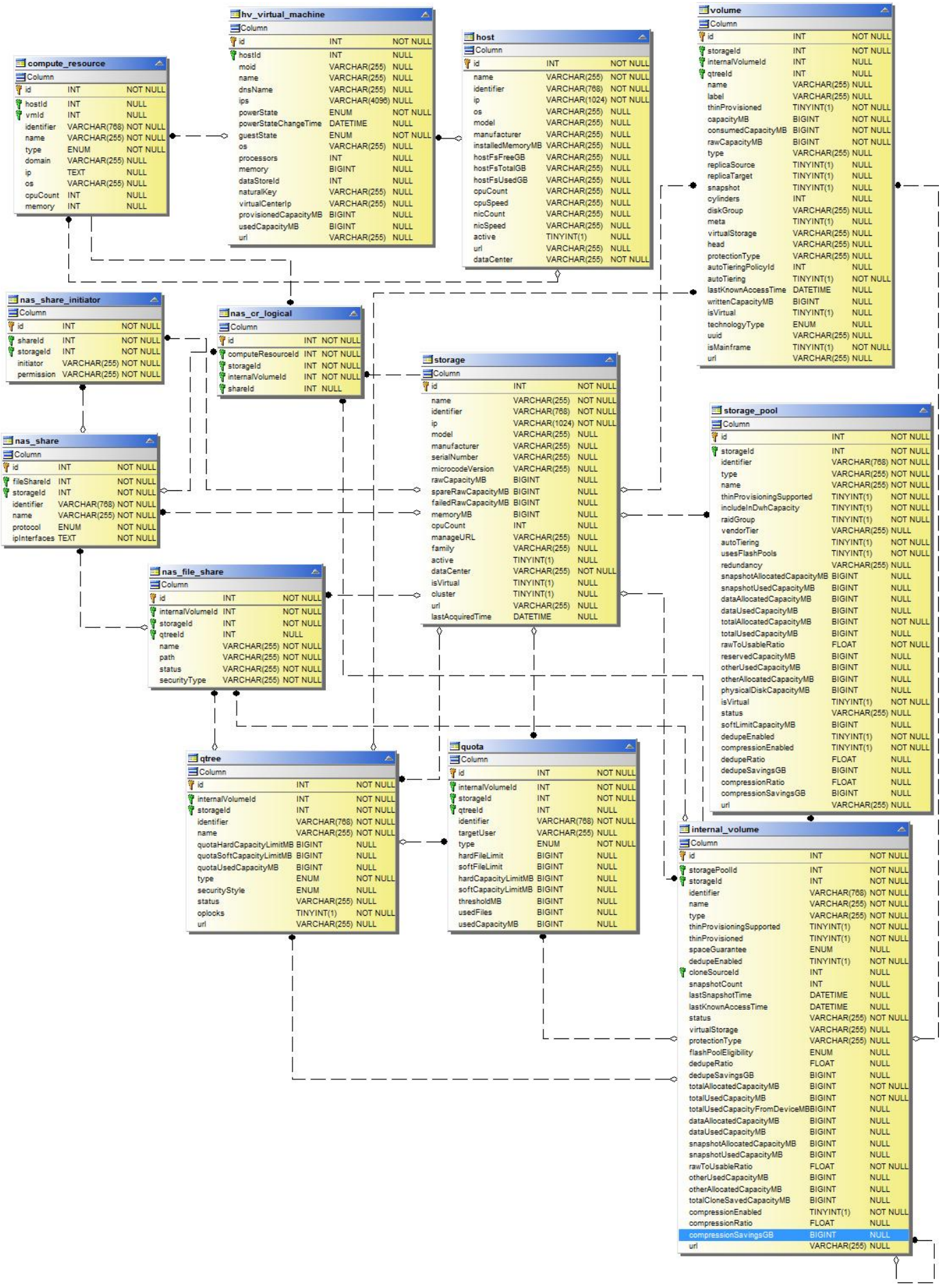
Kubernetes PVC-Metriken-Fakten



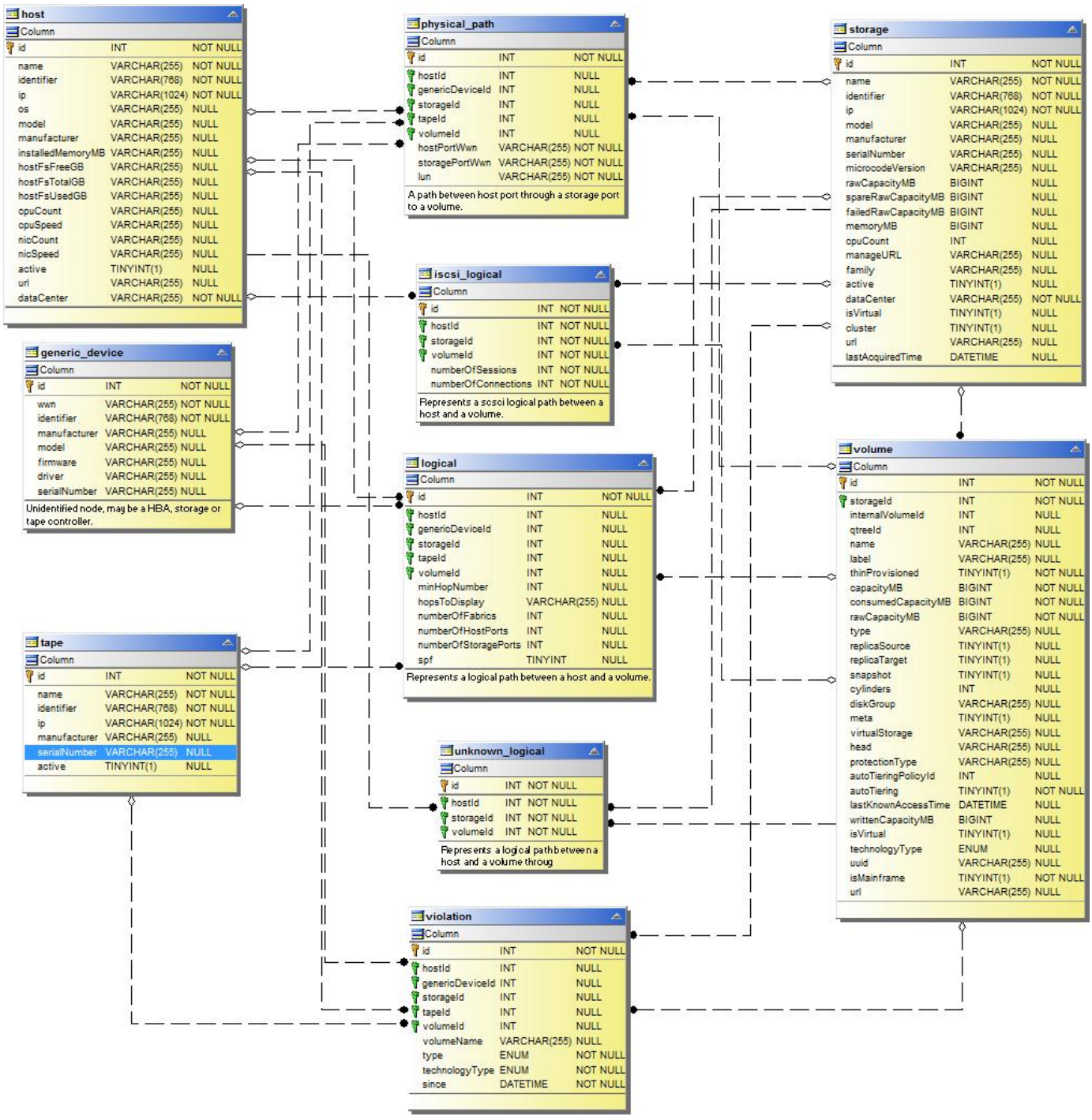
Fakten zu Kubernetes-Workload-Metriken


date_dimension
Column
tk INT
fullDate DATETIME
dayInMonth TINYINT
dayInYear SMALLINT
dateYear SMALLINT
yearLabel CHAR(4)
monthNum TINYINT
monthLabel CHAR(7)
dayInWeekNum TINYINT
quarter TINYINT
quarterLabel CHAR(7)
dayInQuarter SMALLINT
repQuarter TINYINT
repMonth TINYINT
repWeek TINYINT
repDay TINYINT
repMonthOrLatest TINYINT
sspFlag TINYINT
latest TINYINT(1)
future TINYINT(1)
k8s_workload_hourly_metrics_fact
Column
tk INT
timestamp BIGINT
timeTk DOUBLE
dateTk INT
workloadTk INT
clusterTk INT
namespaceTk INT
usageCpuCores DOUBLE
requestCpuCores DOUBLE
limitCpuCores DOUBLE
usageMemoryBytes DOUBLE
requestMemoryBytes DOUBLE
limitMemoryBytes DOUBLE
runningPodCount INT
desiredPodCount INT
k8s_workload_daily_metrics_fact
Column
tk INT
timestamp BIGINT
dateTk INT
workloadTk INT
clusterTk INT
namespaceTk DOUBLE
usageCpuCores DOUBLE
requestCpuCores DOUBLE
limitCpuCores DOUBLE
usageMemoryBytes DOUBLE
requestMemoryBytes DOUBLE
limitMemoryBytes DOUBLE
runningPodCount INT
desiredPodCount INT
time_dimension
Column
tk INT
hourDateTime DATETIME
hour TINYINT
minute TINYINT
second TINYINT
microsecond MEDIUMINT
dateTk INT
k8s_workload_dimension
Column
tk INT
identifier VARCHAR(768)
name VARCHAR(255)
clusterName VARCHAR(255)
id INT
latest TINYINT(1)
dateTk INT
k8s_namespace_dimension
Column
tk INT
identifier VARCHAR(768)
name VARCHAR(255)
clusterName VARCHAR(255)
id INT
latest TINYINT(1)
dateTk INT
k8s_cluster_dimension
Column
tk INT
identifier VARCHAR(768)
name VARCHAR(255)
id INT
latest TINYINT(1)
dateTk INT

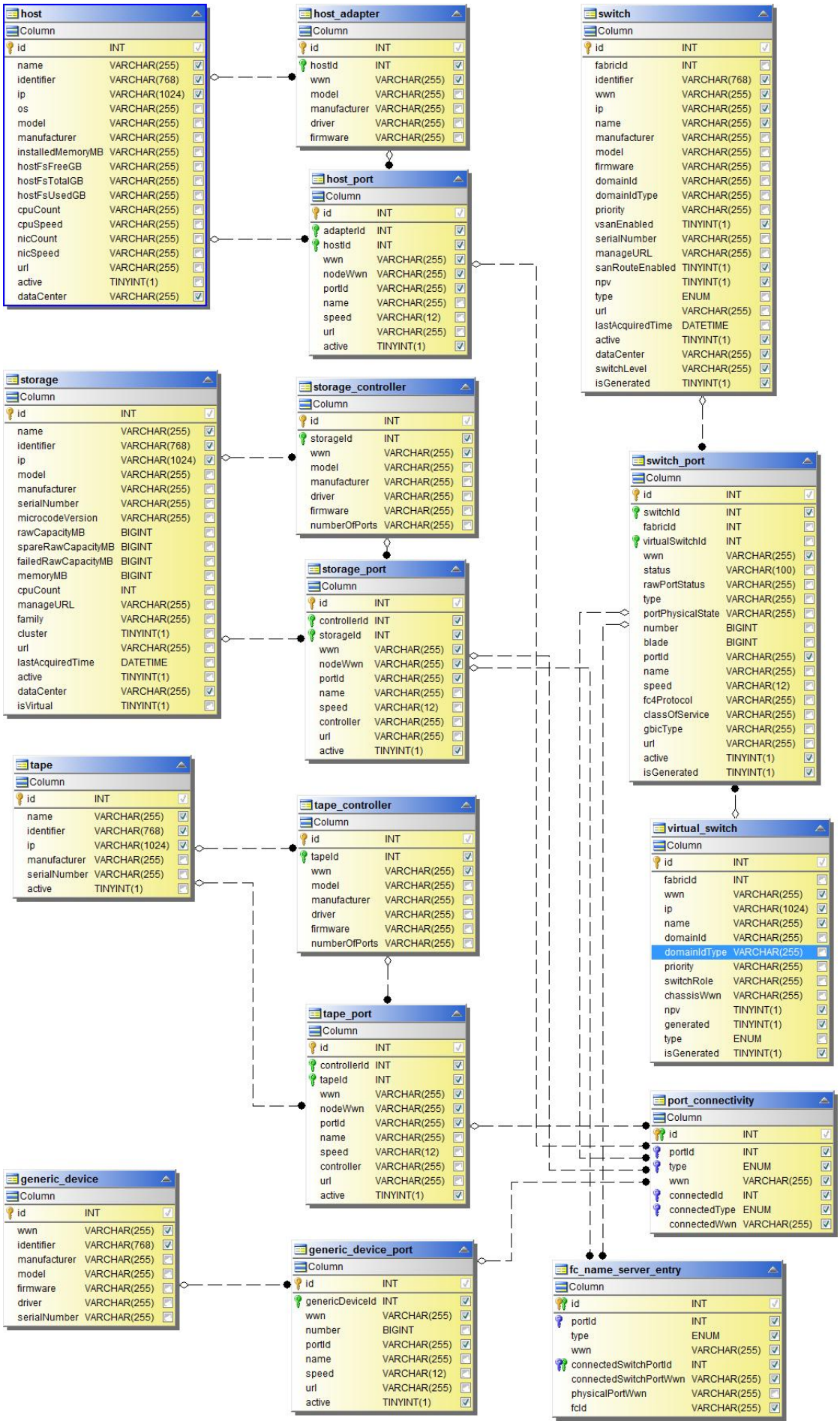
NAS


compute_resource
Column
id INT NOT NULL
hostId INT NULL
vmId INT NULL
identifier VARCHAR(768) NOT NULL
name VARCHAR(255) NOT NULL
type ENUM NOT NULL
domain VARCHAR(255) NULL
ip TEXT NULL
os VARCHAR(255) NULL
cpuCount INT NULL
memory INT NULL
hv_virtual_machine
Column
id INT NOT NULL
hostId INT NULL
moid VARCHAR(255) NULL
name VARCHAR(255) NULL
dnsName VARCHAR(255) NULL
ips VARCHAR(4096) NULL
powerState ENUM NOT NULL
powerStateChangeTime DATETIME NULL
guestState ENUM NOT NULL
os VARCHAR(255) NULL
processors INT NULL
memory BIGINT NULL
dataStoreId INT NULL
naturalKey VARCHAR(255) NULL
virtualCenterIp VARCHAR(255) NULL
provisionedCapacityMB BIGINT NULL
usedCapacityMB BIGINT NULL
url VARCHAR(255) NULL
host
Column
id INT NOT NULL
name VARCHAR(255) NOT NULL
identifier VARCHAR(768) NOT NULL
ip VARCHAR(1024) NOT NULL
os VARCHAR(255) NULL
model VARCHAR(255) NULL
manufacturer VARCHAR(255) NULL
installedMemoryMB VARCHAR(255) NULL
hostFsFreeGB VARCHAR(255) NULL
hostFsTotalGB VARCHAR(255) NULL
hostFsUsedGB VARCHAR(255) NULL
cpuCount VARCHAR(255) NULL
cpuSpeed VARCHAR(255) NULL
nicCount VARCHAR(255) NULL
nicSpeed VARCHAR(255) NULL
active TINYINT(1) NULL
url VARCHAR(255) NULL
dataCenter VARCHAR(255) NOT NULL
volume
Column
id INT NOT NULL
storageId INT NOT NULL
internalVolumeId INT NULL
qtreeId INT NULL
name VARCHAR(255) NULL
label VARCHAR(255) NULL
thinProvisioned TINYINT(1) NOT NULL
capacityMB BIGINT NOT NULL
consumedCapacityMB BIGINT NOT NULL
rawCapacityMB BIGINT NOT NULL
type VARCHAR(255) NULL
replicaSource TINYINT(1) NULL
replicaTarget TINYINT(1) NULL
snapshot TINYINT(1) NULL
cylinders INT NULL
diskGroup VARCHAR(255) NULL
meta TINYINT(1) NULL
virtualStorage VARCHAR(255) NULL
head VARCHAR(255) NULL
protectionType VARCHAR(255) NULL
autoTieringPolicyId INT NULL
autoTiering TINYINT(1) NOT NULL
lastKnownAccessTime DATETIME NULL
writtenCapacityMB BIGINT NULL
isVirtual TINYINT(1) NULL
technologyType ENUM NULL
uuid VARCHAR(255) NULL
isMainframe TINYINT(1) NOT NULL
url VARCHAR(255) NULL
nas_share_initiator
Column
id INT NOT NULL
shareId INT NOT NULL
storageId INT NOT NULL
initiator VARCHAR(255) NOT NULL
permission VARCHAR(255) NOT NULL
nas_cr_logical
Column
id INT NOT NULL
computeResourceId INT NOT NULL
storageId INT NOT NULL
internalVolumeId INT NOT NULL
shareId INT NULL
storage
Column
id INT NOT NULL
name VARCHAR(255) NOT NULL
identifier VARCHAR(768) NOT NULL
ip VARCHAR(1024) NOT NULL
model VARCHAR(255) NULL
manufacturer VARCHAR(255) NULL
serialNumber VARCHAR(255) NULL
microcodeVersion VARCHAR(255) NULL
rawCapacityMB BIGINT NULL
spareRawCapacityMB BIGINT NULL
failedRawCapacityMB BIGINT NULL
memoryMB BIGINT NULL
cpuCount INT NULL
manageURL VARCHAR(255) NULL
family VARCHAR(255) NULL
active TINYINT(1) NULL
dataCenter VARCHAR(255) NOT NULL
isVirtual TINYINT(1) NULL
cluster TINYINT(1) NULL
url VARCHAR(255) NULL
lastAcquiredTime DATETIME NULL
storage_pool
Column
id INT NOT NULL
storageId INT NOT NULL
identifier VARCHAR(768) NOT NULL
type VARCHAR(255) NOT NULL
name VARCHAR(255) NOT NULL
thinProvisioningSupported TINYINT(1) NOT NULL
includeInDwhCapacity TINYINT(1) NOT NULL
raidGroup TINYINT(1) NOT NULL
vendorTier VARCHAR(255) NULL
autoTiering TINYINT(1) NOT NULL
usesFlashPools TINYINT(1) NOT NULL
redundancy VARCHAR(255) NULL
snapshotAllocatedCapacityMB BIGINT NULL
snapshotUsedCapacityMB BIGINT NULL
dataAllocatedCapacityMB BIGINT NULL
dataUsedCapacityMB BIGINT NULL
totalAllocatedCapacityMB BIGINT NOT NULL
totalUsedCapacityMB BIGINT NULL
rawToUsableRatio FLOAT NOT NULL
reservedCapacityMB BIGINT NULL
otherUsedCapacityMB BIGINT NULL
otherAllocatedCapacityMB BIGINT NULL
physicalDiskCapacityMB BIGINT NULL
isVirtual TINYINT(1) NOT NULL
status VARCHAR(255) NULL
softLimitCapacityMB BIGINT NULL
dedupeEnabled TINYINT(1) NOT NULL
compressionEnabled TINYINT(1) NOT NULL
dedupeRatio FLOAT NULL
dedupeSavingsGB BIGINT NULL
compressionRatio FLOAT NULL
compressionSavingsGB BIGINT NULL
url VARCHAR(255) NULL
nas_share
Column
id INT NOT NULL
fileShareId INT NOT NULL
storageId INT NOT NULL
identifier VARCHAR(768) NOT NULL
name VARCHAR(255) NOT NULL
protocol ENUM NOT NULL
ipInterfaces TEXT NOT NULL
nas_file_share
Column
id INT NOT NULL
internalVolumeId INT NOT NULL
storageId INT NOT NULL
qtreeId INT NULL
name VARCHAR(255) NOT NULL
path VARCHAR(255) NOT NULL
status VARCHAR(255) NOT NULL
securityType VARCHAR(255) NOT NULL
qtree
Column
id INT NOT NULL
internalVolumeId INT NOT NULL
storageId INT NOT NULL
identifier VARCHAR(768) NOT NULL
name VARCHAR(255) NOT NULL
quotaHardCapacityLimitMB BIGINT NULL
quotaSoftCapacityLimitMB BIGINT NULL
quotaUsedCapacityMB BIGINT NULL
type ENUM NOT NULL
securityStyle ENUM NULL
status VARCHAR(255) NULL
oplocks TINYINT(1) NOT NULL
url VARCHAR(255) NULL
quota
Column
id INT NOT NULL
internalVolumeId INT NOT NULL
storageId INT NOT NULL
qtreeId INT NULL
identifier VARCHAR(768) NOT NULL
targetUser VARCHAR(255) NULL
type ENUM NOT NULL
hardFileLimit BIGINT NULL
softFileLimit BIGINT NULL
hardCapacityLimitMB BIGINT NULL
softCapacityLimitMB BIGINT NULL
thresholdMB BIGINT NULL
usedFiles BIGINT NULL
usedCapacityMB BIGINT NULL
internal_volume
Column
id INT NOT NULL
storagePoolId INT NOT NULL
storageId INT NOT NULL
identifier VARCHAR(768) NOT NULL
name VARCHAR(255) NOT NULL
type VARCHAR(255) NOT NULL
thinProvisioningSupported TINYINT(1) NOT NULL
thinProvisioned TINYINT(1) NOT NULL
spaceGuarantee ENUM NULL
dedupeEnabled TINYINT(1) NOT NULL
cloneSourceId INT NULL
snapshotCount INT NULL
lastSnapshotTime DATETIME NULL
lastKnownAccessTime DATETIME NULL
status VARCHAR(255) NOT NULL
virtualStorage VARCHAR(255) NULL
protectionType VARCHAR(255) NULL
flashPoolEligibility ENUM NULL
dedupeRatio FLOAT NULL
dedupeSavingsGB BIGINT NULL
totalAllocatedCapacityMB BIGINT NOT NULL
totalUsedCapacityMB BIGINT NOT NULL
totalUsedCapacityFromDeviceMB BIGINT NULL
dataAllocatedCapacityMB BIGINT NULL
dataUsedCapacityMB BIGINT NULL
snapshotAllocatedCapacityMB BIGINT NULL
snapshotUsedCapacityMB BIGINT NULL
rawToUsableRatio FLOAT NOT NULL
otherUsedCapacityMB BIGINT NULL
otherAllocatedCapacityMB BIGINT NULL
totalCloneSavedCapacityMB BIGINT NULL
compressionEnabled TINYINT(1) NOT NULL
compressionRatio FLOAT NULL
compressionSavingsGB BIGINT NULL
url VARCHAR(255) NULL

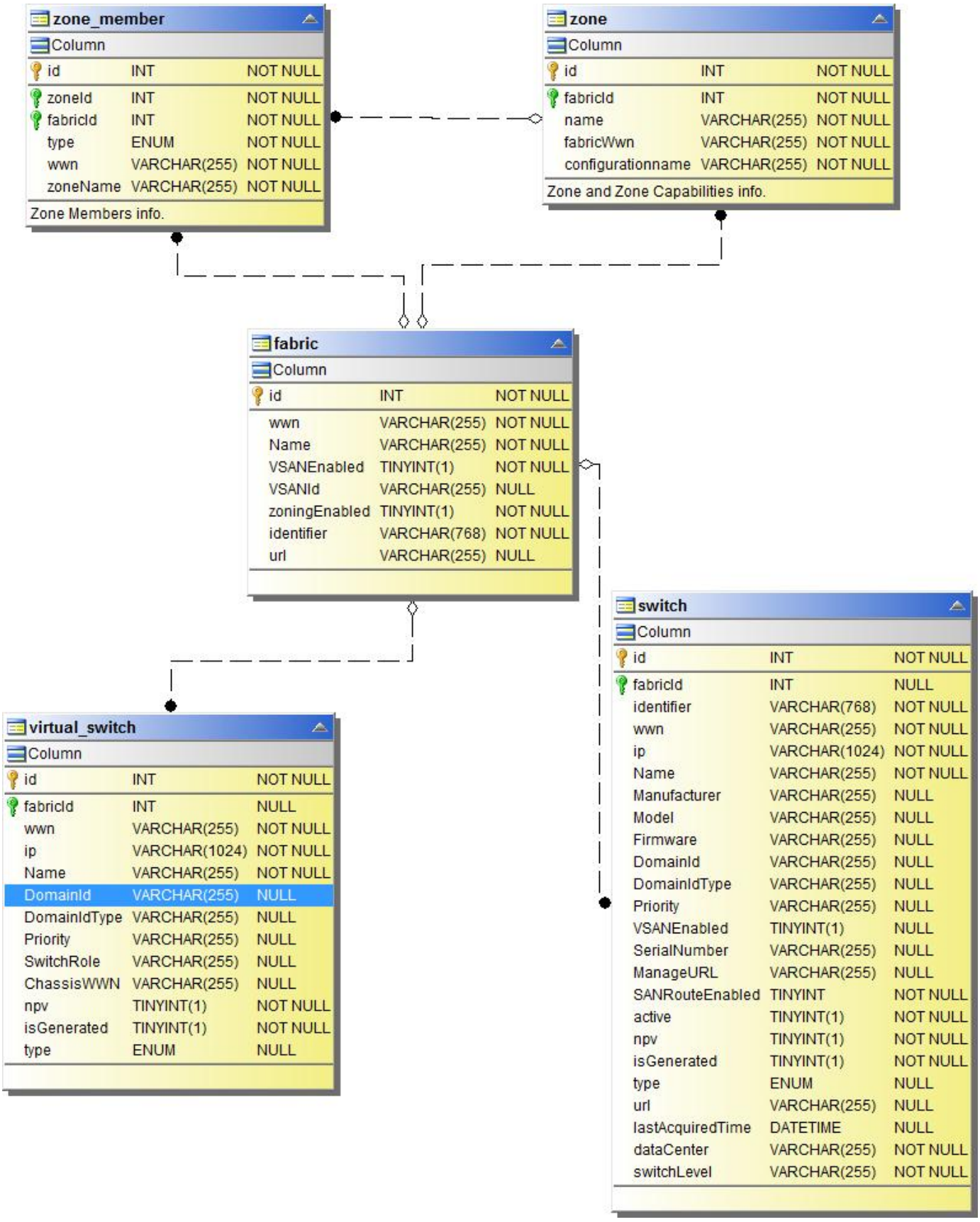
Pfade und Verstöße



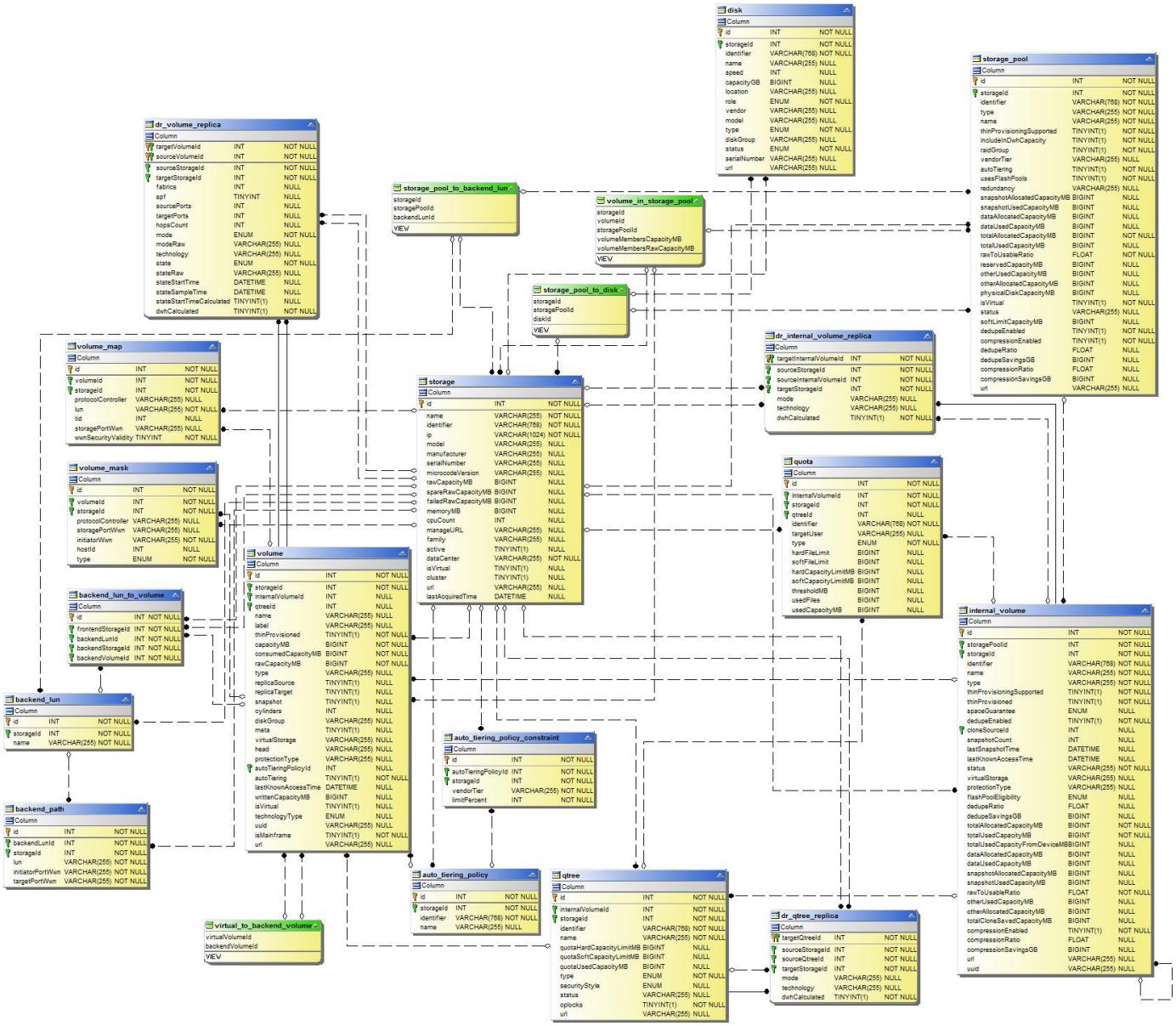
Port-Konnektivität


host
Column
id INT
name VARCHAR(255)
identifier VARCHAR(768)
ip VARCHAR(1024)
os VARCHAR(255)
model VARCHAR(255)
manufacturer VARCHAR(255)
installedMemoryMB VARCHAR(255)
hostFsFreeGB VARCHAR(255)
hostFsTotalGB VARCHAR(255)
hostFsUsedGB VARCHAR(255)
cpuCount VARCHAR(255)
cpuSpeed VARCHAR(255)
nicCount VARCHAR(255)
nicSpeed VARCHAR(255)
url VARCHAR(255)
active TINYINT(1)
dataCenter VARCHAR(255)
host_adapter
Column
id INT
hostId INT
wwn VARCHAR(255)
model VARCHAR(255)
manufacturer VARCHAR(255)
driver VARCHAR(255)
firmware VARCHAR(255)
host_port
Column
id INT
adapterId INT
hostId INT
wwn VARCHAR(255)
nodeWwn VARCHAR(255)
portId VARCHAR(255)
name VARCHAR(255)
speed VARCHAR(12)
url VARCHAR(255)
active TINYINT(1)
switch
Column
id INT
fabricId INT
identifier VARCHAR(768)
wwn VARCHAR(255)
ip VARCHAR(255)
name VARCHAR(255)
manufacturer VARCHAR(255)
model VARCHAR(255)
firmware VARCHAR(255)
domainId VARCHAR(255)
domainIdType VARCHAR(255)
priority VARCHAR(255)
vsanEnabled TINYINT(1)
serialNumber VARCHAR(255)
manageURL VARCHAR(255)
sanRouteEnabled TINYINT(1)
npv TINYINT(1)
type ENUM
url VARCHAR(255)
lastAcquiredTime DATETIME
active TINYINT(1)
dataCenter VARCHAR(255)
switchLevel VARCHAR(255)
isGenerated TINYINT(1)
storage
Column
id INT
name VARCHAR(255)
identifier VARCHAR(768)
ip VARCHAR(1024)
model VARCHAR(255)
manufacturer VARCHAR(255)
serialNumber VARCHAR(255)
microcodeVersion VARCHAR(255)
rawCapacityMB BIGINT
spareRawCapacityMB BIGINT
failedRawCapacityMB BIGINT
memoryMB BIGINT
cpuCount INT
manageURL VARCHAR(255)
family VARCHAR(255)
cluster TINYINT(1)
url VARCHAR(255)
lastAcquiredTime DATETIME
active TINYINT(1)
dataCenter VARCHAR(255)
isVirtual TINYINT(1)
storage_controller
Column
id INT
storageId INT
wwn VARCHAR(255)
model VARCHAR(255)
manufacturer VARCHAR(255)
driver VARCHAR(255)
firmware VARCHAR(255)
numberOfPorts VARCHAR(255)
storage_port
Column
id INT
controllerId INT
storageId INT
wwn VARCHAR(255)
nodeWwn VARCHAR(255)
portId VARCHAR(255)
name VARCHAR(255)
speed VARCHAR(12)
controller VARCHAR(255)
url VARCHAR(255)
active TINYINT(1)
switch_port
Column
id INT
switchId INT
fabricId INT
virtualSwitchId INT
wwn VARCHAR(255)
status VARCHAR(100)
rawPortStatus VARCHAR(255)
type VARCHAR(255)
portPhysicalState VARCHAR(255)
number BIGINT
blade BIGINT
portId VARCHAR(255)
name VARCHAR(255)
speed VARCHAR(12)
fc4Protocol VARCHAR(255)
classOfService VARCHAR(255)
gbicType VARCHAR(255)
url VARCHAR(255)
active TINYINT(1)
isGenerated TINYINT(1)
tape
Column
id INT
name VARCHAR(255)
identifier VARCHAR(768)
ip VARCHAR(1024)
manufacturer VARCHAR(255)
serialNumber VARCHAR(255)
active TINYINT(1)
tape_controller
Column
id INT
tapeId INT
wwn VARCHAR(255)
model VARCHAR(255)
manufacturer VARCHAR(255)
driver VARCHAR(255)
firmware VARCHAR(255)
numberOfPorts VARCHAR(255)
virtual_switch
Column
id INT
fabricId INT
wwn VARCHAR(255)
ip VARCHAR(1024)
name VARCHAR(255)
domainId VARCHAR(255)
domainIdType VARCHAR(255)
priority VARCHAR(255)
switchRole VARCHAR(255)
chassisWwn VARCHAR(255)
npv TINYINT(1)
generated TINYINT(1)
type ENUM
isGenerated TINYINT(1)
tape_port
Column
id INT
controllerId INT
tapeId INT
wwn VARCHAR(255)
nodeWwn VARCHAR(255)
portId VARCHAR(255)
name VARCHAR(255)
speed VARCHAR(12)
controller VARCHAR(255)
url VARCHAR(255)
active TINYINT(1)
port_connectivity
Column
id INT
portId INT
type ENUM
wwn VARCHAR(255)
connectedId INT
connectedType ENUM
connectedWwn VARCHAR(255)
generic_device
Column
id INT
wwn VARCHAR(255)
identifier VARCHAR(768)
manufacturer VARCHAR(255)
model VARCHAR(255)
firmware VARCHAR(255)
driver VARCHAR(255)
serialNumber VARCHAR(255)
generic_device_port
Column
id INT
genericDeviceId INT
wwn VARCHAR(255)
number BIGINT
portId VARCHAR(255)
name VARCHAR(255)
speed VARCHAR(12)
url VARCHAR(255)
active TINYINT(1)
fc_name_server_entry
Column
id INT
portId INT
type ENUM
wwn VARCHAR(255)
connectedSwitchPortId INT
connectedSwitchPortWwn VARCHAR(255)
physicalPortWwn VARCHAR(255)
fcId VARCHAR(255)

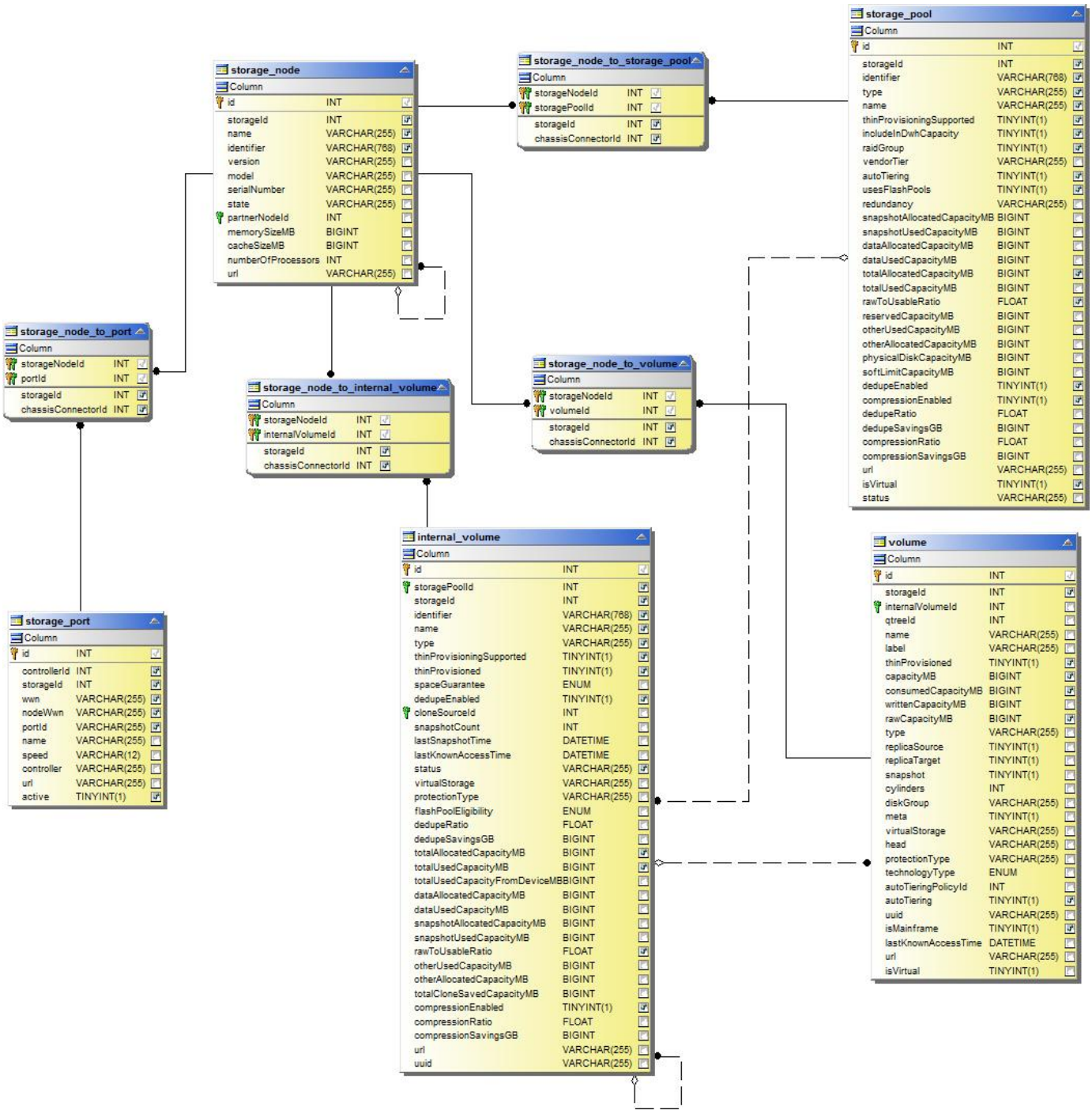
SAN-Gewebe


zone_member
Column
id INT NOT NULL
zoneId INT NOT NULL
fabricId INT NOT NULL
type ENUM NOT NULL
wwn VARCHAR(255) NOT NULL
zoneName VARCHAR(255) NOT NULL
Zone Members info.
zone
Column
id INT NOT NULL
fabricId INT NOT NULL
name VARCHAR(255) NOT NULL
fabricWwn VARCHAR(255) NOT NULL
configurationname VARCHAR(255) NOT NULL
Zone and Zone Capabilities info.
fabric
Column
id INT NOT NULL
wwn VARCHAR(255) NOT NULL
Name VARCHAR(255) NOT NULL
VSANEnabled TINYINT(1) NOT NULL
VSANId VARCHAR(255) NULL
zoningEnabled TINYINT(1) NOT NULL
identifier VARCHAR(768) NOT NULL
url VARCHAR(255) NULL
switch
Column
id INT NOT NULL
fabricId INT NULL
identifier VARCHAR(768) NOT NULL
wwn VARCHAR(255) NOT NULL
ip VARCHAR(1024) NOT NULL
Name VARCHAR(255) NOT NULL
Manufacturer VARCHAR(255) NULL
Model VARCHAR(255) NULL
Firmware VARCHAR(255) NULL
DomainId VARCHAR(255) NULL
DomainIdType VARCHAR(255) NULL
Priority VARCHAR(255) NULL
VSANEnabled TINYINT(1) NULL
SerialNumber VARCHAR(255) NULL
ManageURL VARCHAR(255) NULL
SANRouteEnabled TINYINT NOT NULL
active TINYINT(1) NOT NULL
npv TINYINT(1) NOT NULL
isGenerated TINYINT(1) NOT NULL
type ENUM NULL
url VARCHAR(255) NULL
lastAcquiredTime DATETIME NULL
dataCenter VARCHAR(255) NOT NULL
switchLevel VARCHAR(255) NOT NULL
virtual_switch
Column
id INT NOT NULL
fabricId INT NULL
wwn VARCHAR(255) NOT NULL
ip VARCHAR(1024) NOT NULL
Name VARCHAR(255) NOT NULL
DomainId VARCHAR(255) NULL
DomainIdType VARCHAR(255) NULL
Priority VARCHAR(255) NULL
SwitchRole VARCHAR(255) NULL
ChassisWWN VARCHAR(255) NULL
npv TINYINT(1) NOT NULL
isGenerated TINYINT(1) NOT NULL
type ENUM NULL

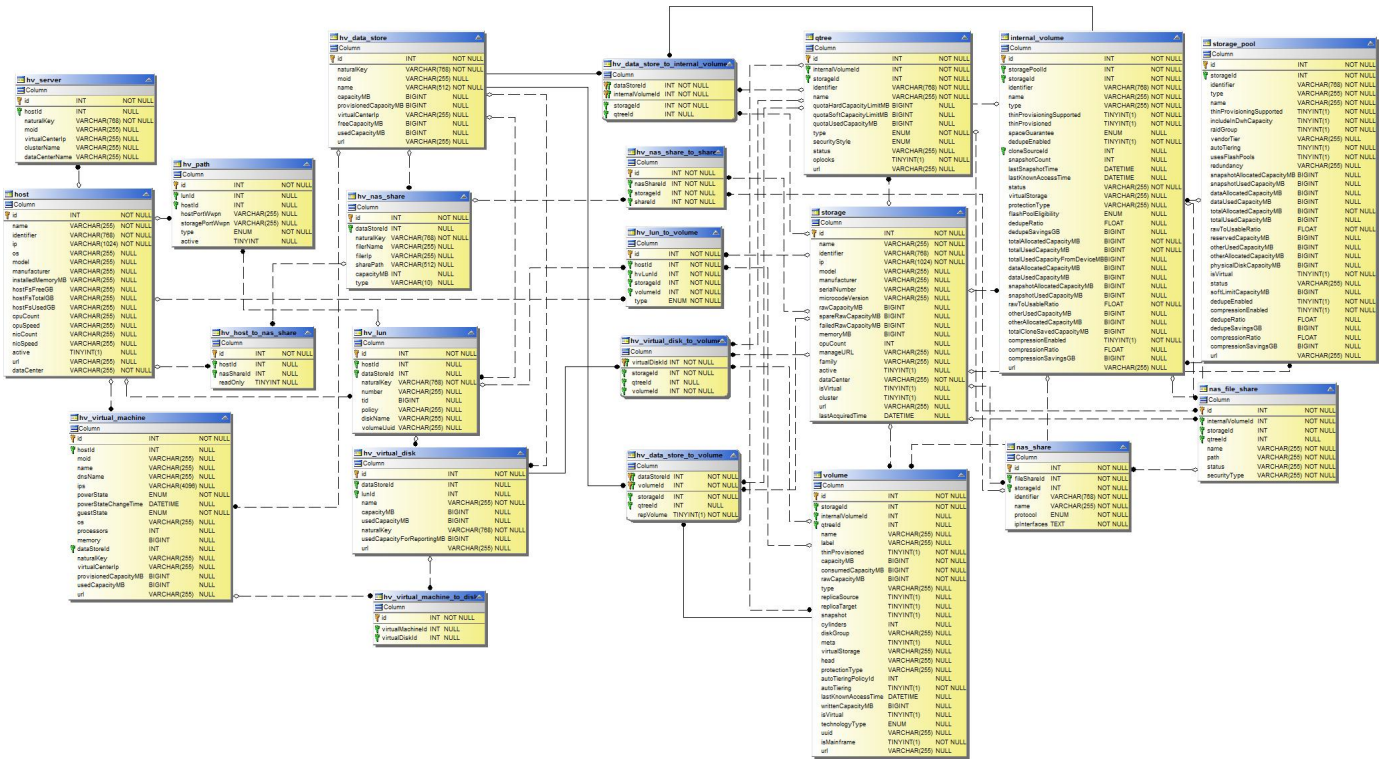
Storage



Speicherknoten


storage_node
Column
id INT
storageId INT
name VARCHAR(255)
identifier VARCHAR(768)
version VARCHAR(255)
model VARCHAR(255)
serialNumber VARCHAR(255)
state VARCHAR(255)
partnerNodeId INT
memorySizeMB BIGINT
cacheSizeMB BIGINT
numberOfProcessors INT
url VARCHAR(255)
storage_node_to_storage_pool
Column
storageNodeId INT
storagePoolId INT
storageId INT
chassisConnectorId INT
storage_pool
Column
id INT
storageId INT
identifier VARCHAR(768)
type VARCHAR(255)
name VARCHAR(255)
thinProvisioningSupported TINYINT(1)
includeInDwhCapacity TINYINT(1)
raidGroup TINYINT(1)
vendorTier VARCHAR(255)
autoTiering TINYINT(1)
usesFlashPools TINYINT(1)
redundancy VARCHAR(255)
snapshotAllocatedCapacityMB BIGINT
snapshotUsedCapacityMB BIGINT
dataAllocatedCapacityMB BIGINT
dataUsedCapacityMB BIGINT
totalAllocatedCapacityMB BIGINT
totalUsedCapacityMB BIGINT
rawToUsableRatio FLOAT
reservedCapacityMB BIGINT
otherUsedCapacityMB BIGINT
otherAllocatedCapacityMB BIGINT
physicalDiskCapacityMB BIGINT
softLimitCapacityMB BIGINT
dedupeEnabled TINYINT(1)
compressionEnabled TINYINT(1)
dedupeRatio FLOAT
dedupeSavingsGB BIGINT
compressionRatio FLOAT
compressionSavingsGB BIGINT
url VARCHAR(255)
isVirtual TINYINT(1)
status VARCHAR(255)
storage_node_to_port
Column
storageNodeId INT
portId INT
storageId INT
chassisConnectorId INT
storage_node_to_internal_volume
Column
storageNodeId INT
internalVolumeId INT
storageId INT
chassisConnectorId INT
storage_node_to_volume
Column
storageNodeId INT
volumeId INT
storageId INT
chassisConnectorId INT
internal_volume
Column
id INT
storagePoolId INT
storageId INT
identifier VARCHAR(768)
name VARCHAR(255)
type VARCHAR(255)
thinProvisioningSupported TINYINT(1)
thinProvisioned TINYINT(1)
spaceGuarantee ENUM
dedupeEnabled TINYINT(1)
cloneSourceId INT
snapshotCount INT
lastSnapshotTime DATETIME
lastKnownAccessTime DATETIME
status VARCHAR(255)
virtualStorage VARCHAR(255)
protectionType VARCHAR(255)
flashPoolEligibility ENUM
dedupeRatio FLOAT
dedupeSavingsGB BIGINT
totalAllocatedCapacityMB BIGINT
totalUsedCapacityMB BIGINT
totalUsedCapacityFromDeviceMB BIGINT
dataAllocatedCapacityMB BIGINT
dataUsedCapacityMB BIGINT
snapshotAllocatedCapacityMB BIGINT
snapshotUsedCapacityMB BIGINT
rawToUsableRatio FLOAT
otherUsedCapacityMB BIGINT
otherAllocatedCapacityMB BIGINT
totalCloneSavedCapacityMB BIGINT
compressionEnabled TINYINT(1)
compressionRatio FLOAT
compressionSavingsGB BIGINT
url VARCHAR(255)
uuid VARCHAR(255)
volume
Column
id INT
storageId INT
internalVolumeId INT
qtreeId INT
name VARCHAR(255)
label VARCHAR(255)
thinProvisioned TINYINT(1)
capacityMB BIGINT
consumedCapacityMB BIGINT
writtenCapacityMB BIGINT
rawCapacityMB BIGINT
type VARCHAR(255)
replicaSource TINYINT(1)
replicaTarget TINYINT(1)
snapshot TINYINT(1)
cylinders INT
diskGroup VARCHAR(255)
meta TINYINT(1)
virtualStorage VARCHAR(255)
head VARCHAR(255)
protectionType VARCHAR(255)
technologyType ENUM
autoTieringPolicyId INT
autoTiering TINYINT(1)
uuid VARCHAR(255)
isMainframe TINYINT(1)
lastKnownAccessTime DATETIME
url VARCHAR(255)
isVirtual TINYINT(1)
storage_port
Column
id INT
controllerId INT
storageId INT
wwn VARCHAR(255)
nodeWwn VARCHAR(255)
portId VARCHAR(255)
name VARCHAR(255)
speed VARCHAR(12)
controller VARCHAR(255)
url VARCHAR(255)
active TINYINT(1)

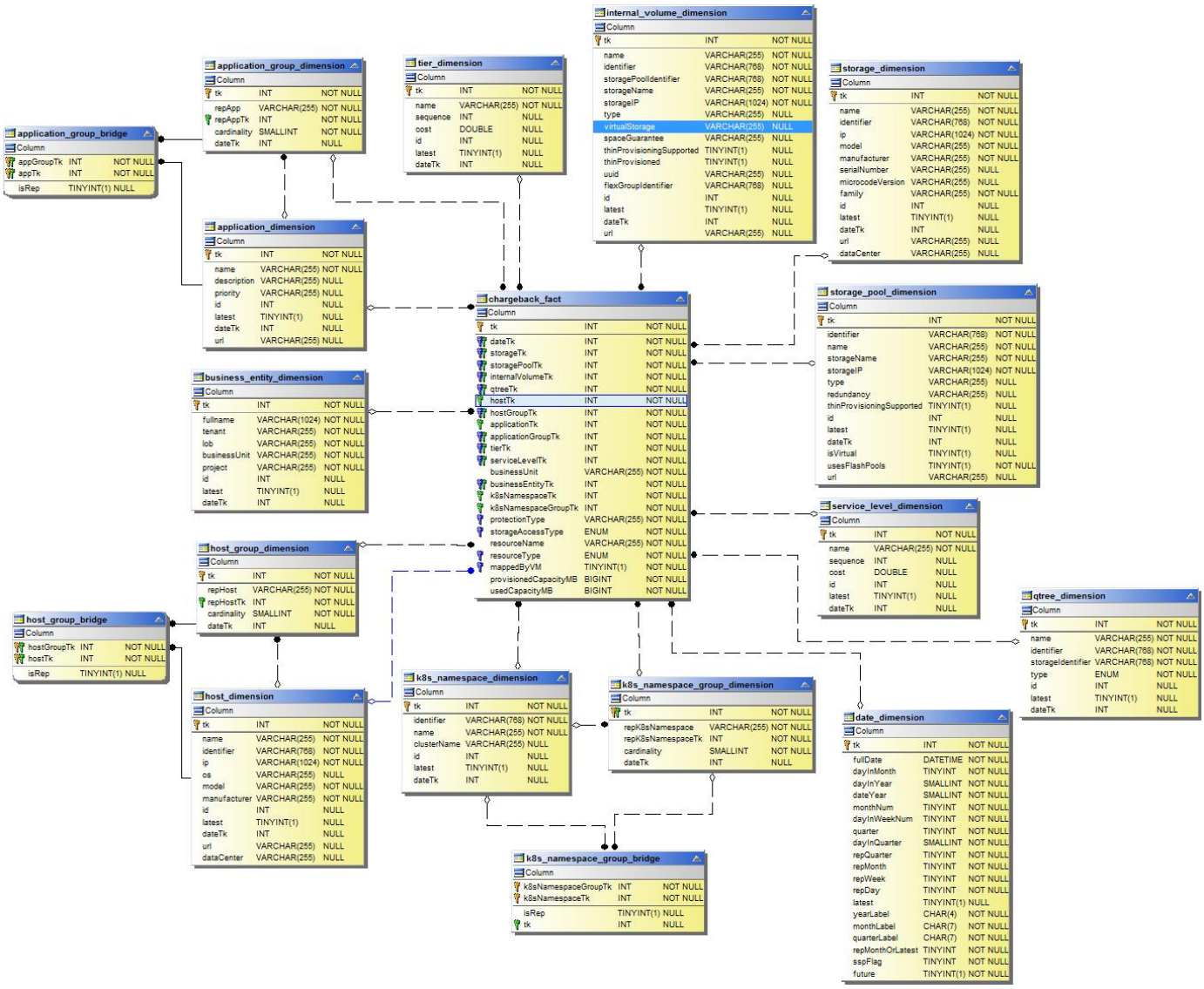
VM



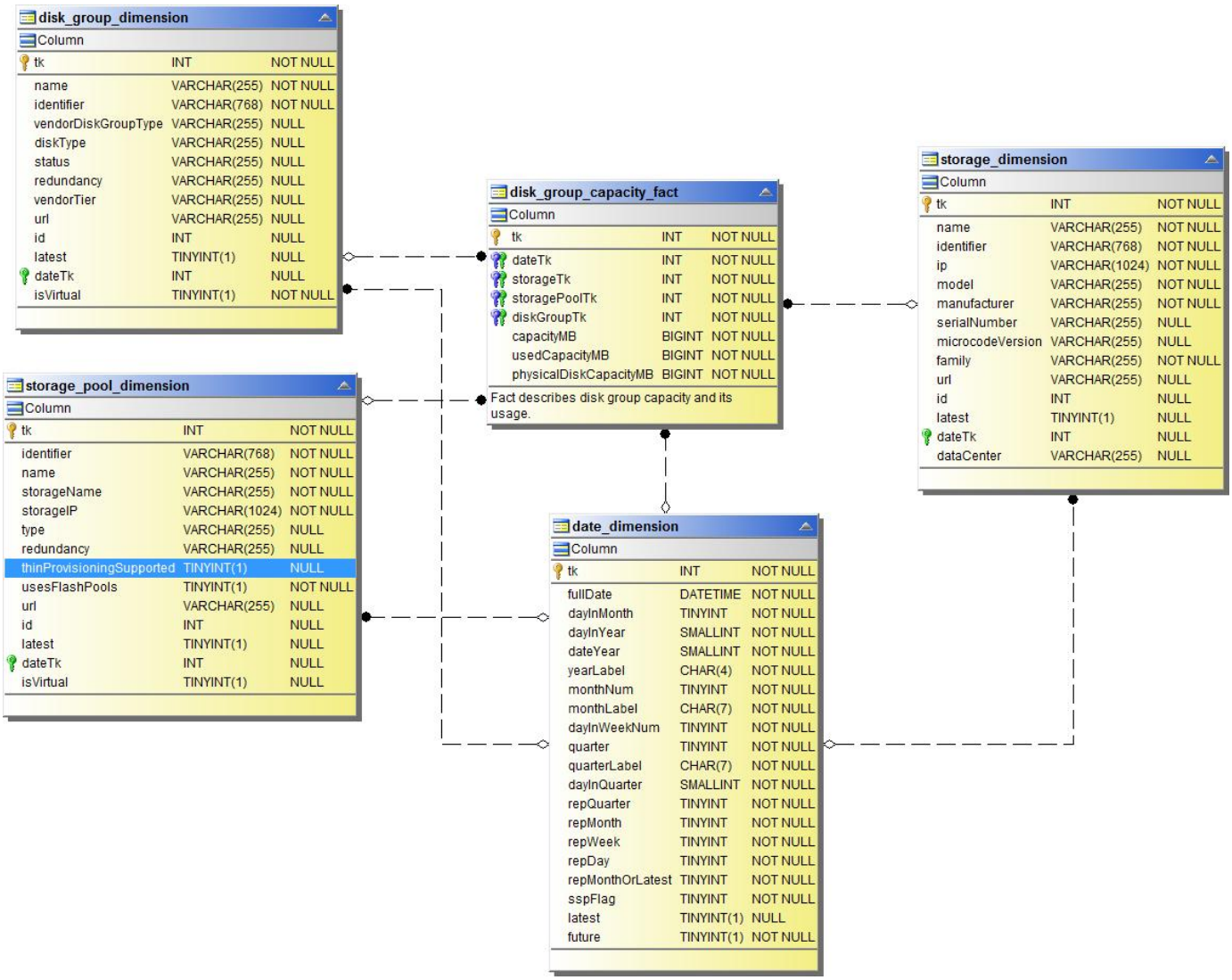
Kapazitäts-Datamart

Die folgenden Bilder beschreiben den Kapazitäts-Datamart.

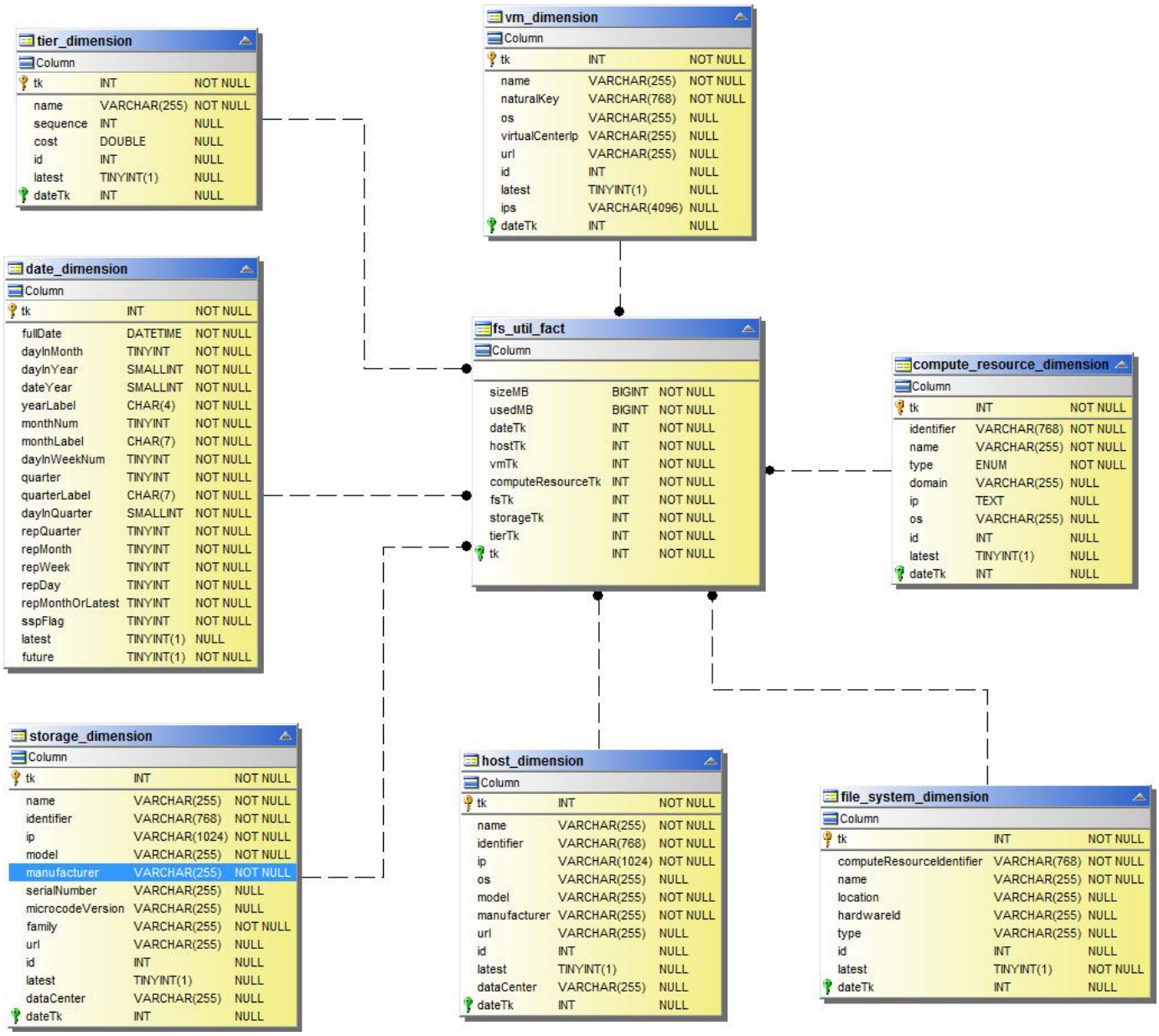
Rückbuchung



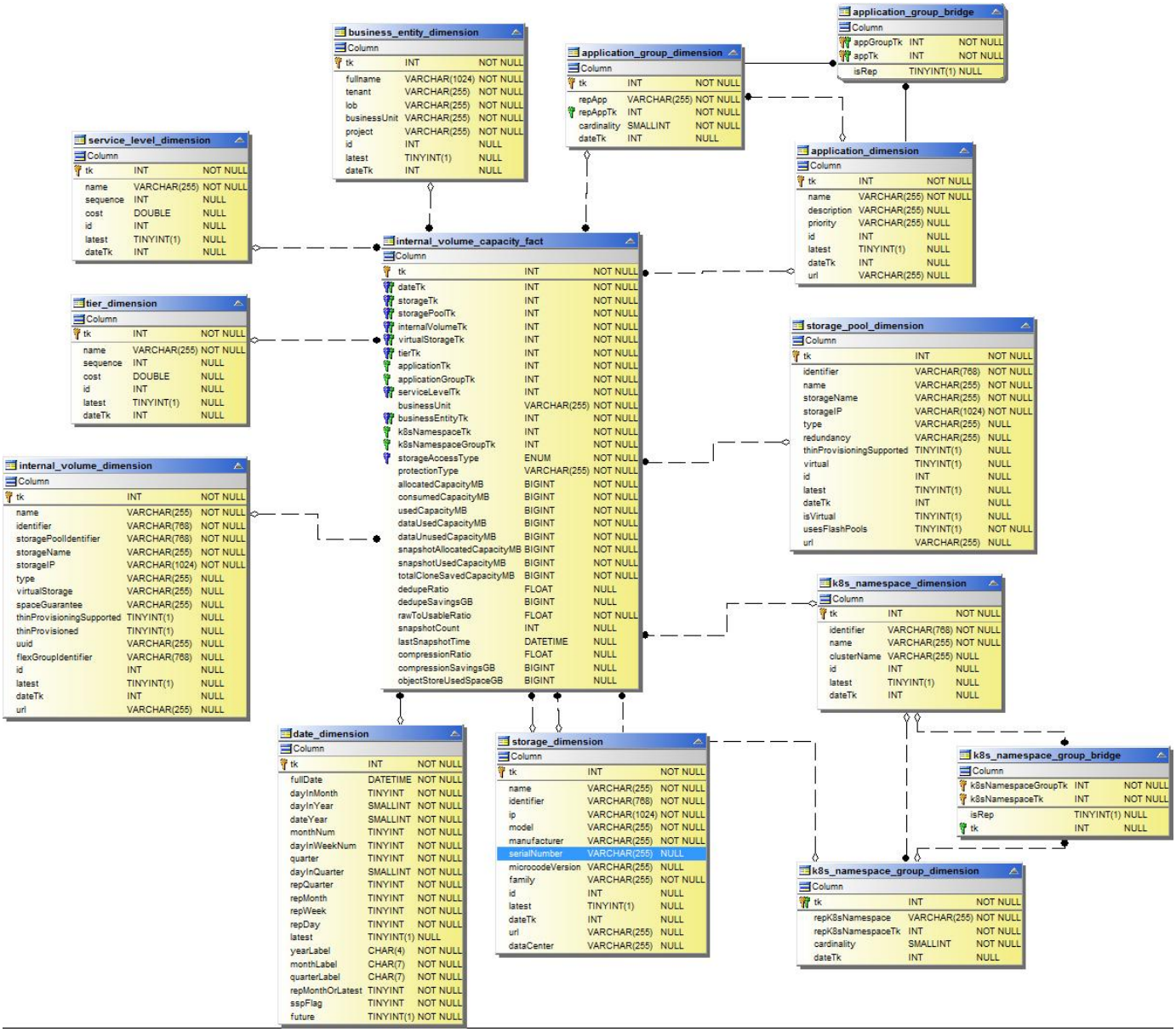
Kapazität der Datenträgergruppe



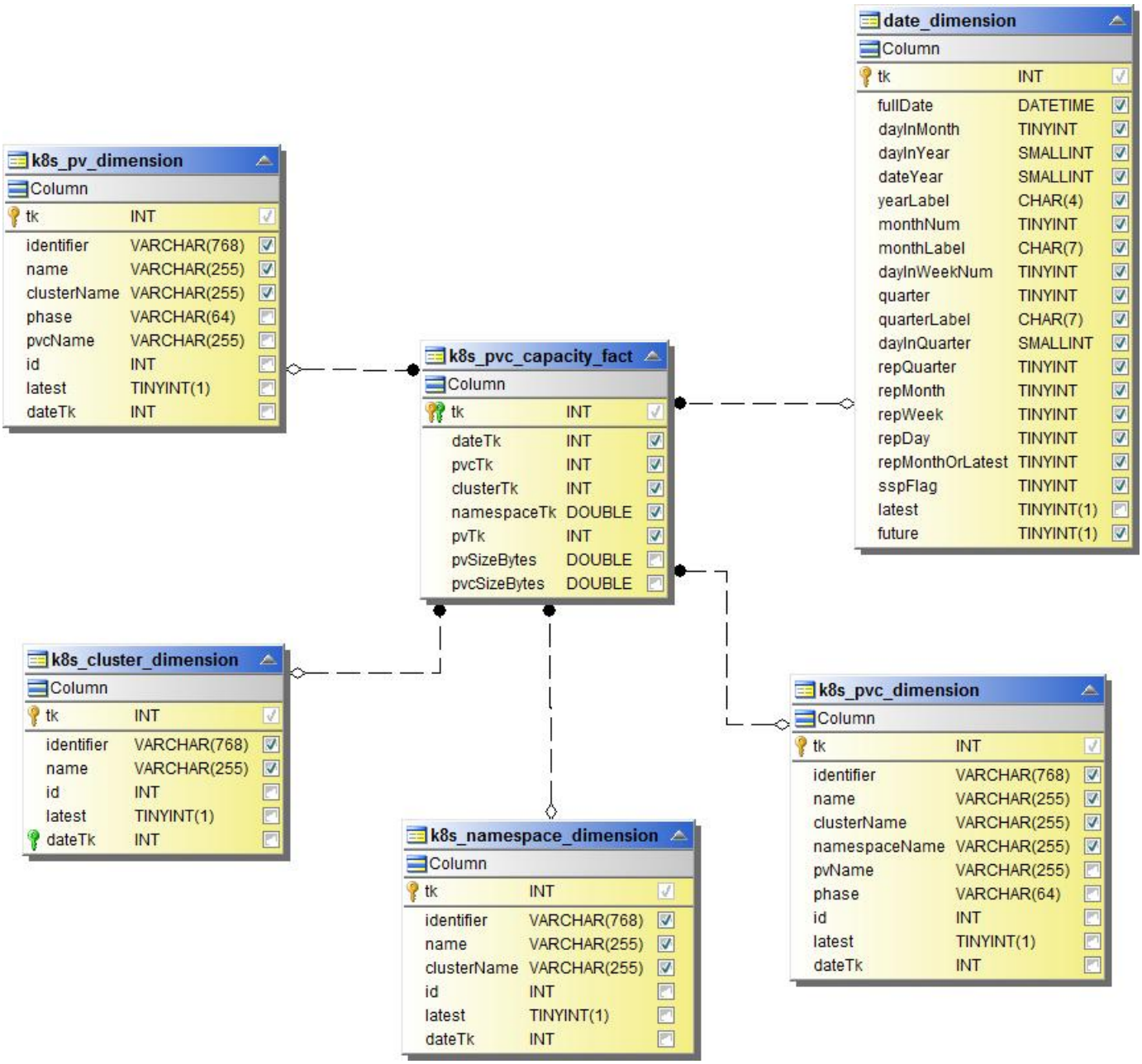
Dateisystemauslastung



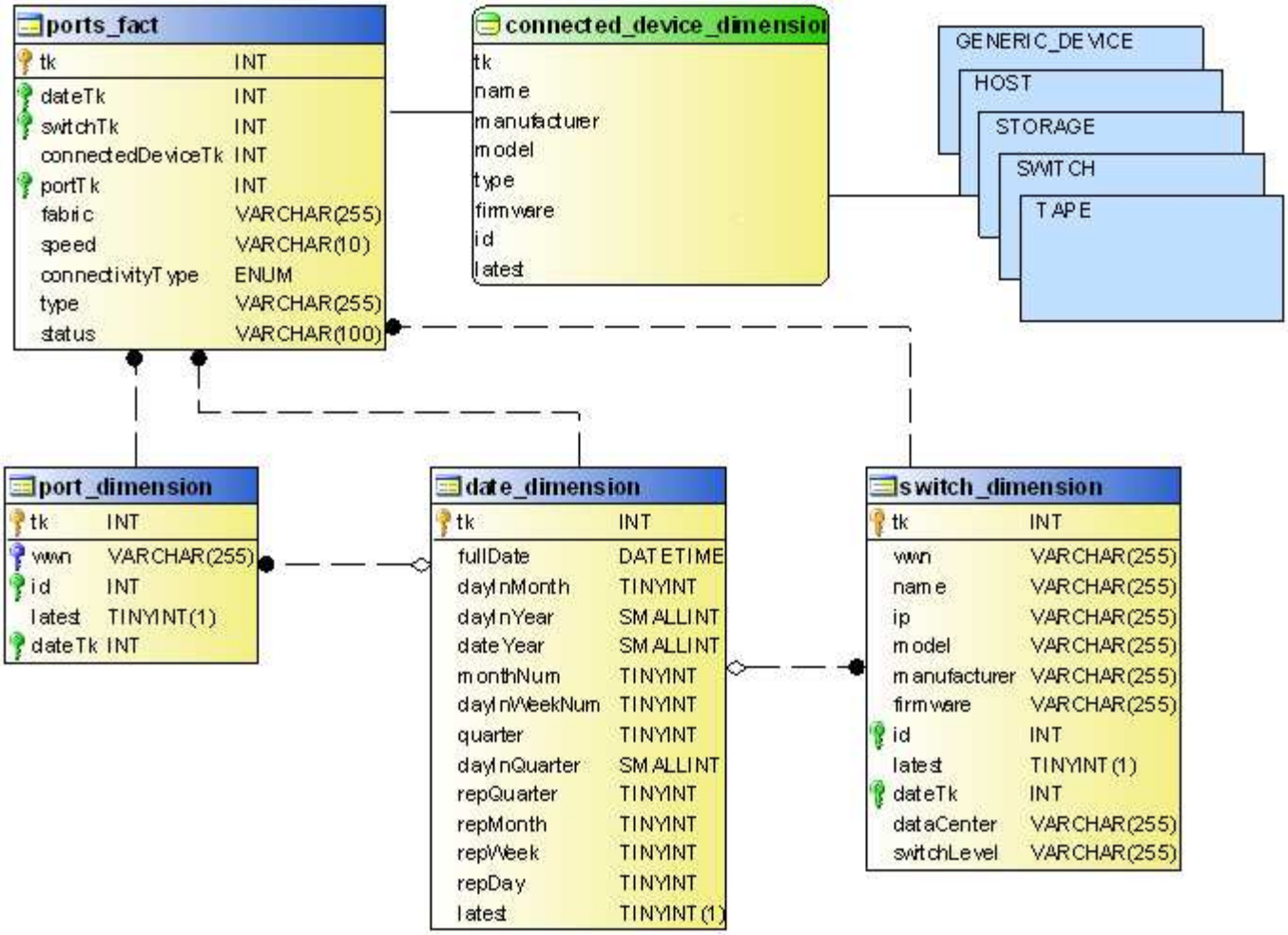
Interne Volumenkapazität



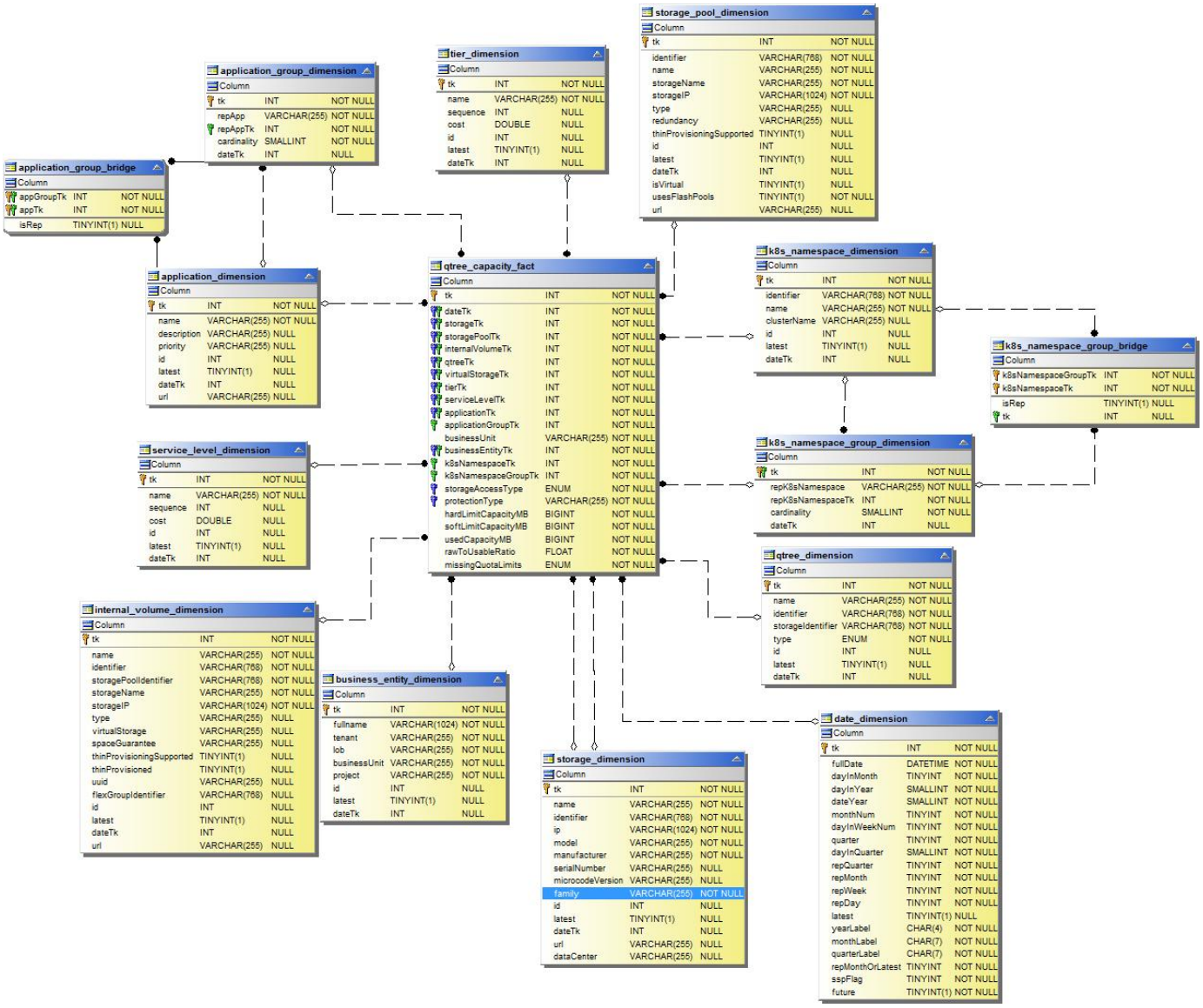
Kubernetes PV-Kapazität



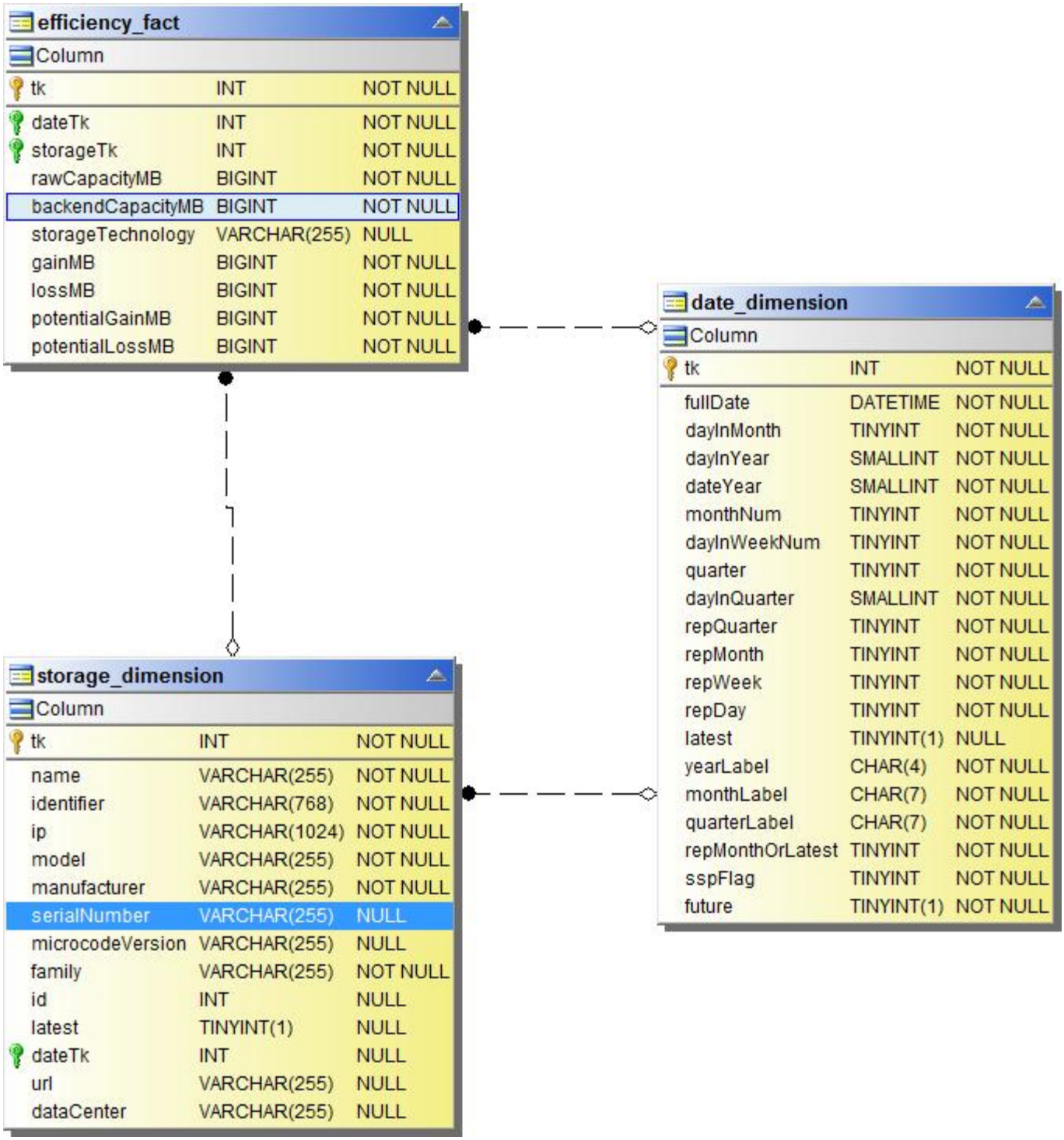
Hafenkapazität



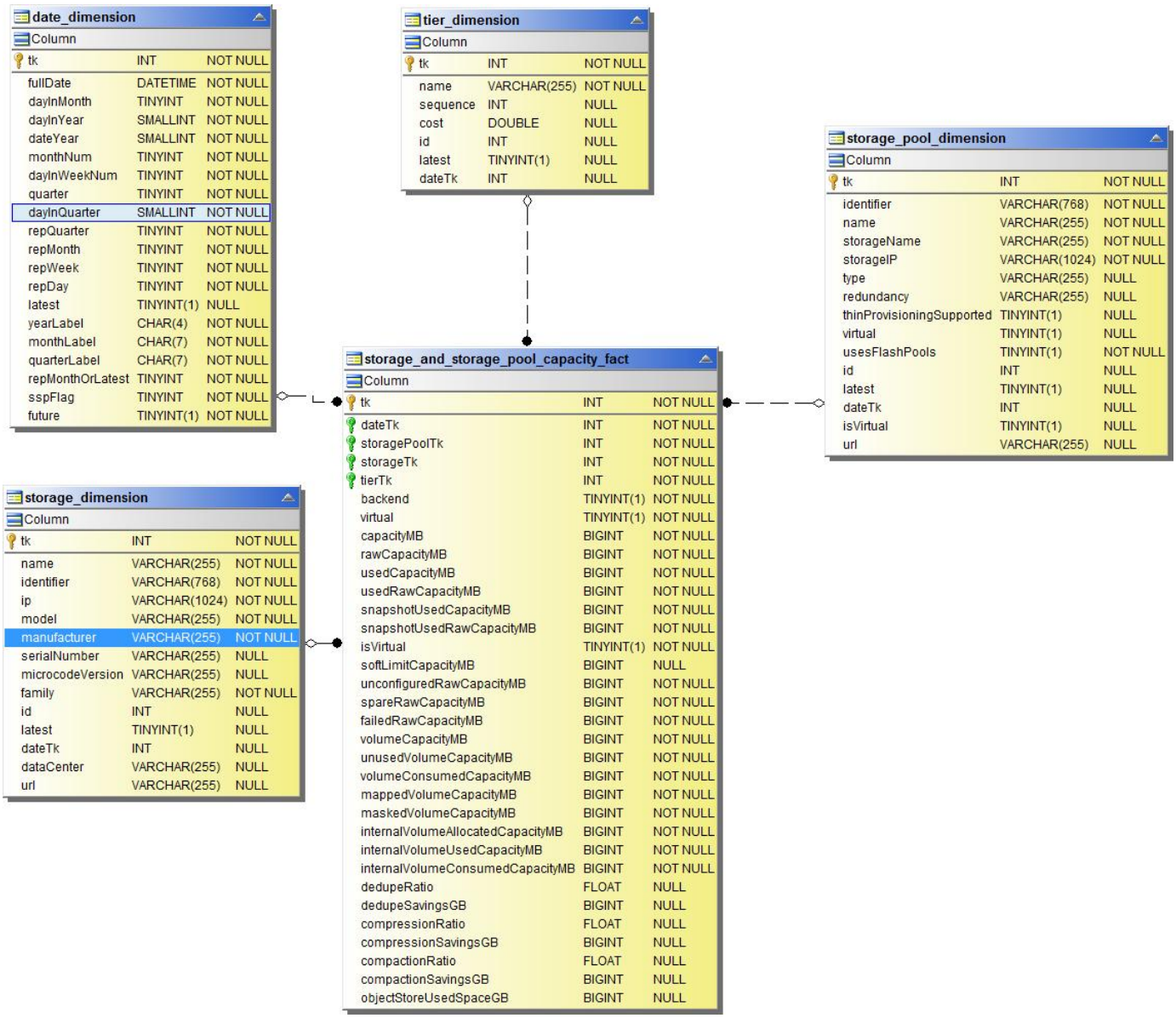
Qtree-Kapazität



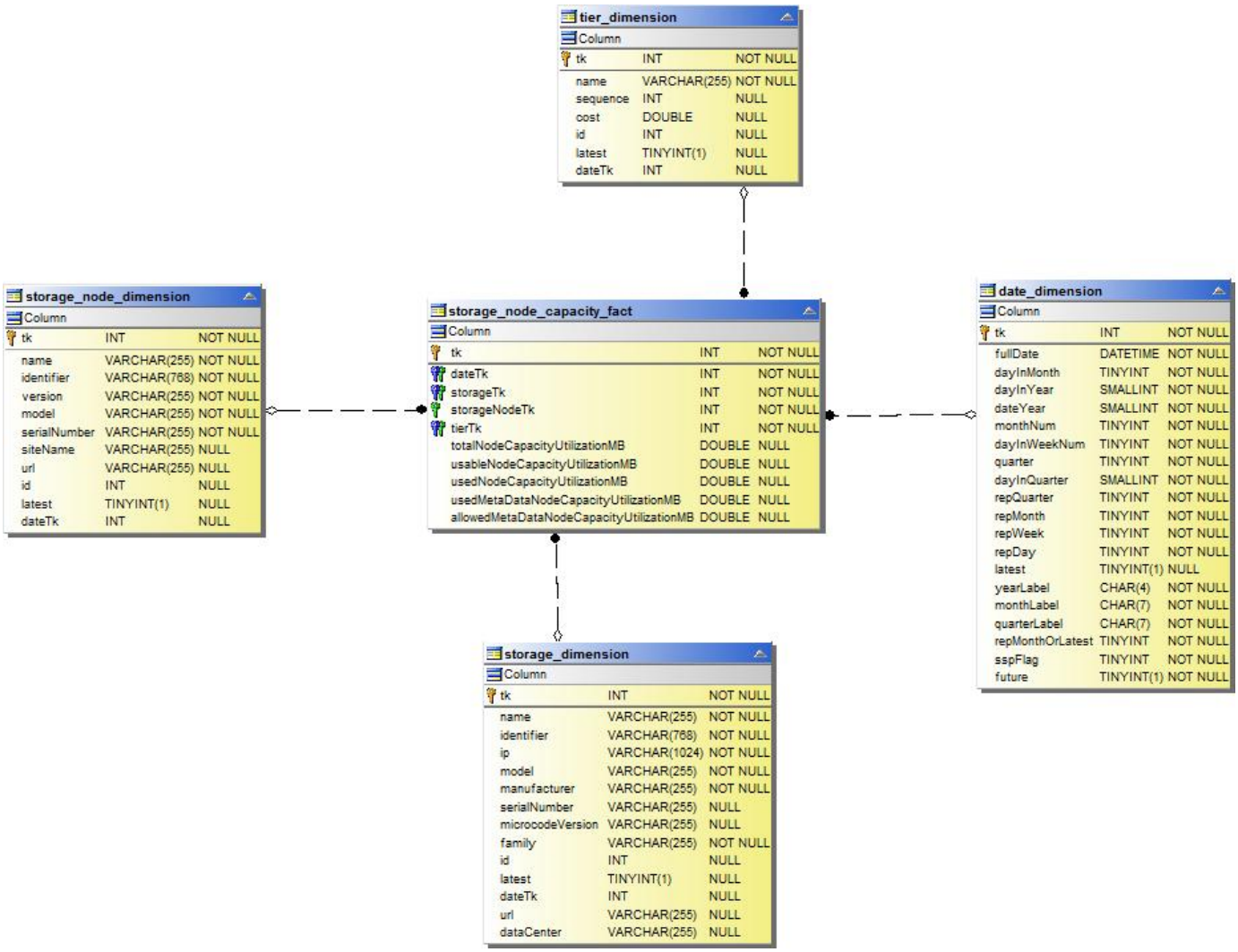
Speicherkapazitätseffizienz



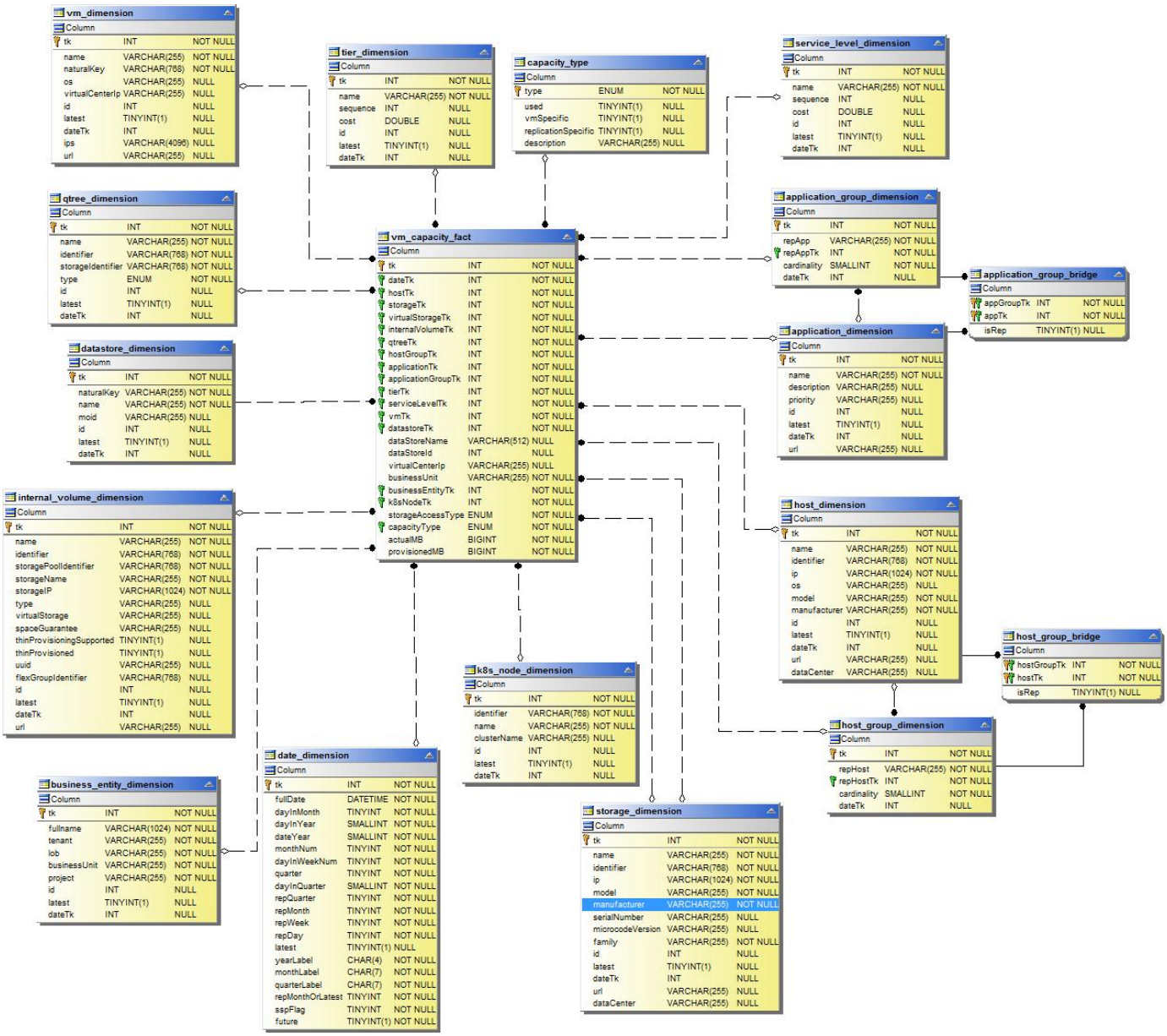
Speicher- und Speicherpoolkapazität



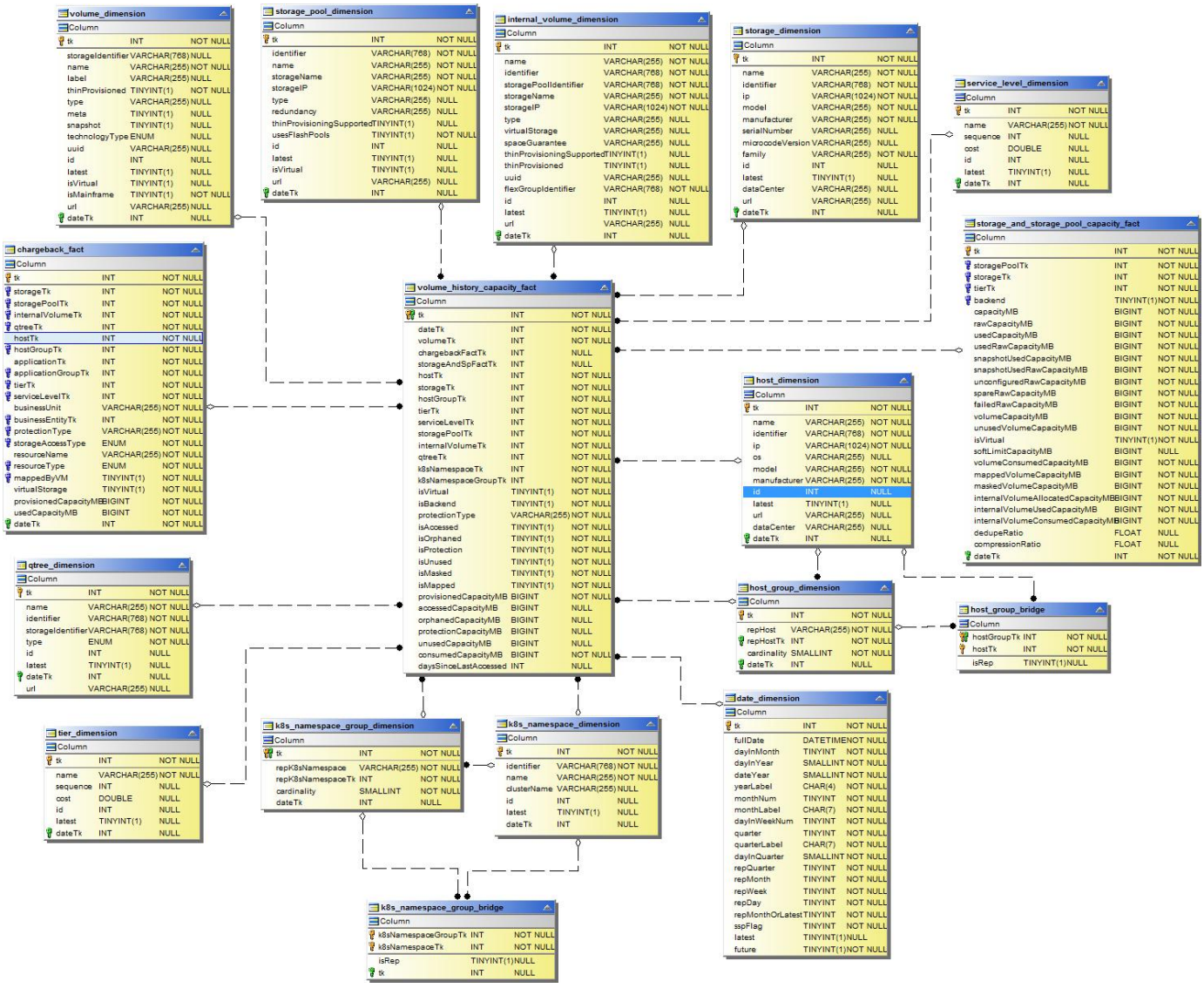
Speicherknotenkapazität



VM-Kapazität



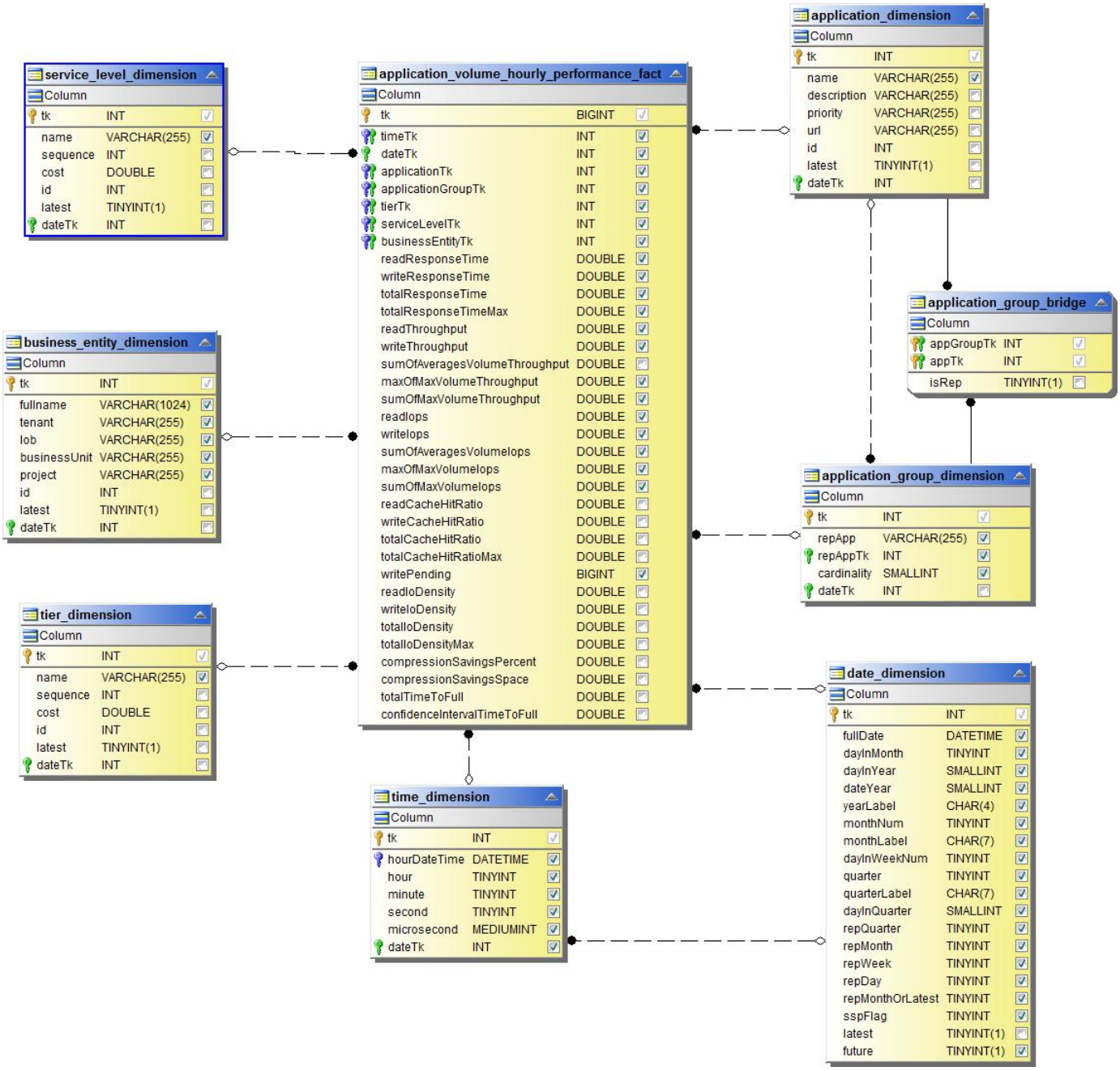
Volumenkapazität



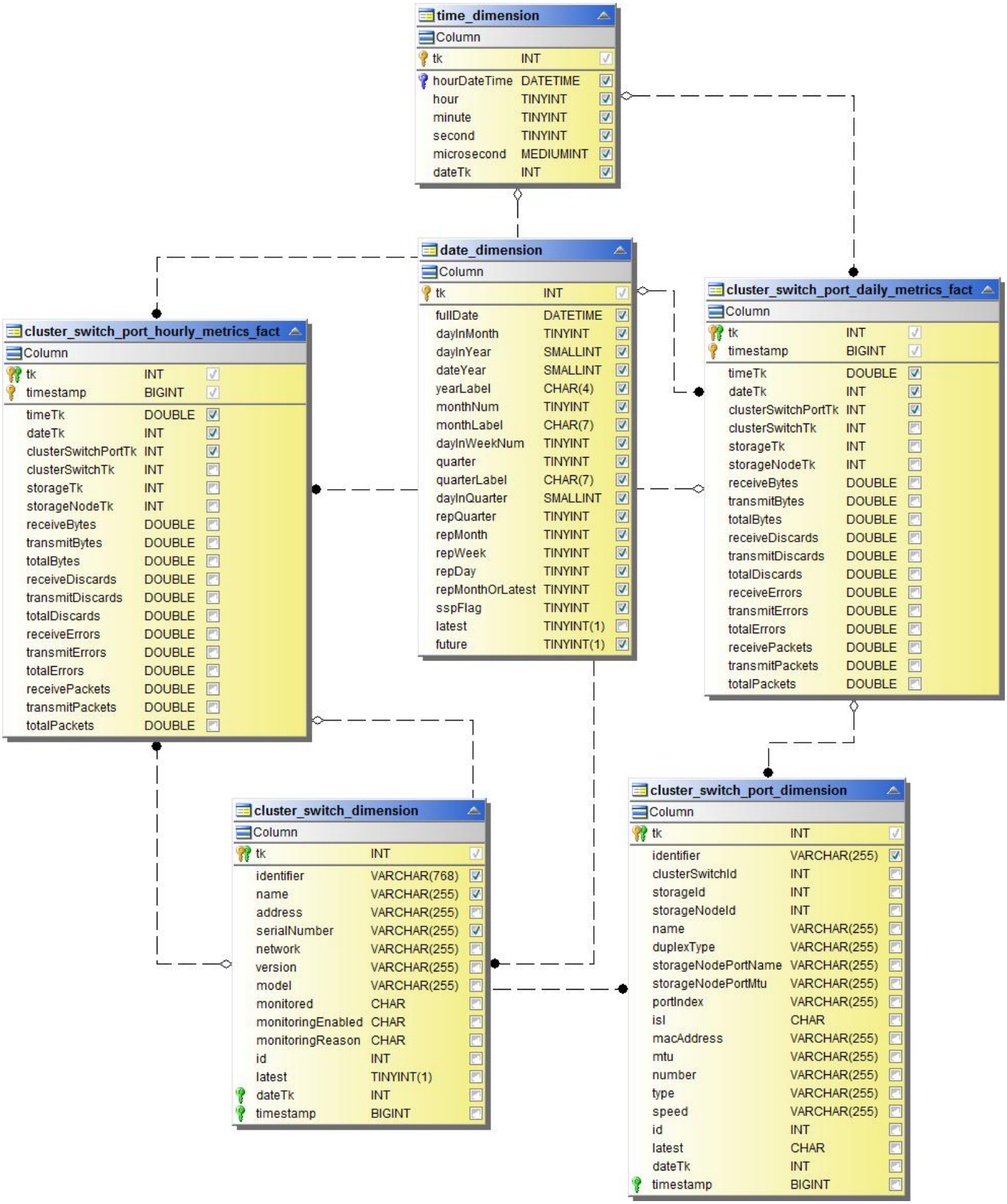
Leistungs-Datamart

Die folgenden Bilder beschreiben den Performance-Datamart.

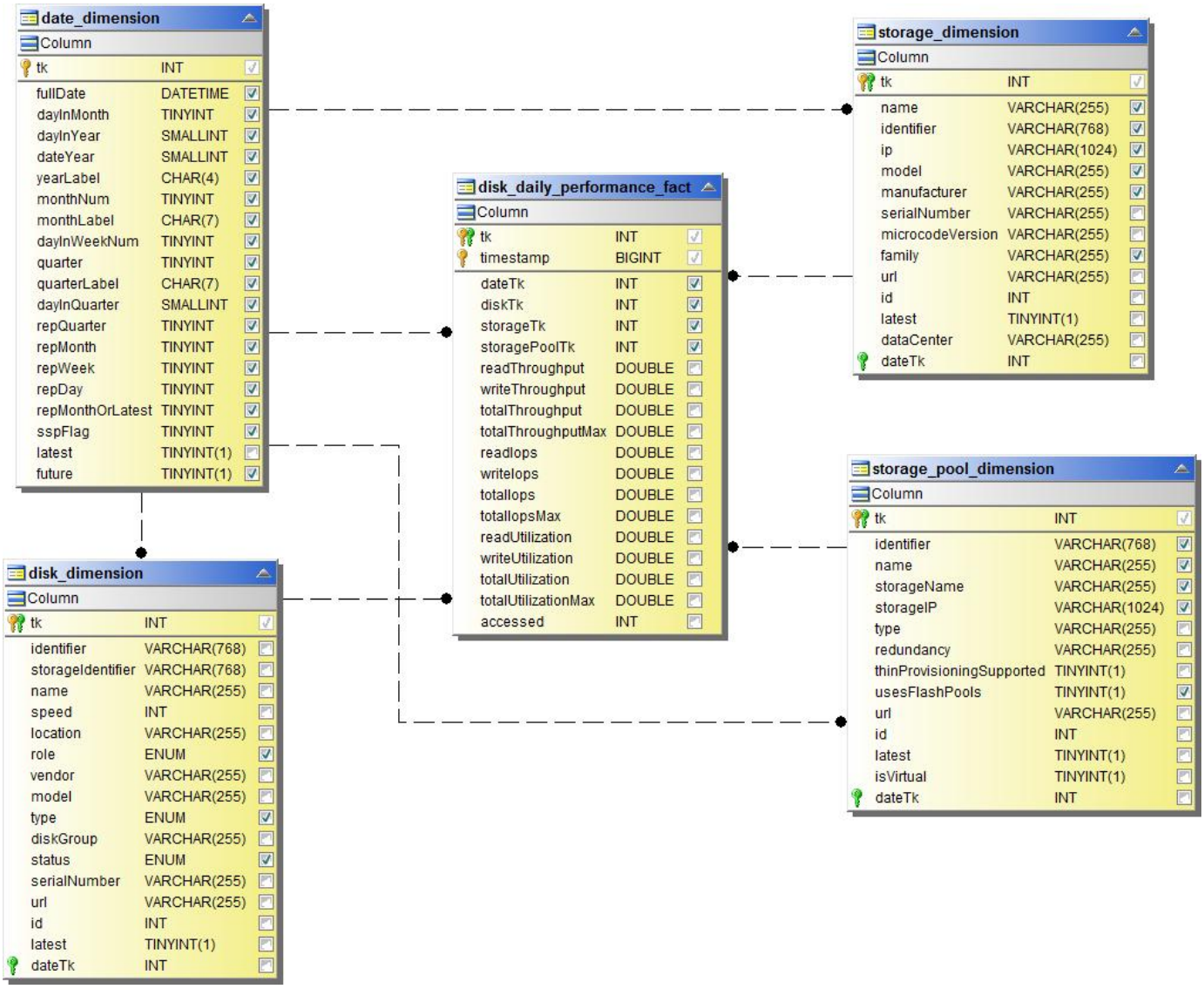
Anwendungsvolumen Stündliche Leistung



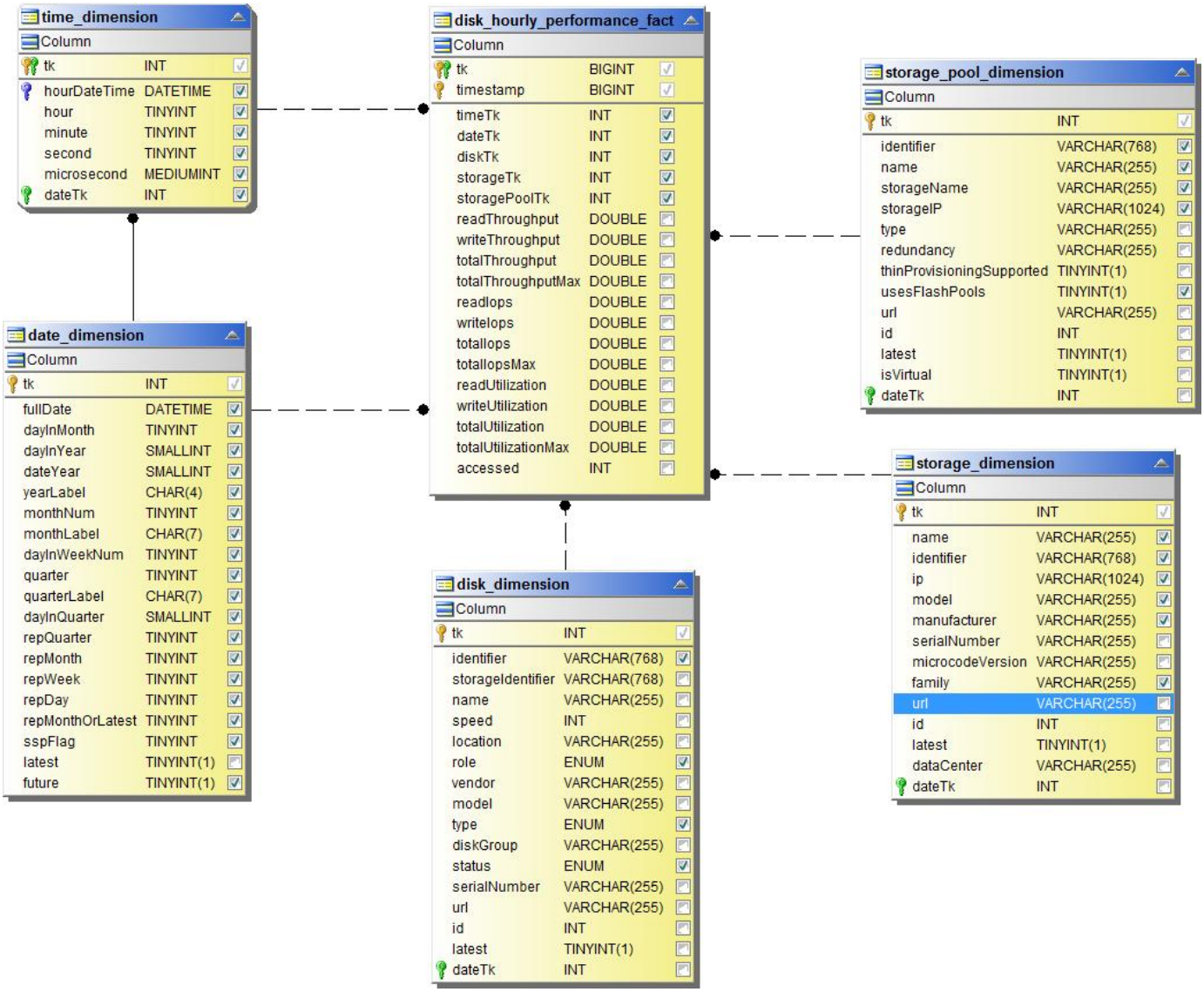
Cluster-Switch-Leistung



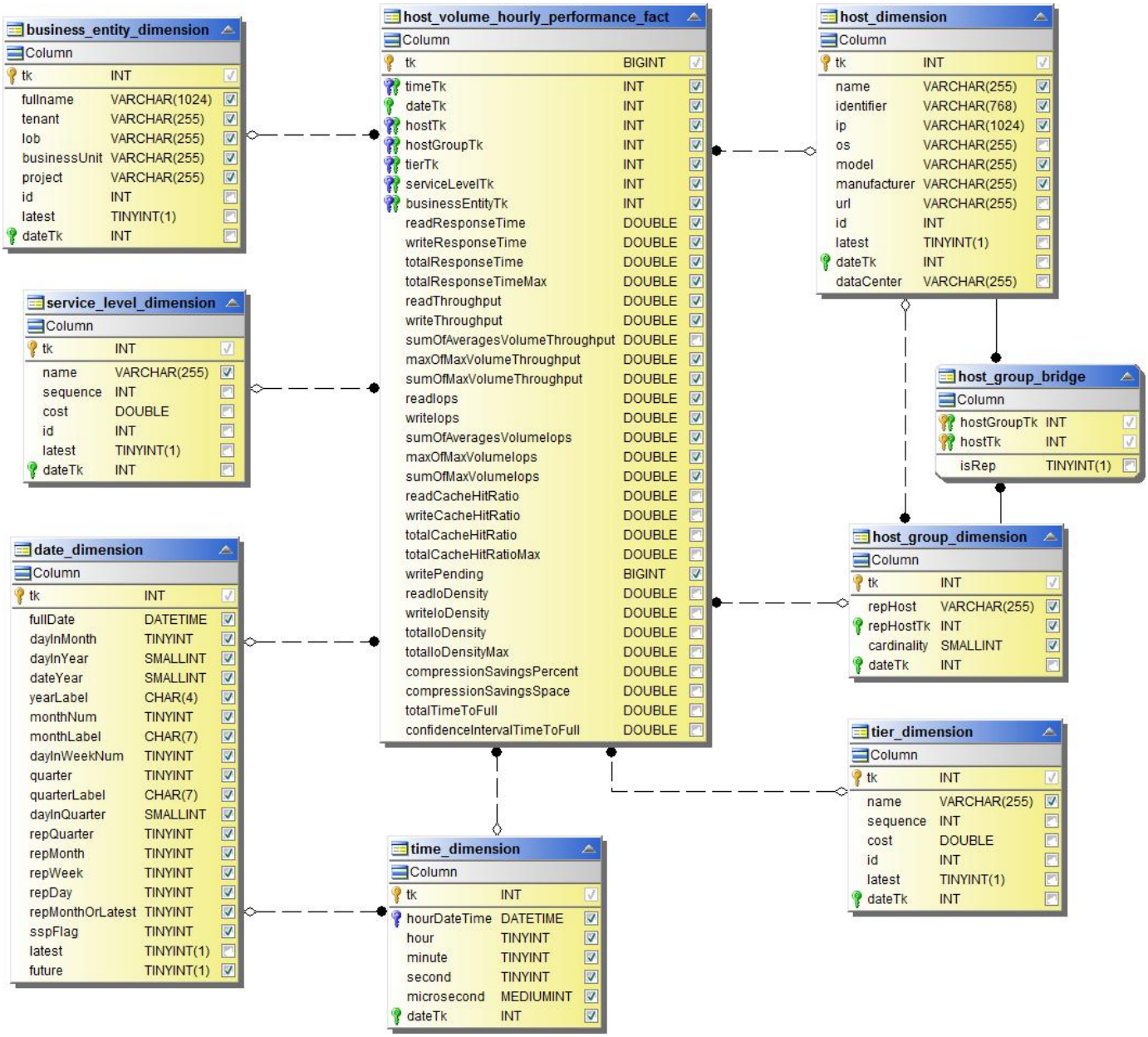
Tägliche Festplattenleistung



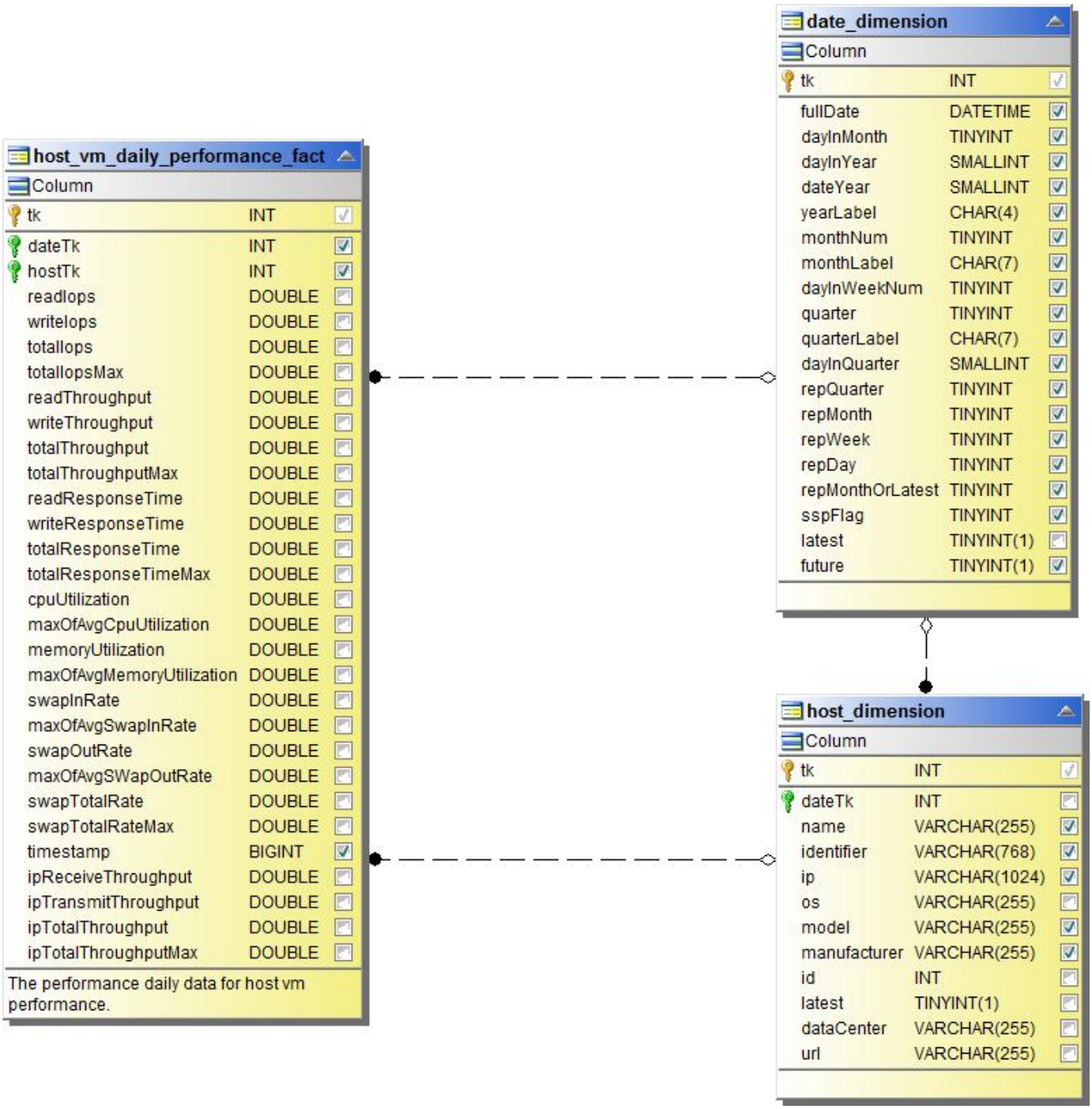
Stündliche Festplattenleistung



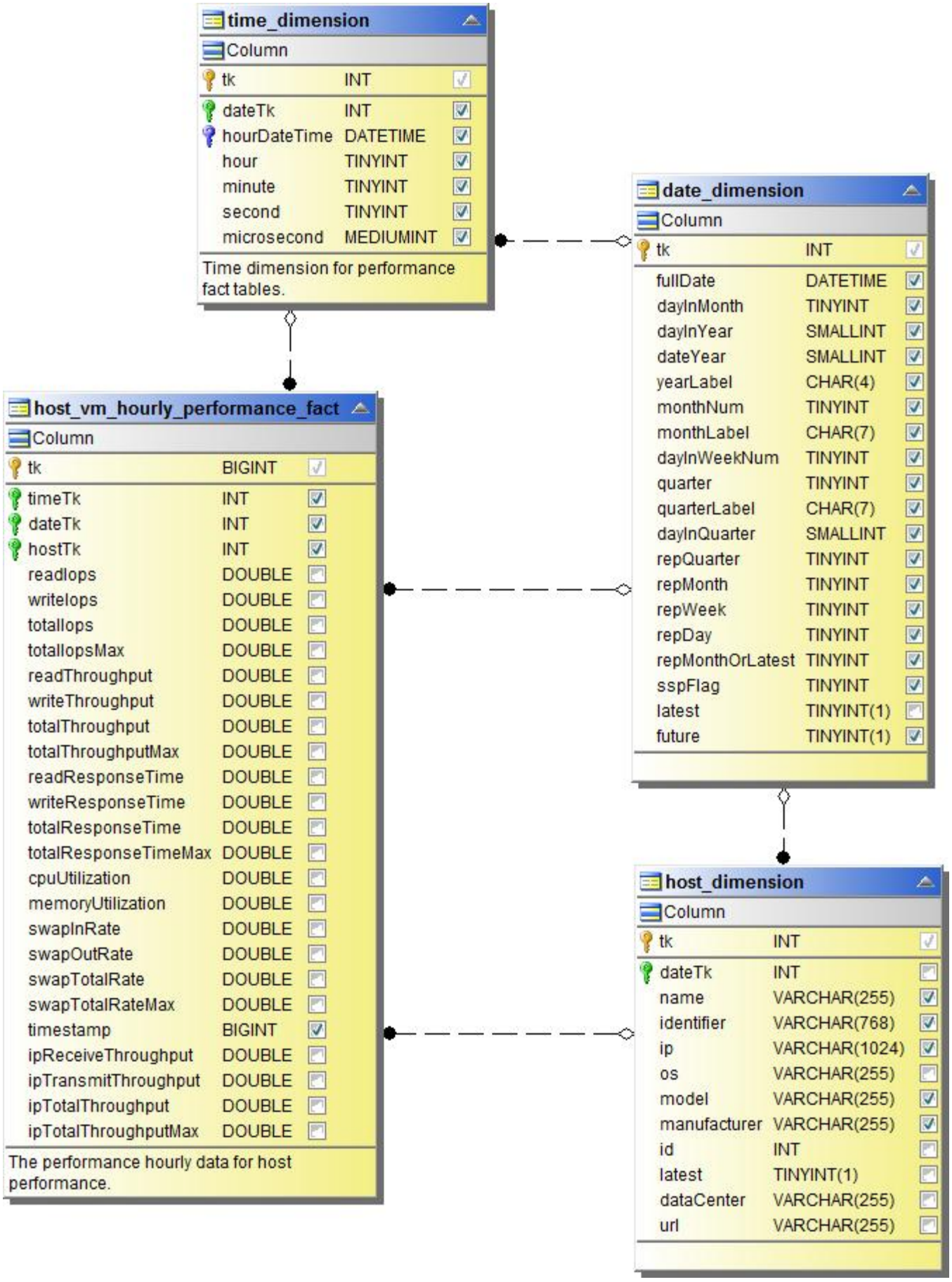
Host-Stundenleistung



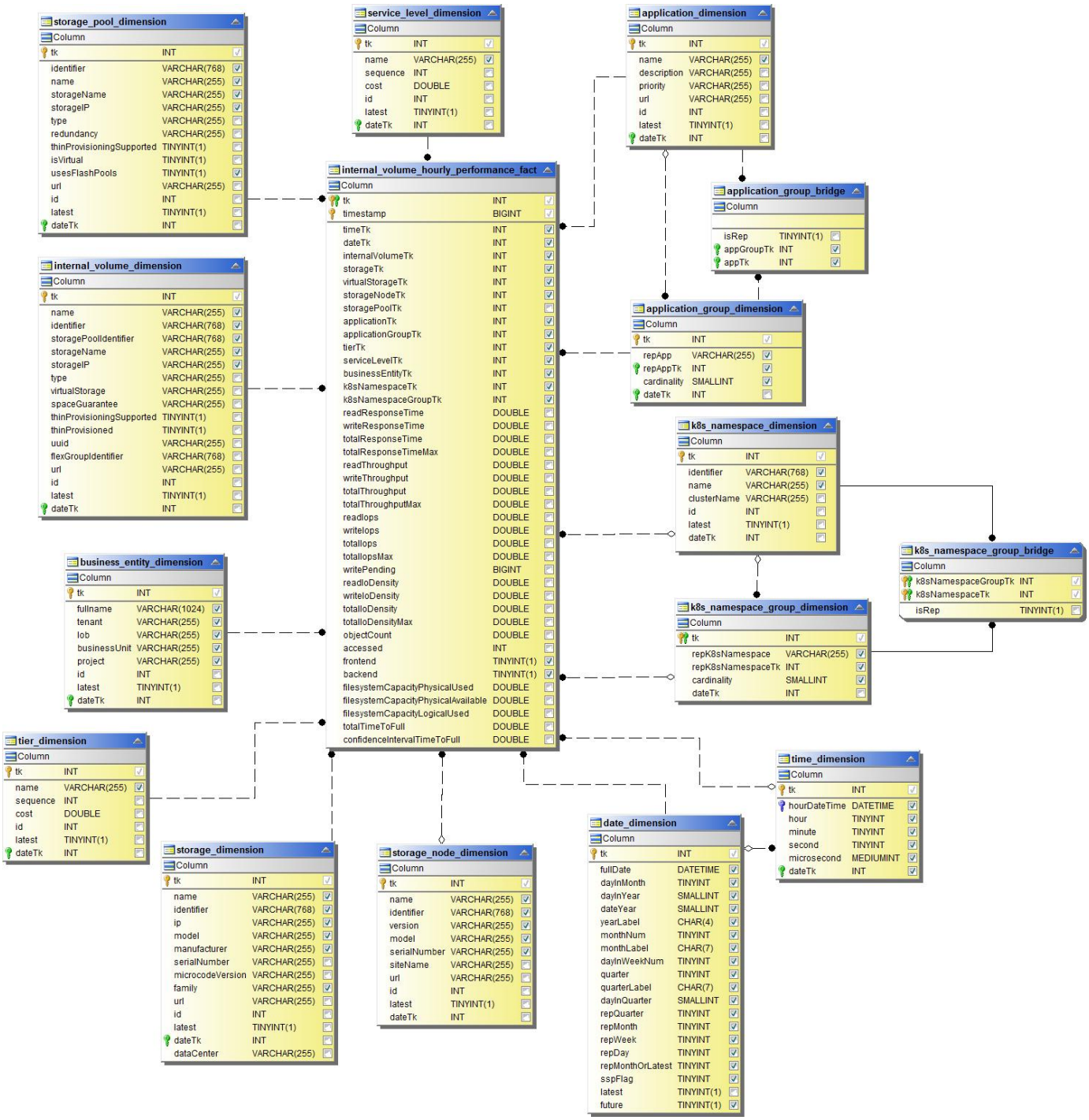
Tägliche Leistung der Host-VM



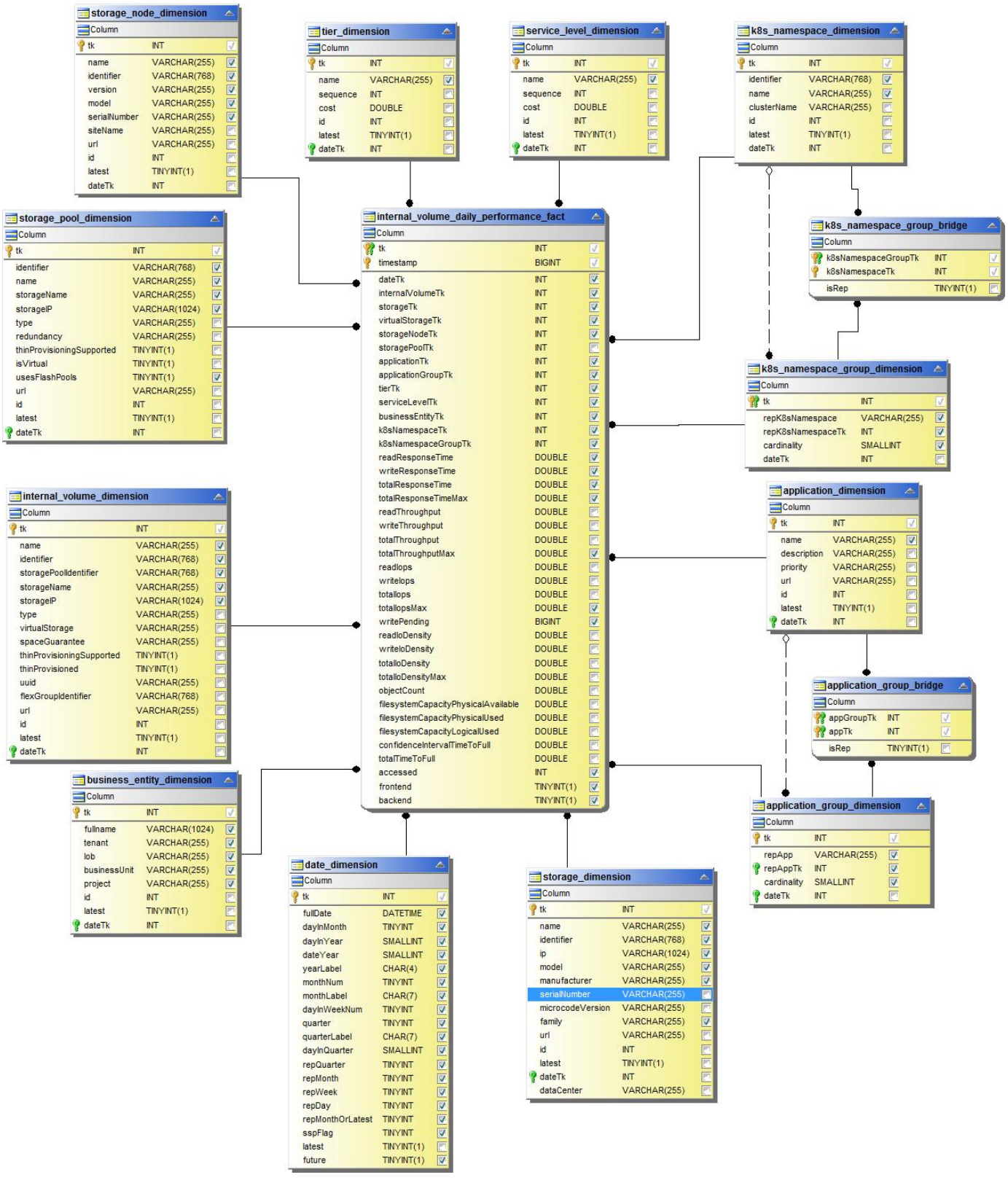
Host-VM-Stündliche Leistung


time_dimension
Column
tk INT
dateTk INT
hourDateTime DATETIME
hour TINYINT
minute TINYINT
second TINYINT
microsecond MEDIUMINT
Time dimension for performance fact tables.
date_dimension
Column
tk INT
fullDate DATETIME
dayInMonth TINYINT
dayInYear SMALLINT
dateYear SMALLINT
yearLabel CHAR(4)
monthNum TINYINT
monthLabel CHAR(7)
dayInWeekNum TINYINT
quarter TINYINT
quarterLabel CHAR(7)
dayInQuarter SMALLINT
repQuarter TINYINT
repMonth TINYINT
repWeek TINYINT
repDay TINYINT
repMonthOrLatest TINYINT
sspFlag TINYINT
latest TINYINT(1)
future TINYINT(1)
host_vm_hourly_performance_fact
Column
tk BIGINT
timeTk INT
dateTk INT
hostTk INT
readIops DOUBLE
writeIops DOUBLE
totalIops DOUBLE
totalIopsMax DOUBLE
readThroughput DOUBLE
writeThroughput DOUBLE
totalThroughput DOUBLE
totalThroughputMax DOUBLE
readResponseTime DOUBLE
writeResponseTime DOUBLE
totalResponseTime DOUBLE
totalResponseTimeMax DOUBLE
cpuUtilization DOUBLE
memoryUtilization DOUBLE
swapInRate DOUBLE
swapOutRate DOUBLE
swapTotalRate DOUBLE
swapTotalRateMax DOUBLE
timestamp BIGINT
ipReceiveThroughput DOUBLE
ipTransmitThroughput DOUBLE
ipTotalThroughput DOUBLE
ipTotalThroughputMax DOUBLE
The performance hourly data for host performance.
host_dimension
Column
tk INT
dateTk INT
name VARCHAR(255)
identifier VARCHAR(768)
ip VARCHAR(1024)
os VARCHAR(255)
model VARCHAR(255)
manufacturer VARCHAR(255)
id INT
latest TINYINT(1)
dataCenter VARCHAR(255)
url VARCHAR(255)

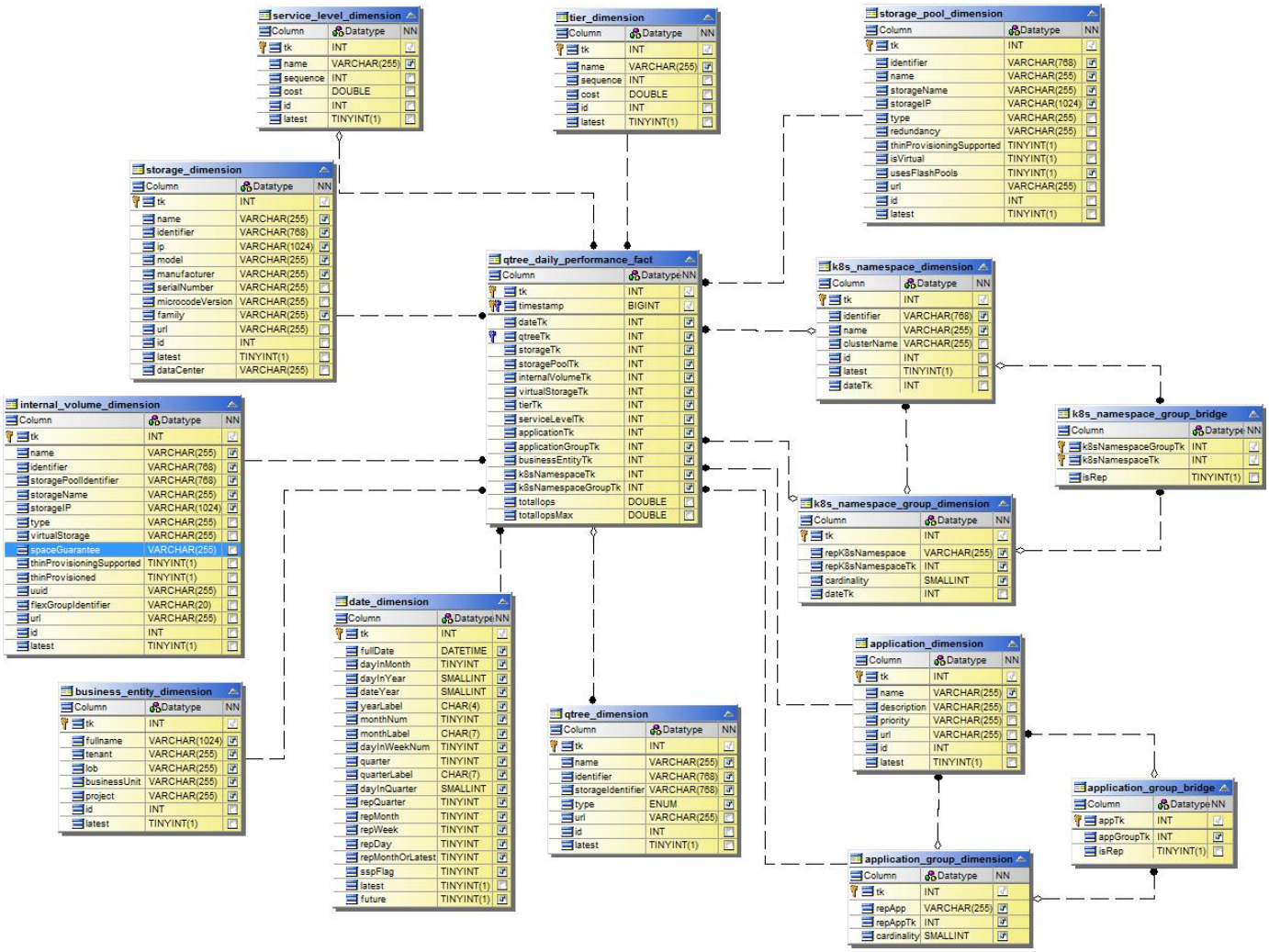
Internes Volumen, stündliche Leistung



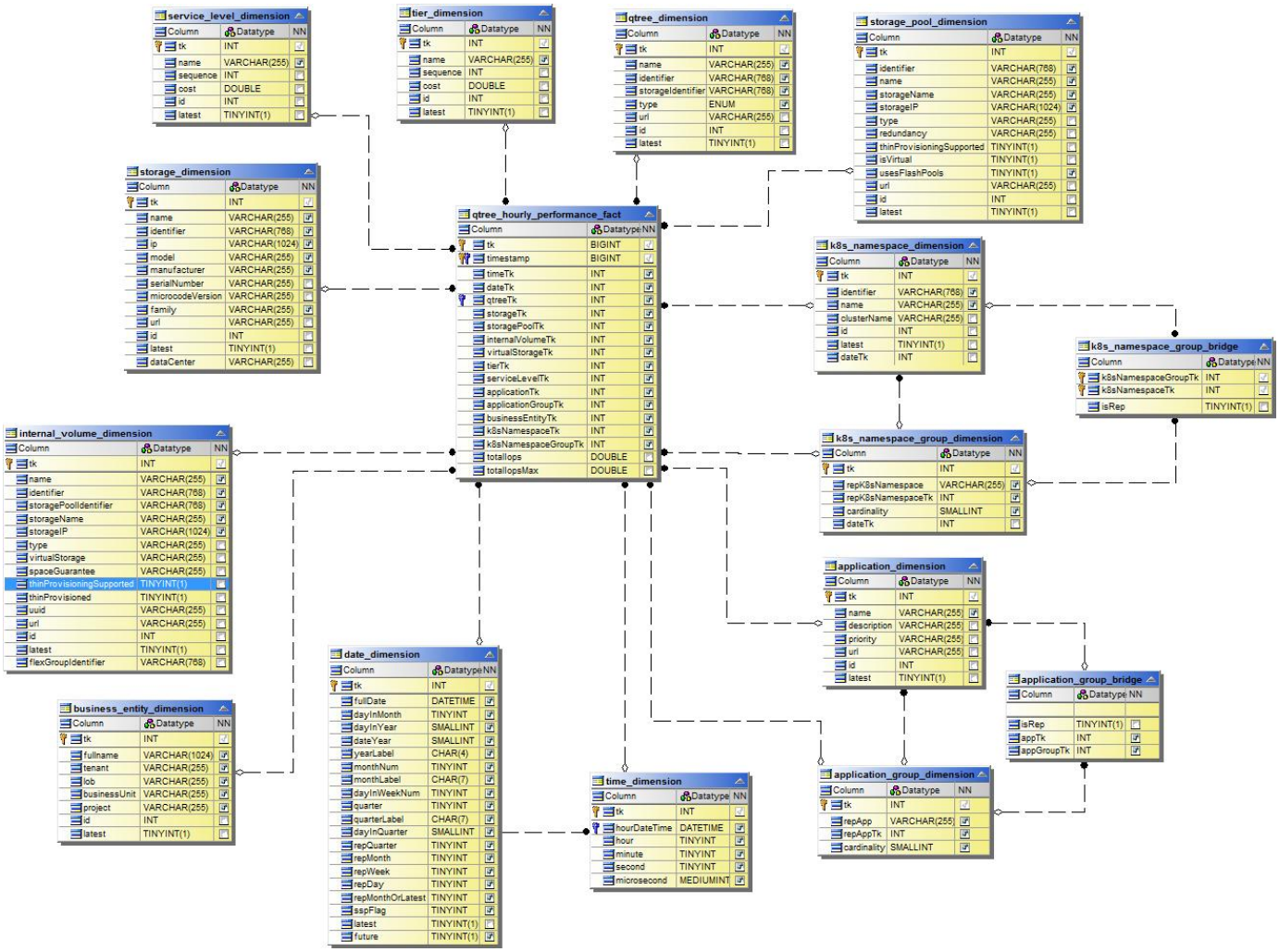
Internes Volumen – Tägliche Leistung



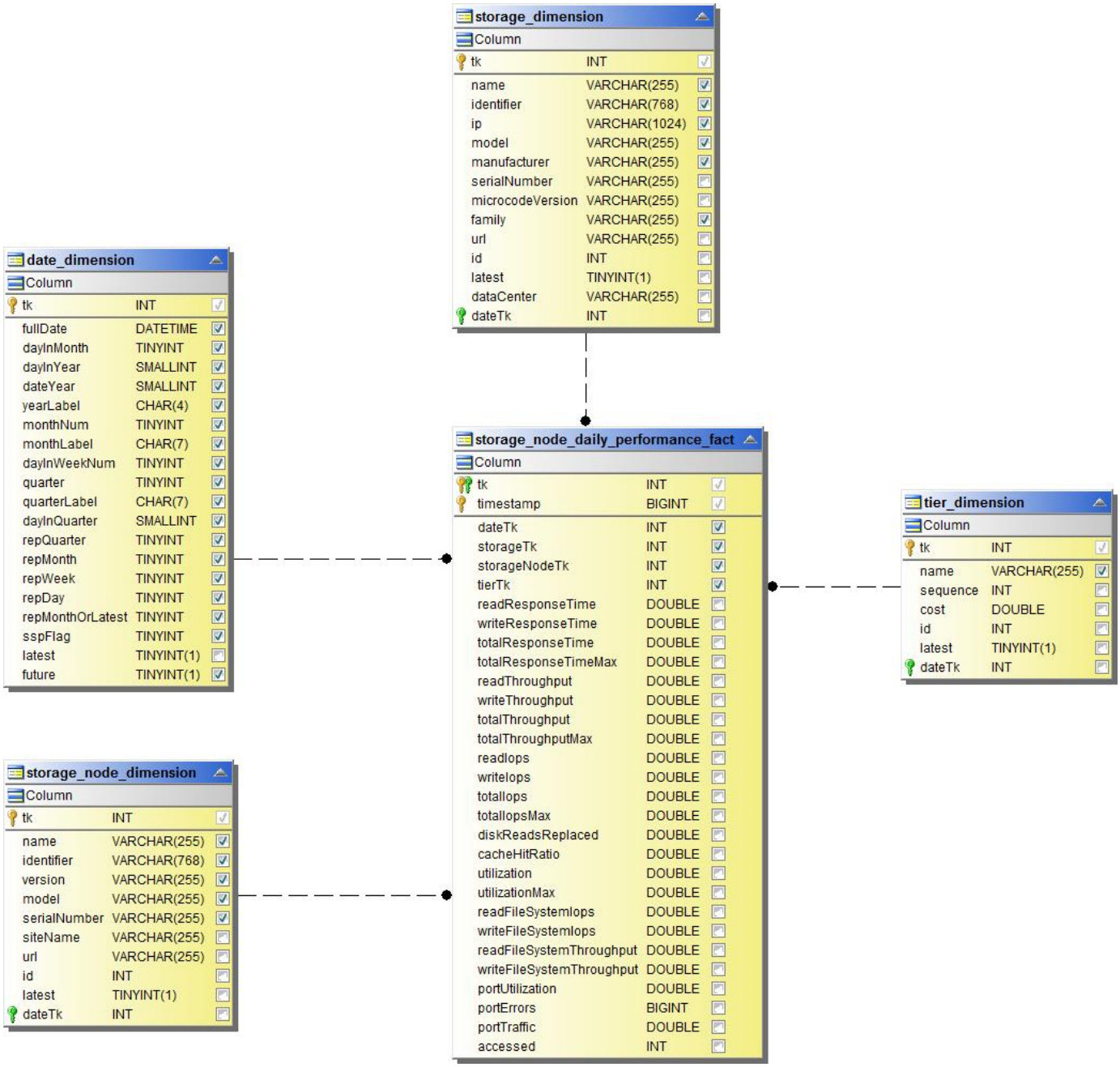
Qtree Tägliche Leistung



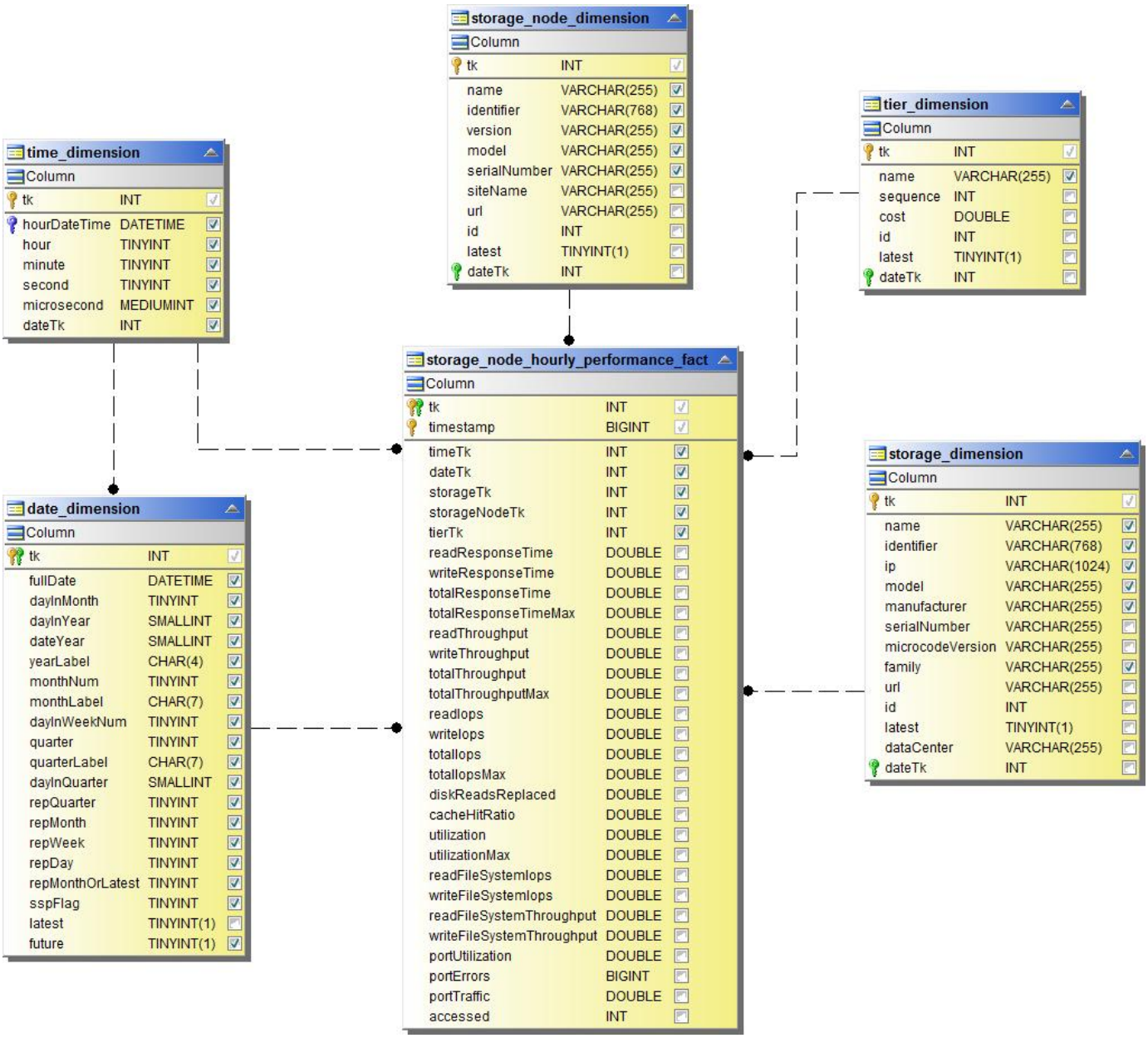
Qtree Stundenleistung



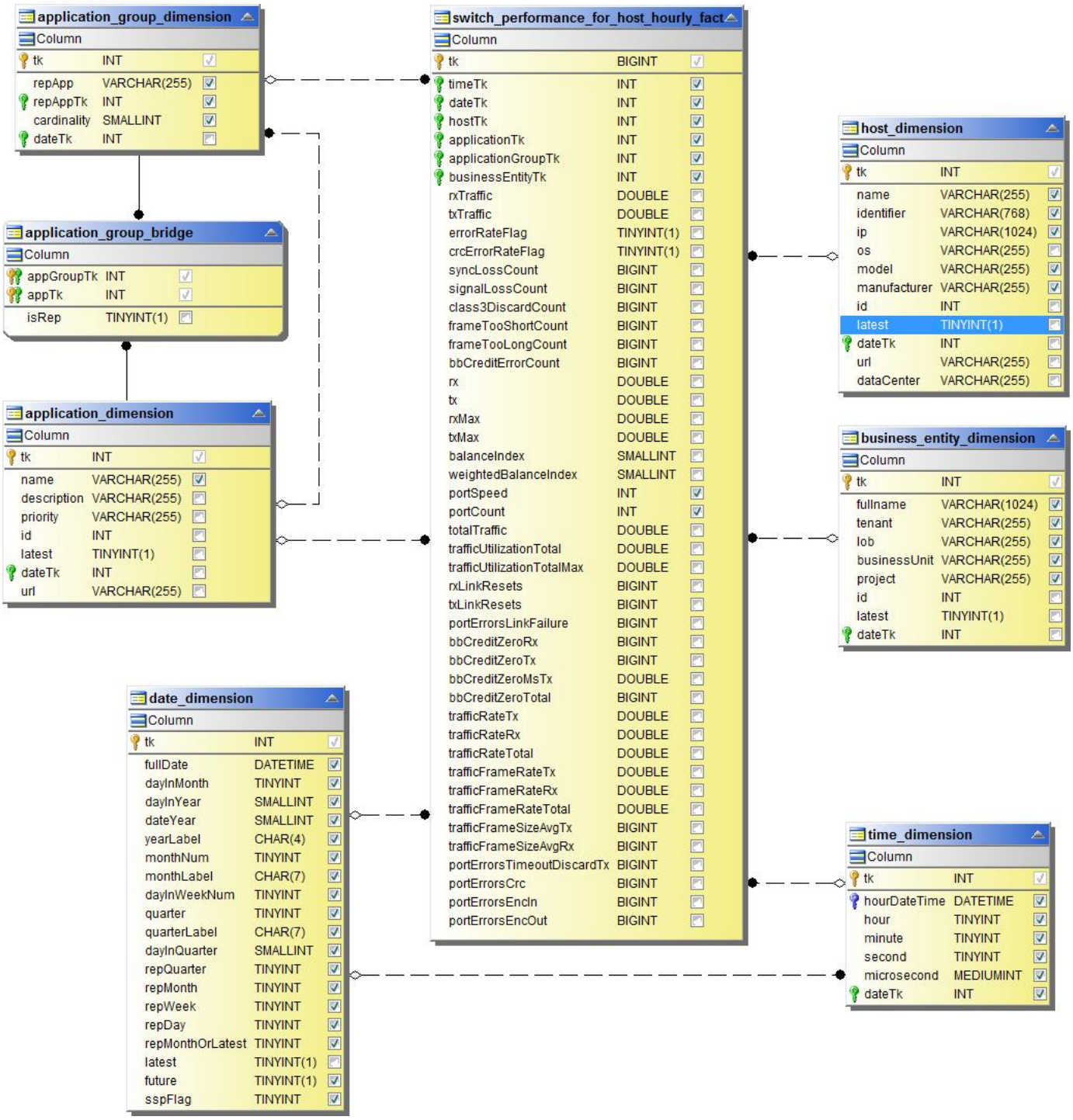
Tägliche Leistung des Speicherknotens



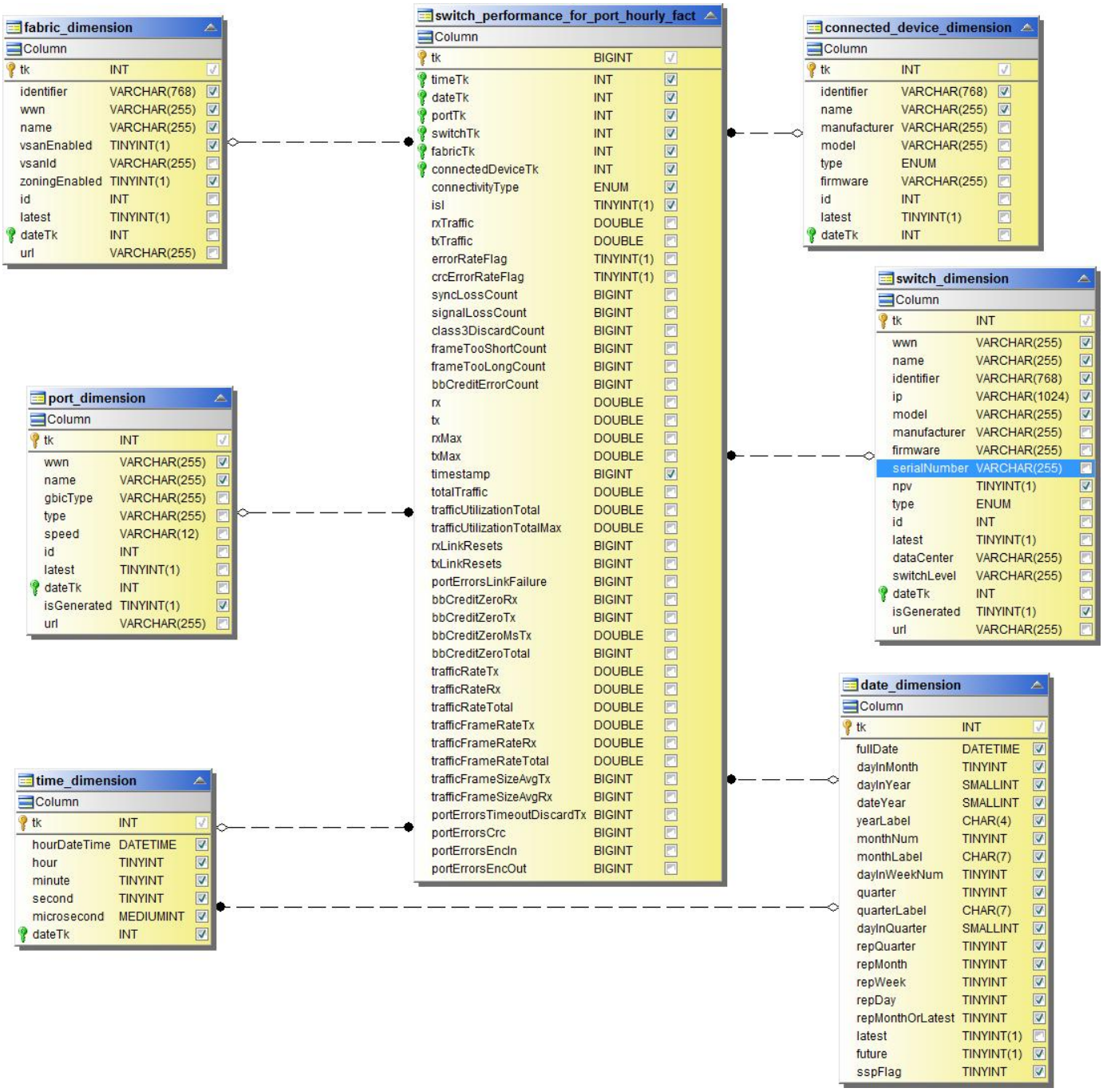
Stündliche Leistung des Speicherknotens



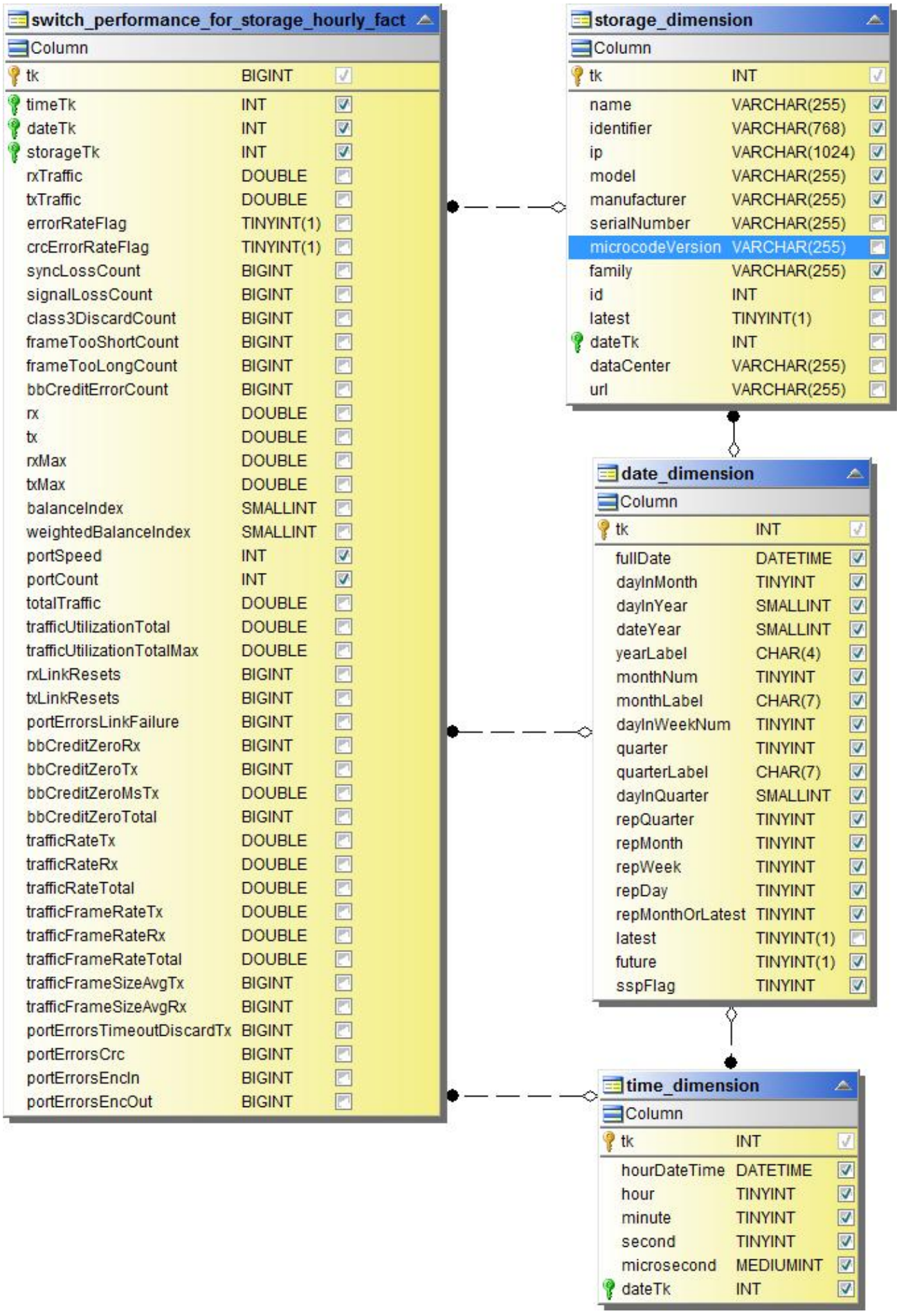
Switch-Stundenleistung für Host



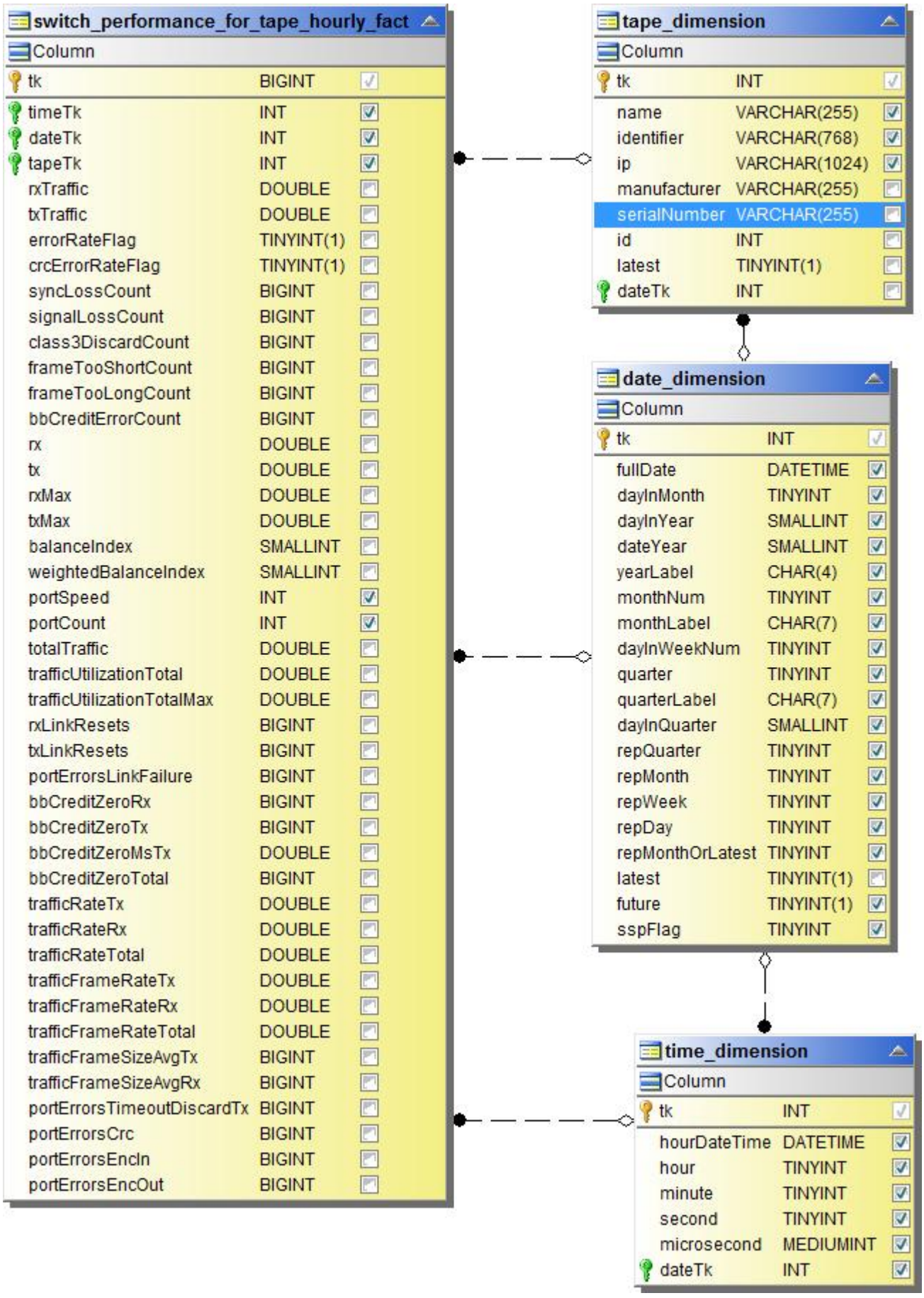
Switch-Stundenleistung für Port



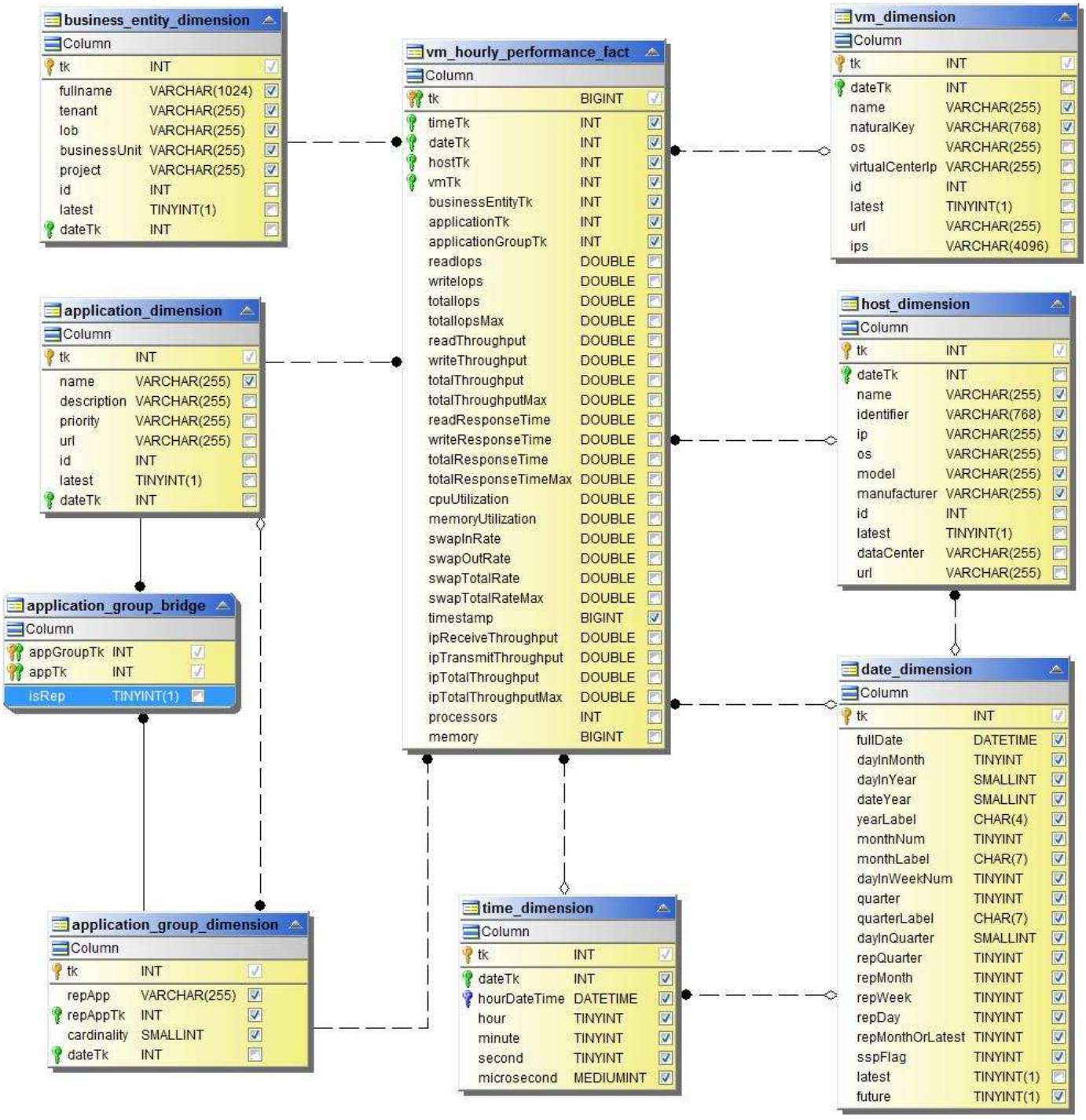
Switch-Stundenleistung für Speicher


switch_performance_for_storage_hourly_fact
Column
tk BIGINT
timeTk INT
dateTk INT
storageTk INT
rxTraffic DOUBLE
txTraffic DOUBLE
errorRateFlag TINYINT(1)
crcErrorRateFlag TINYINT(1)
syncLossCount BIGINT
signalLossCount BIGINT
class3DiscardCount BIGINT
frameTooShortCount BIGINT
frameTooLongCount BIGINT
bbCreditErrorCount BIGINT
rx DOUBLE
tx DOUBLE
rxMax DOUBLE
txMax DOUBLE
balanceIndex SMALLINT
weightedBalanceIndex SMALLINT
portSpeed INT
portCount INT
totalTraffic DOUBLE
trafficUtilizationTotal DOUBLE
trafficUtilizationTotalMax DOUBLE
rxLinkResets BIGINT
txLinkResets BIGINT
portErrorsLinkFailure BIGINT
bbCreditZeroRx BIGINT
bbCreditZeroTx BIGINT
bbCreditZeroMsTx DOUBLE
bbCreditZeroTotal BIGINT
trafficRateTx DOUBLE
trafficRateRx DOUBLE
trafficRateTotal DOUBLE
trafficFrameRateTx DOUBLE
trafficFrameRateRx DOUBLE
trafficFrameRateTotal DOUBLE
trafficFrameSizeAvgTx BIGINT
trafficFrameSizeAvgRx BIGINT
portErrorsTimeoutDiscardTx BIGINT
portErrorsCrc BIGINT
portErrorsEncIn BIGINT
portErrorsEncOut BIGINT
storage_dimension
Column
tk INT
name VARCHAR(255)
identifier VARCHAR(768)
ip VARCHAR(1024)
model VARCHAR(255)
manufacturer VARCHAR(255)
serialNumber VARCHAR(255)
microcodeVersion VARCHAR(255)
family VARCHAR(255)
id INT
latest TINYINT(1)
dateTk INT
dataCenter VARCHAR(255)
url VARCHAR(255)
date_dimension
Column
tk INT
fullDate DATETIME
dayInMonth TINYINT
dayInYear SMALLINT
dateYear SMALLINT
yearLabel CHAR(4)
monthNum TINYINT
monthLabel CHAR(7)
dayInWeekNum TINYINT
quarter TINYINT
quarterLabel CHAR(7)
dayInQuarter SMALLINT
repQuarter TINYINT
repMonth TINYINT
repWeek TINYINT
repDay TINYINT
repMonthOrLatest TINYINT
latest TINYINT(1)
future TINYINT(1)
sspFlag TINYINT
time_dimension
Column
tk INT
hourDateTime DATETIME
hour TINYINT
minute TINYINT
second TINYINT
microsecond MEDIUMINT
dateTk INT

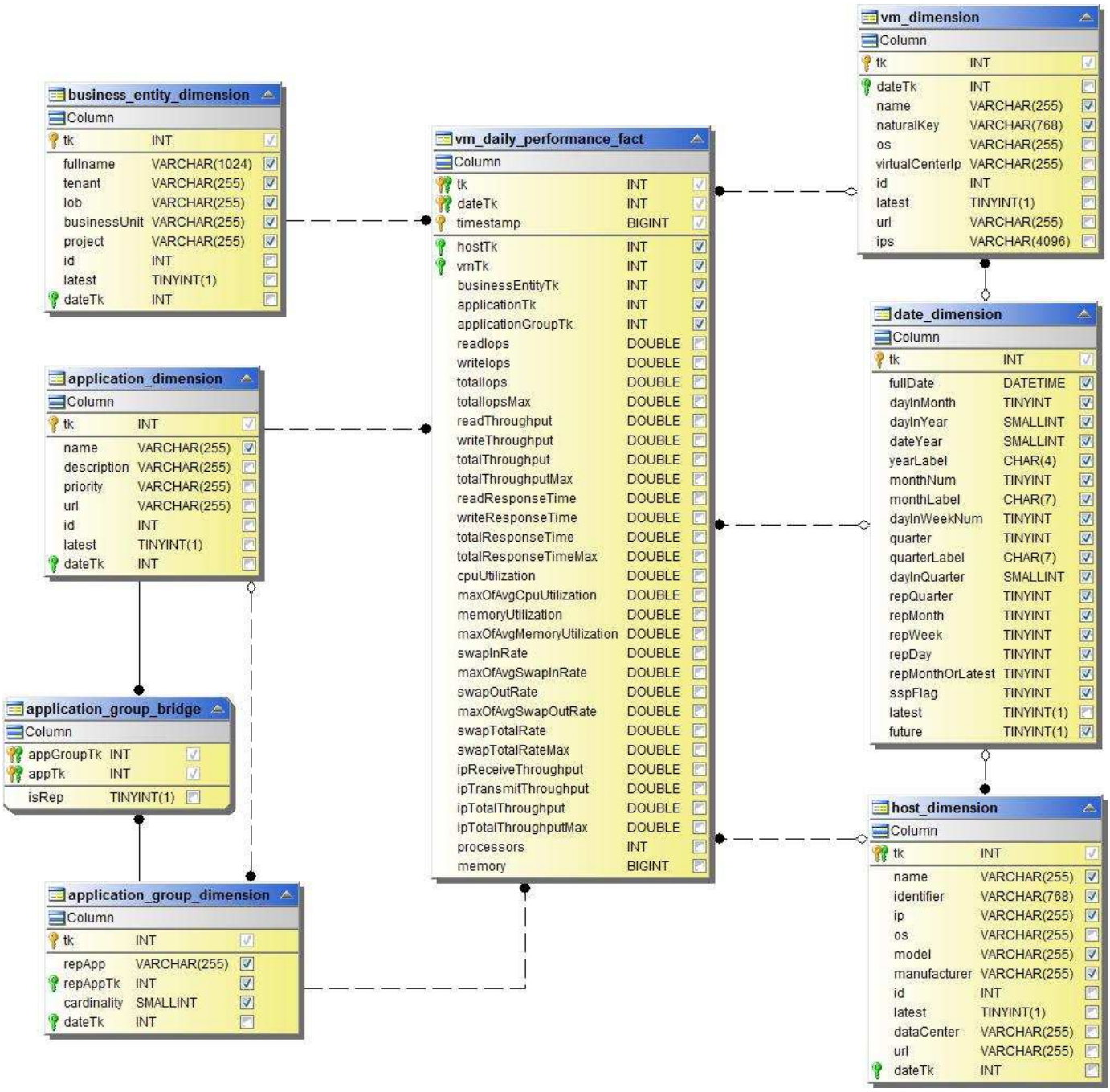
Switch-Stundenleistung für Band



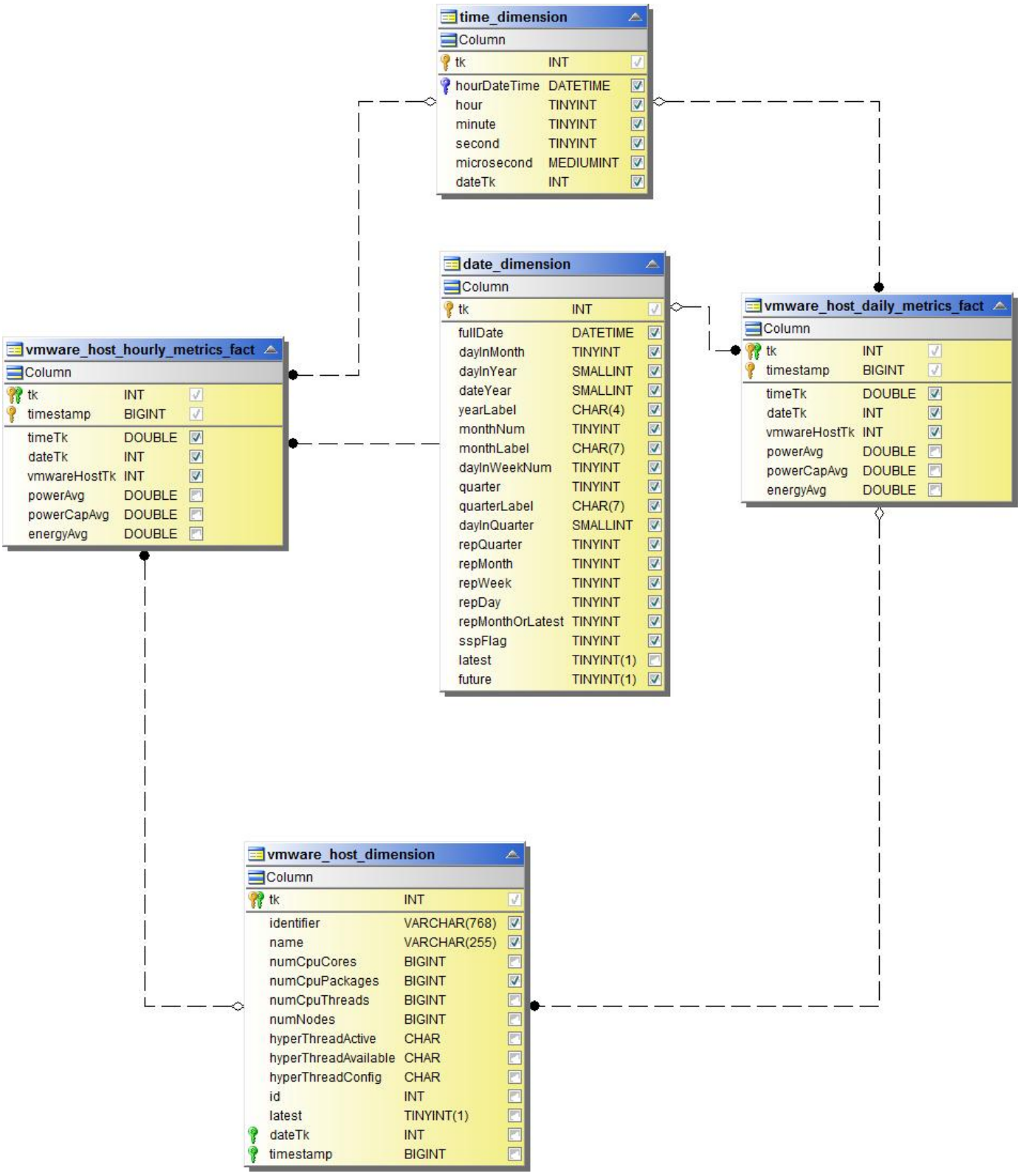
VM-Leistung



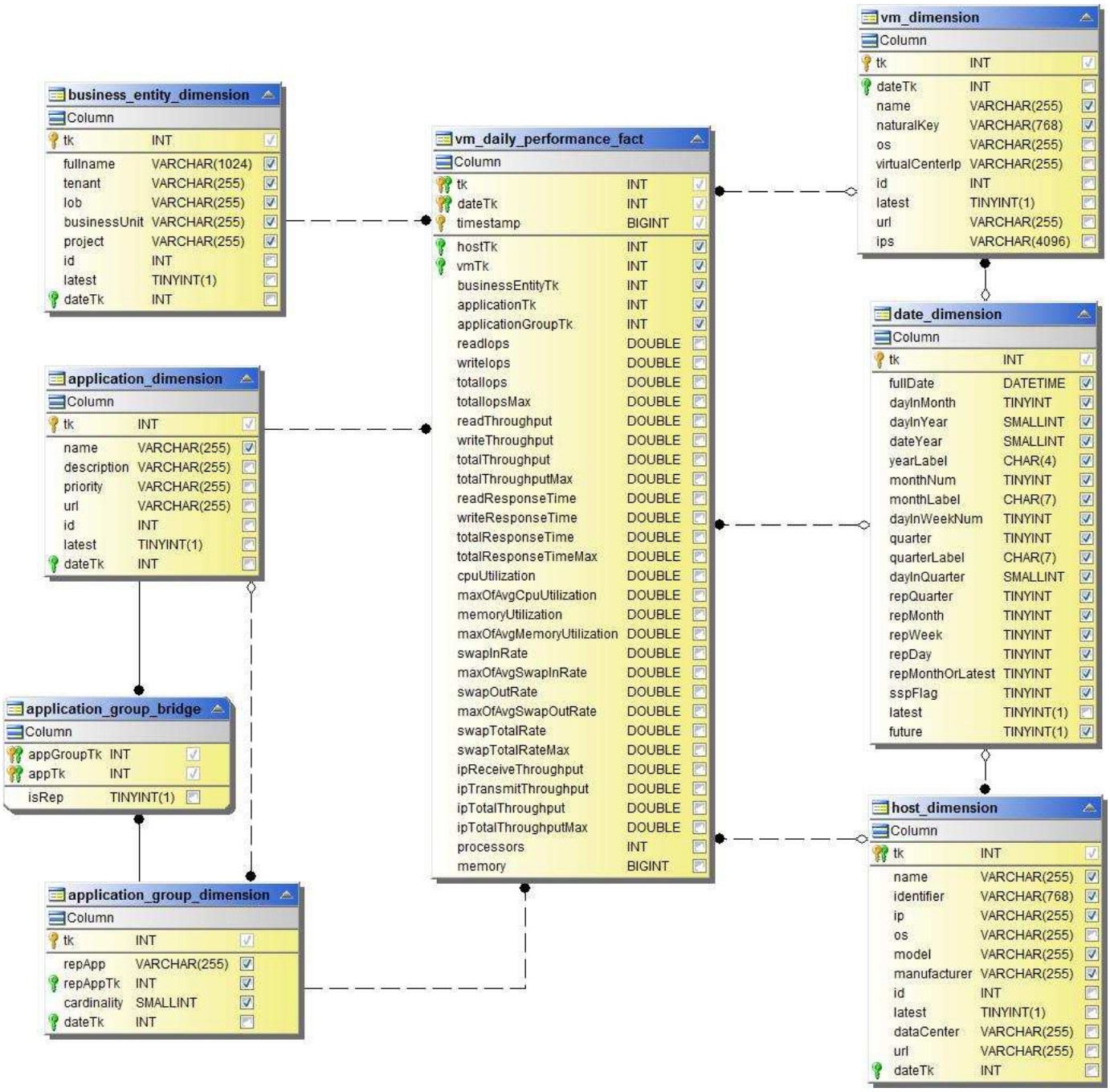
Tägliche VM-Leistung für Host



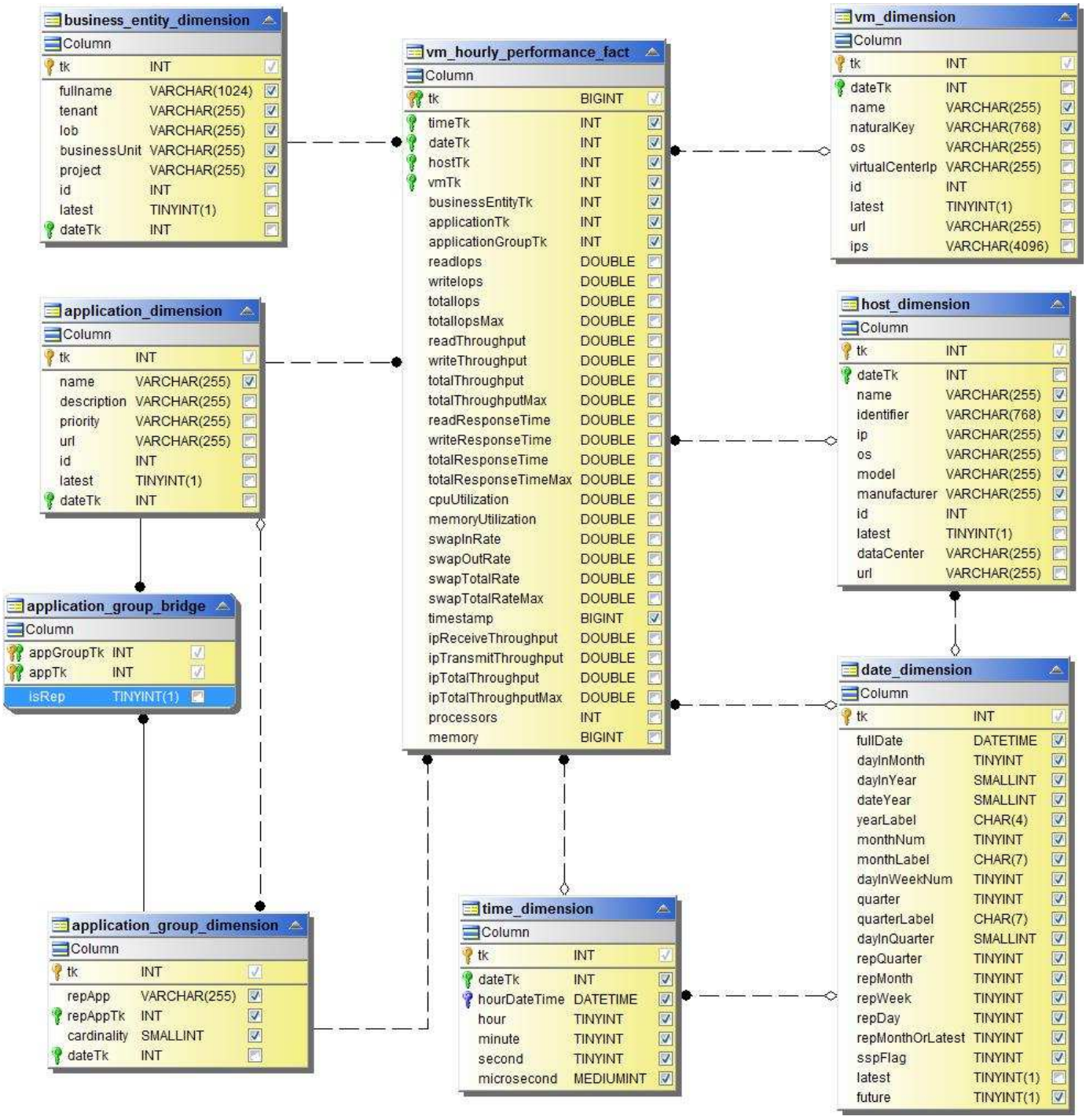
VM-Stundenleistung für Host



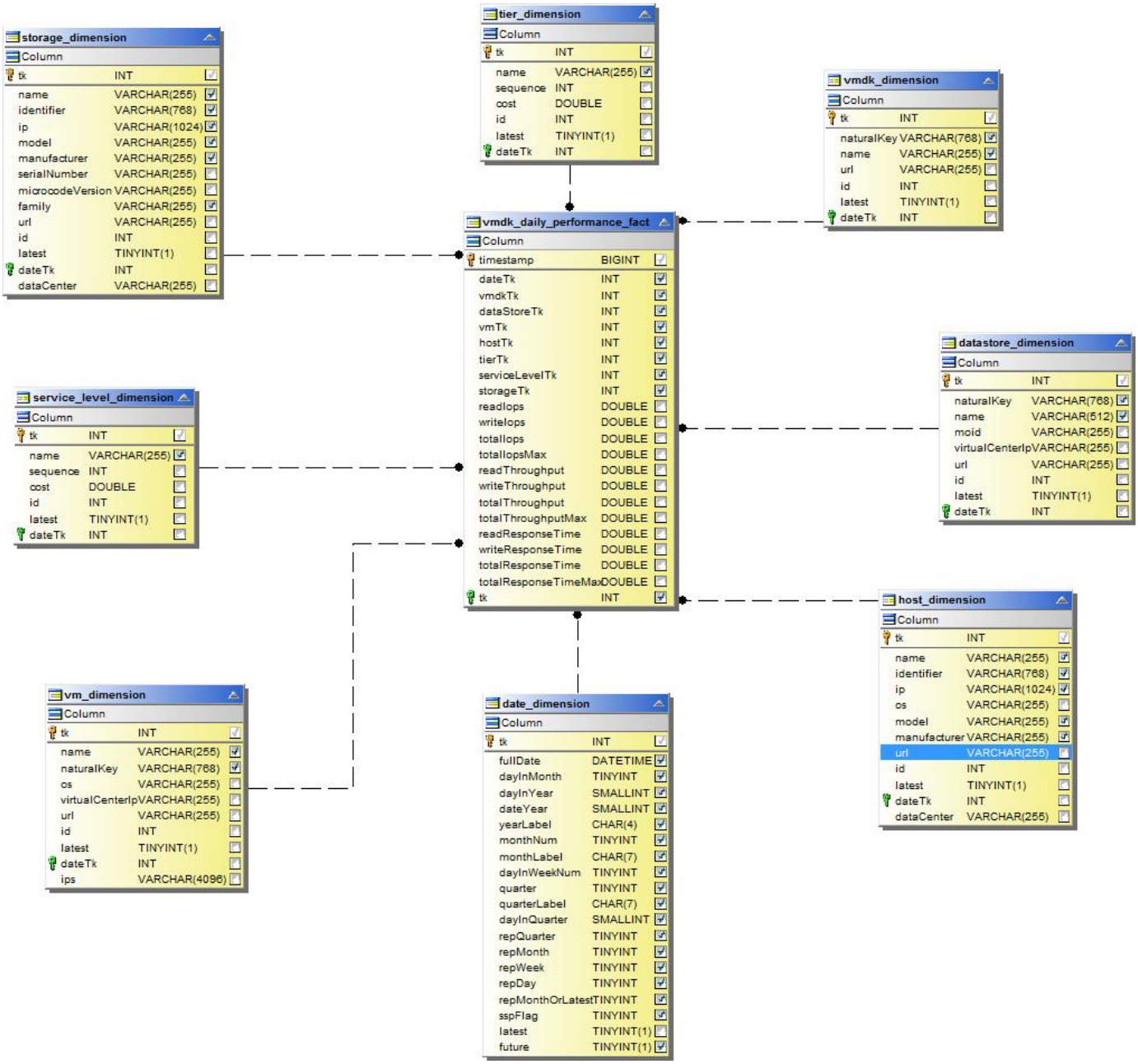
Tägliche VM-Leistung für Host



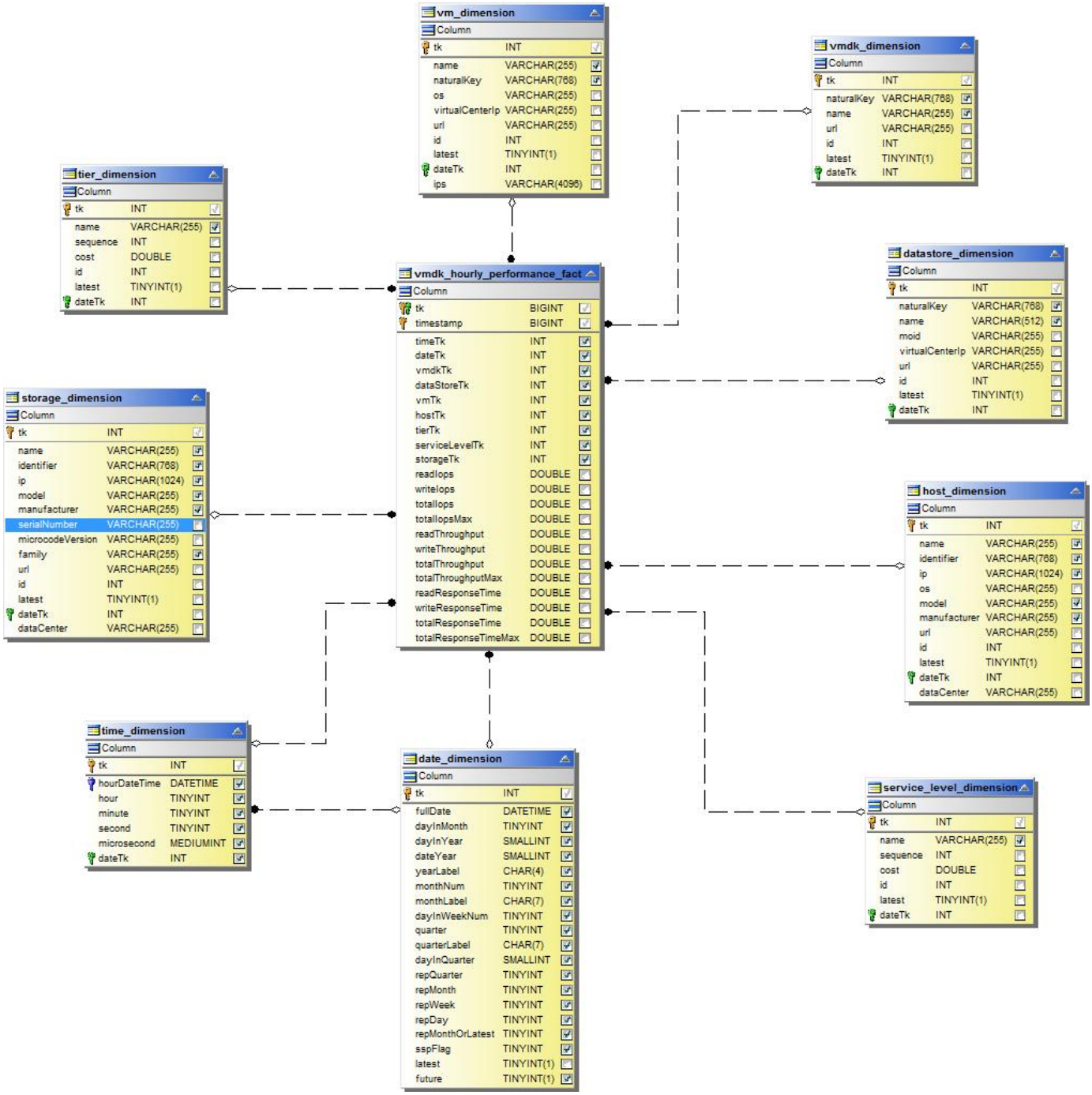
VM-Stundenleistung für Host



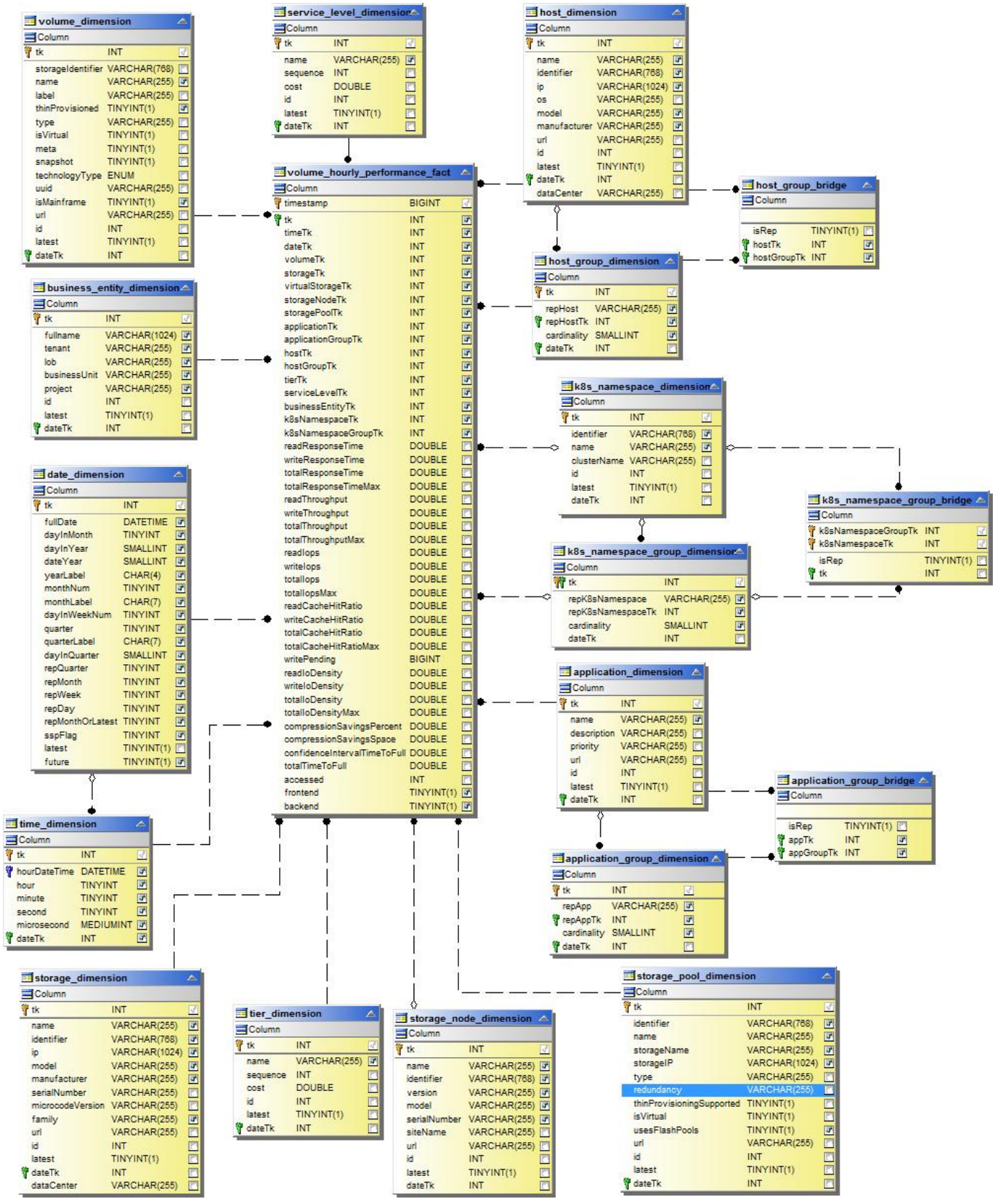
Tägliche VMDK-Leistung



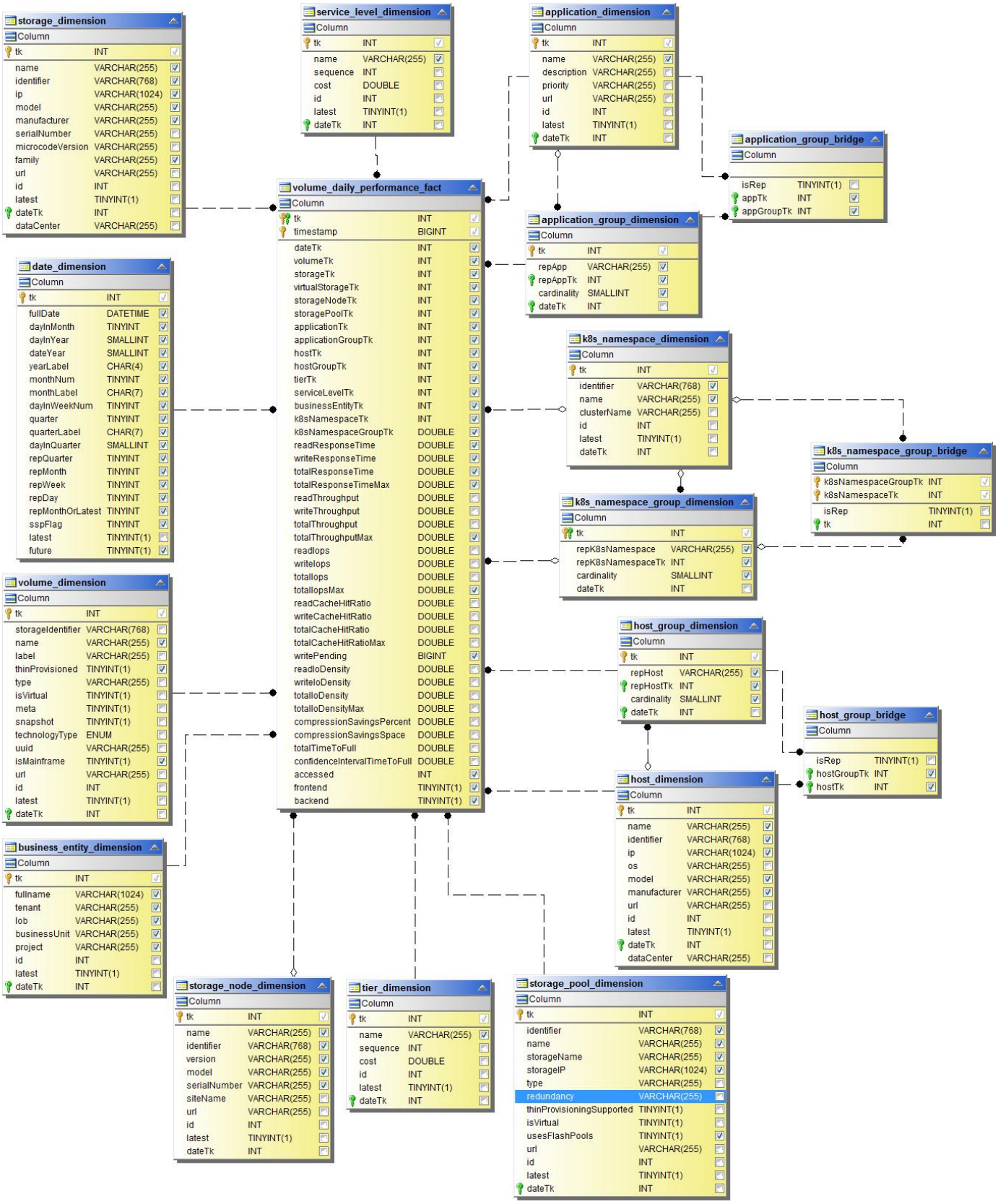
VMDK-Stundenleistung



Volumen Stündliche Leistung



Volumen Tägliche Leistung



Data Infrastructure Insights Schemas für die Berichterstellung

Diese Schematabellen und Diagramme werden hier als Referenz für Data Infrastructure Insights Reporting bereitgestellt.

"Schematabellen"im PDF-Format. Klicken Sie zum Öffnen auf den Link oder klicken Sie mit der rechten Maustaste und wählen Sie *Speichern unter…* zum Herunterladen.

"Schemadiagramme"

Die Berichtsfunktion ist in Data Infrastructure Insights verfügbar"Premium Edition" .

Kubernetes

Übersicht über Kubernetes-Cluster

Der Data Infrastructure Insights Kubernetes Explorer ist ein leistungsstarkes Tool zur Anzeige des Gesamtzustands und der Nutzung Ihrer Kubernetes-Cluster und ermöglicht Ihnen eine einfache Detailansicht der Untersuchungsbereiche.

Durch Klicken auf **Dashboards > Kubernetes Explorer** wird die Seite mit der Kubernetes-Clusterliste geöffnet. Diese Übersichtsseite enthält eine Tabelle der Kubernetes-Cluster auf Ihrem Mandanten.

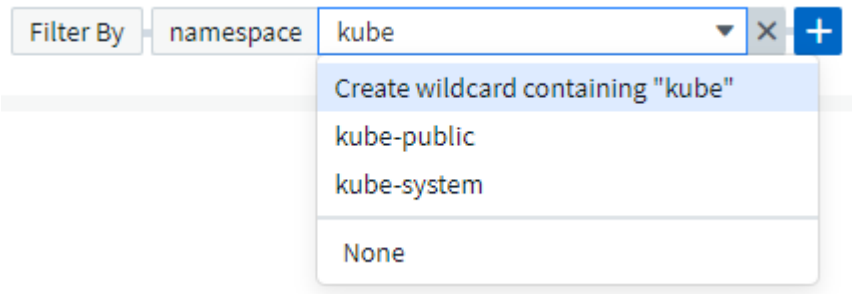
Clusterliste

Die Clusterliste zeigt die folgenden Informationen für jeden Cluster auf Ihrem Mandanten an:

- Cluster **Name**. Durch Klicken auf einen Clusternamen wird das"**Detailseite**" für diesen Cluster.
- *Sättigungs*prozentsätze. Die Gesamtsättigung ist die höchste CPU-, Speicher- oder Speichersättigung.
- Anzahl der **Knoten** im Cluster. Durch Klicken auf diese Nummer wird die Seite mit der Knotenliste geöffnet.
- Anzahl der **Pods** im Cluster. Durch Klicken auf diese Nummer wird die Pod-Listenseite geöffnet.
- Anzahl der **Namespaces** im Cluster. Durch Klicken auf diese Nummer wird die Seite mit der Namespace-Liste geöffnet.
- Anzahl der **Workloads** im Cluster. Durch Klicken auf diese Nummer wird die Seite mit der Arbeitslastliste geöffnet.

Verfeinern des Filters

Wenn Sie beim Filtern mit der Eingabe beginnen, wird Ihnen die Option angezeigt, einen **Platzhalterfilter** basierend auf dem aktuellen Text zu erstellen. Wenn Sie diese Option auswählen, werden alle Ergebnisse zurückgegeben, die mit dem Platzhalterausdruck übereinstimmen. Sie können **Ausdrücke** auch mit NOT oder AND erstellen oder die Option „Keine“ auswählen, um nach Nullwerten im Feld zu filtern.



Filter, die auf Platzhaltern oder Ausdrücken basieren (z. B. NICHT, UND, „Keine“ usw.), werden im Filterfeld

dunkelblau angezeigt. Elemente, die Sie direkt aus der Liste auswählen, werden hellblau angezeigt.

Kubernetes-Filter sind kontextbezogen. Das bedeutet beispielsweise, dass, wenn Sie sich auf einer bestimmten Knotenseite befinden, der Filter „pod_name“ nur Pods auflistet, die mit diesem Knoten in Zusammenhang stehen. Wenn Sie außerdem einen Filter für einen bestimmten Namespace anwenden, listet der Pod_Name-Filter nur Pods auf diesem Knoten *und* in diesem Namespace auf.

Beachten Sie, dass die Platzhalter- und Ausdrucksfilterung mit Text oder Listen funktioniert, jedoch nicht mit Zahlen, Datumsangaben oder Booleschen Werten.

Vor der Installation oder Aktualisierung des NetApp Kubernetes Monitoring Operator

Lesen Sie diese Informationen, bevor Sie das"Kubernetes-Überwachungsoperator" .

Komponente	Erfordernis
Kubernetes-Version	Kubernetes v1.20 und höher.
Kubernetes-Distributionen	AWS Elastic Kubernetes Service (EKS) Azure Kubernetes Service (AKS) Google Kubernetes Engine (GKE) Red Hat OpenShift Rancher Kubernetes Engine (RKE) VMware Tanzu
Linux-Betriebssystem	Data Infrastructure Insights unterstützt keine Knoten, die mit Arm64-Architektur ausgeführt werden. Netzwerküberwachung: Es muss Linux-Kernel Version 4.18.0 oder höher ausgeführt werden. Photon OS wird nicht unterstützt.
Labels	Data Infrastructure Insights unterstützt die Überwachung von Kubernetes-Knoten, auf denen Linux ausgeführt wird, indem ein Kubernetes-Knotenselektor angegeben wird, der auf diesen Plattformen nach den folgenden Kubernetes-Labels sucht: Kubernetes v1.20 und höher: Kubernetes.io/os = Linux Rancher + cattle.io als Orchestrierungs-/Kubernetes-Plattform: cattle.io/os = Linux
Befehle	Die Befehle „curl“ und „kubectl“ müssen verfügbar sein. Für optimale Ergebnisse fügen Sie diese Befehle dem PATH hinzu.

Komponente	Erfordernis
Konnektivität	kubectl cli ist für die Kommunikation mit dem Ziel-K8s-Cluster konfiguriert und verfügt über eine Internetverbindung zu Ihrer Data Infrastructure Insights -Umgebung. Wenn Sie sich während der Installation hinter einem Proxy befinden, folgen Sie den Anweisungen im"Konfigurieren der Proxy-Unterstützung" Abschnitt der Operator-Installation. Für eine genaue Prüfung und Datenberichterstattung synchronisieren Sie die Zeit auf dem Agent-Computer mithilfe des Network Time Protocol (NTP) oder Simple Network Time Protocol (SNTP).
Sonstige	Wenn Sie OpenShift 4.6 oder höher verwenden, müssen Sie die folgenden Schritte ausführen:"OpenShift-Anweisungen" zusätzlich zur Sicherstellung, dass diese Voraussetzungen erfüllt sind.
API-Token	Wenn Sie den Operator erneut bereitstellen (d. h. ihn aktualisieren oder ersetzen), müssen Sie kein neues API-Token erstellen. Sie können das vorherige Token wiederverwenden.

Wichtige Hinweise vor dem Start

Wenn Sie mit einemProxy , haben einebenutzerdefiniertes Repository oder verwendenOpenShift , lesen Sie die folgenden Abschnitte sorgfältig durch.

Lesen Sie auch überBerechtigungen .

Konfigurieren der Proxy-Unterstützung

Es gibt zwei Stellen, an denen Sie einen Proxy auf Ihrem Mandanten verwenden können, um den NetApp Kubernetes Monitoring Operator zu installieren. Dabei kann es sich um dasselbe oder um separate Proxy-Systeme handeln:

- Proxy, der während der Ausführung des Installationscode-Snippets (mit „curl“) benötigt wird, um das System, auf dem das Snippet ausgeführt wird, mit Ihrer Data Infrastructure Insights -Umgebung zu verbinden
- Proxy, der vom Ziel-Kubernetes-Cluster zur Kommunikation mit Ihrer Data Infrastructure Insights -Umgebung benötigt wird

Wenn Sie für eines oder beides einen Proxy verwenden, müssen Sie zur Installation des NetApp Kubernetes Operating Monitor zunächst sicherstellen, dass Ihr Proxy so konfiguriert ist, dass eine gute Kommunikation mit Ihrer Data Infrastructure Insights Umgebung möglich ist. Beispielsweise müssen Sie von den Servern/VMs, von denen Sie den Operator installieren möchten, auf Data Infrastructure Insights zugreifen und Binärdateien von Data Infrastructure Insights herunterladen können.

Legen Sie für den Proxy, der zur Installation des NetApp Kubernetes Operating Monitor verwendet wird, vor der Installation des Operators die Umgebungsvariablen *http_proxy/https_proxy* fest. Für einige Proxy-Umgebungen müssen Sie möglicherweise auch die Umgebungsvariable *no_proxy* festlegen.

Um die Variable(n) festzulegen, führen Sie **vor** der Installation des NetApp Kubernetes Monitoring Operator die

folgenden Schritte auf Ihrem System aus:

1. Legen Sie die Umgebungsvariable(n) *https_proxy* und/oder *http_proxy* für den aktuellen Benutzer fest:
   a. Wenn der einzurichtende Proxy keine Authentifizierung (Benutzername/Passwort) hat, führen Sie den folgenden Befehl aus:

```
 export https_proxy=<proxy_server>:<proxy_port>
.. Wenn der einzurichtende Proxy über eine Authentifizierung
(Benutzername/Passwort) verfügt, führen Sie diesen Befehl aus:
```

```
export
http_proxy=<proxy_username>:<proxy_password>@<proxy_server>:<proxy_po
rt>
```

Damit der für Ihren Kubernetes-Cluster verwendete Proxy mit Ihrer Data Infrastructure Insights -Umgebung kommunizieren kann, installieren Sie nach dem Lesen aller dieser Anweisungen den NetApp Kubernetes Monitoring Operator.

Konfigurieren Sie den Proxy-Abschnitt der AgentConfiguration in operator-config.yaml, bevor Sie den NetApp Kubernetes Monitoring Operator bereitstellen.

```
agent:
  ...
  proxy:
    server: <server for proxy>
    port: <port for proxy>
    username: <username for proxy>
    password: <password for proxy>

    # In the noproxy section, enter a comma-separated list of
    # IP addresses and/or resolvable hostnames that should bypass
    # the proxy
    noproxy: <comma separated list>

    isTelegrafProxyEnabled: true
    isFluentbitProxyEnabled: <true or false> # true if Events Log enabled
    isCollectorsProxyEnabled: <true or false> # true if Network
Performance and Map enabled
    isAuProxyEnabled: <true or false> # true if AU enabled
  ...
...
```

Verwenden eines benutzerdefinierten oder privaten Docker-Repositorys

Standardmäßig ruft der NetApp Kubernetes Monitoring Operator Container-Images aus dem Data Infrastructure Insights -Repository ab. Wenn Sie einen Kubernetes-Cluster als Ziel für die Überwachung verwenden und dieser Cluster so konfiguriert ist, dass er nur Container-Images aus einem benutzerdefinierten oder privaten Docker-Repository oder einer Container-Registrierung abruft, müssen Sie den Zugriff auf die vom NetApp Kubernetes Monitoring Operator benötigten Container konfigurieren.

Führen Sie das „Image Pull Snippet“ aus der Installationskachel des NetApp Monitoring Operator aus. Mit diesem Befehl melden Sie sich beim Data Infrastructure Insights -Repository an, rufen alle Bildabhängigkeiten für den Operator ab und melden sich vom Data Infrastructure Insights -Repository ab. Geben Sie bei der entsprechenden Aufforderung das bereitgestellte temporäre Repository-Passwort ein. Dieser Befehl lädt alle vom Bediener verwendeten Bilder herunter, auch für optionale Funktionen. Unten sehen Sie, für welche Funktionen diese Bilder verwendet werden.

Kernoperator-Funktionalität und Kubernetes-Überwachung

- NetApp-Überwachung
- Kube-RBAC-Proxy
- Kube-State-Metriken
- Telegraf
- Distroless-Root-Benutzer

Ereignisprotokoll

- fließendes Bit
- Kubernetes-Ereignis-Exporteur

Netzwerkleistung und Karte

- ci-net-observer

Übertragen Sie das Operator-Docker-Image gemäß Ihren Unternehmensrichtlinien in Ihr privates/lokales/Unternehmens-Docker-Repository. Stellen Sie sicher, dass die Bild-Tags und Verzeichnispfade zu diesen Bildern in Ihrem Repository mit denen im Data Infrastructure Insights -Repository übereinstimmen.

Bearbeiten Sie die Bereitstellung des Überwachungsoperators in operator-deployment.yaml und ändern Sie alle Bildreferenzen, um Ihr privates Docker-Repository zu verwenden.

```
image: <docker repo of the enterprise/corp docker repo>/kube-rbac-
proxy:<kube-rbac-proxy version>
image: <docker repo of the enterprise/corp docker repo>/netapp-
monitoring:<version>
```

Bearbeiten Sie die AgentConfiguration in operator-config.yaml, um den neuen Speicherort des Docker-Repositorys widerzuspiegeln. Erstellen Sie ein neues imagePullSecret für Ihr privates Repository. Weitere Informationen finden Sie unter *https://kubernetes.io/docs/tasks/configure-pod-container/pull-image-private-registry/*

```
agent:
  ...
  # An optional docker registry where you want docker images to be pulled
from as compared to CI's docker registry
  # Please see documentation for
xref:{relative_path}task_config_telegraf_agent_k8s.html#using-a-custom-or-
private-docker-repository[using a custom or private docker repository].
  dockerRepo: your.docker.repo/long/path/to/test
  # Optional: A docker image pull secret that maybe needed for your
private docker registry
  dockerImagePullSecret: docker-secret-name
```

OpenShift-Anweisungen

Wenn Sie OpenShift 4.6 oder höher verwenden, müssen Sie die AgentConfiguration in *operator-config.yaml* bearbeiten, um die Einstellung *runPrivileged* zu aktivieren:

```
# Set runPrivileged to true SELinux is enabled on your kubernetes nodes
runPrivileged: true
```

Openshift implementiert möglicherweise eine zusätzliche Sicherheitsebene, die den Zugriff auf einige Kubernetes-Komponenten blockieren kann.

Berechtigungen

Wenn der Cluster, den Sie überwachen, benutzerdefinierte Ressourcen enthält, die keine ClusterRole haben, die"Aggregate zum Anzeigen" , müssen Sie dem Operator manuell Zugriff auf diese Ressourcen gewähren, um sie mit Ereignisprotokollen zu überwachen.

1. Bearbeiten Sie *operator-additional-permissions.yaml* vor der Installation oder bearbeiten Sie nach der Installation die Ressource *ClusterRole/<namespace>-additional-permissions*
2. Erstellen Sie eine neue Regel für die gewünschten API-Gruppen und Ressourcen mit den Verben ["get", "watch", "list"]. Siehe https://kubernetes.io/docs/reference/access-authn-authz/rbac/
3. Wenden Sie Ihre Änderungen auf den Cluster an

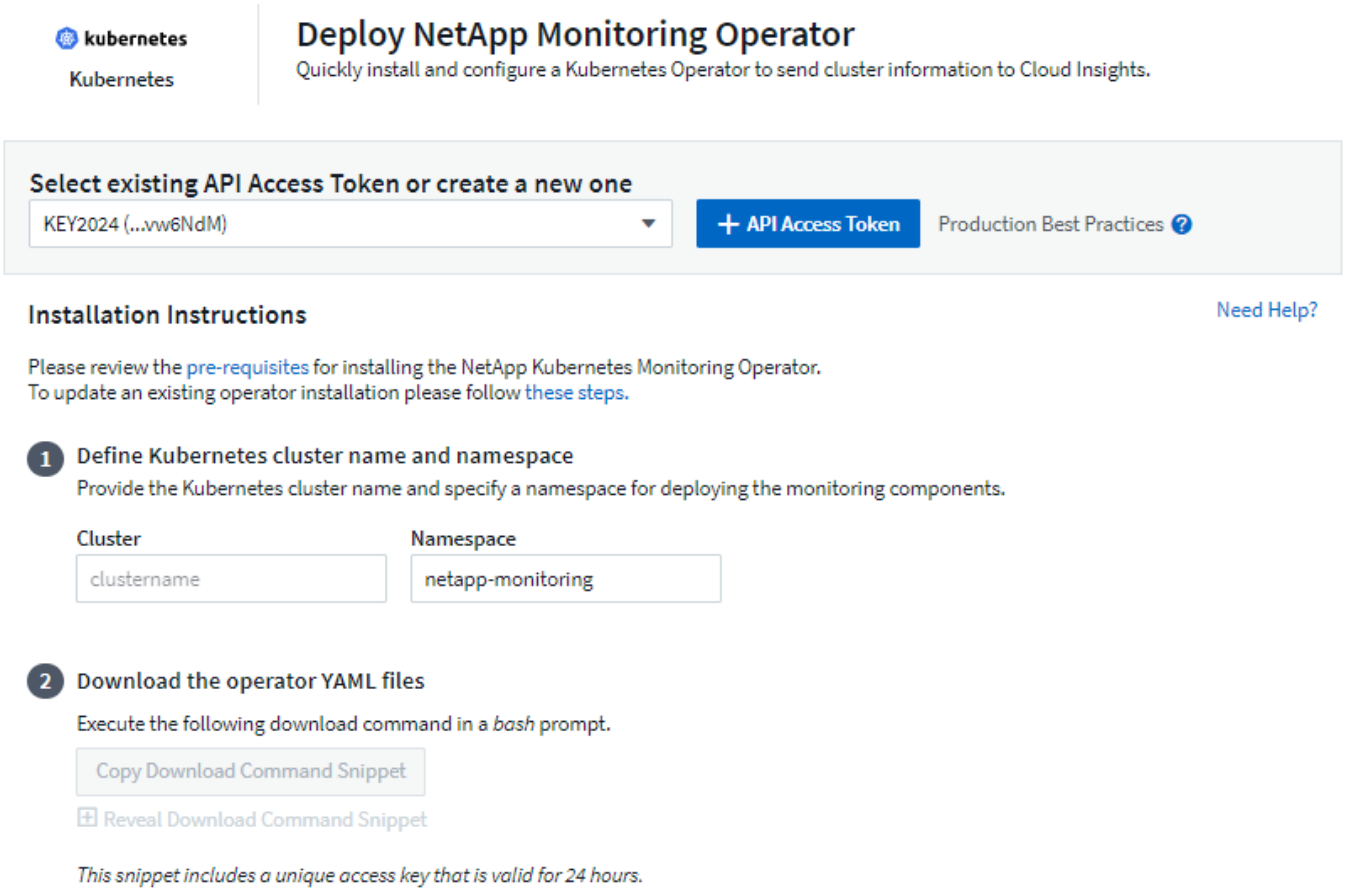
Installation und Konfiguration des Kubernetes Monitoring Operators

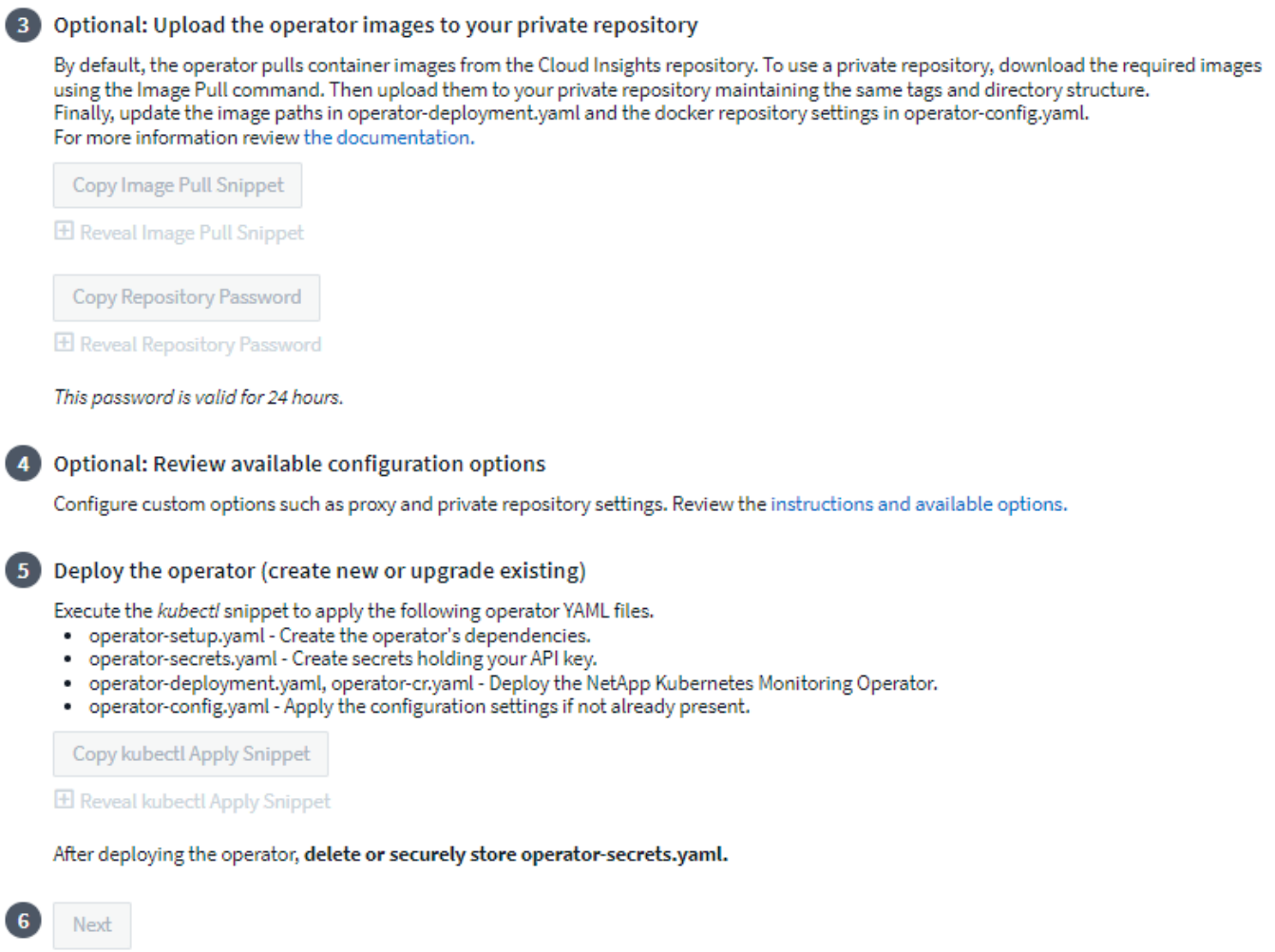
Data Infrastructure Insights bietet den **Kubernetes Monitoring Operator** für die Kubernetes-Sammlung. Navigieren Sie zu **Kubernetes > Collectors > +Kubernetes Collector**, um einen neuen Operator bereitzustellen.

Vor der Installation des Kubernetes Monitoring Operator

Siehe die"Voraussetzungen" Dokumentation, bevor Sie den Kubernetes Monitoring Operator installieren oder aktualisieren.

Installieren des Kubernetes Monitoring Operators





Schritte zum Installieren des Kubernetes Monitoring Operator-Agenten auf Kubernetes:

1. Geben Sie einen eindeutigen Clusternamen und Namespace ein. Wenn SieUpgrade von einem vorherigen Kubernetes-Operator, verwenden Sie denselben Clusternamen und Namespace.
2. Sobald diese eingegeben sind, können Sie den Download-Befehlsausschnitt in die Zwischenablage kopieren.
3. Fügen Sie den Snippet in ein *Bash*-Fenster ein und führen Sie ihn aus. Die Operator-Installationsdateien werden heruntergeladen. Beachten Sie, dass das Snippet einen eindeutigen Schlüssel hat und 24 Stunden gültig ist.
4. Wenn Sie ein benutzerdefiniertes oder privates Repository haben, kopieren Sie den optionalen Image Pull-Ausschnitt, fügen Sie ihn in eine *Bash*-Shell ein und führen Sie ihn aus. Sobald die Bilder abgerufen wurden, kopieren Sie sie in Ihr privates Repository. Achten Sie darauf, dieselben Tags und dieselbe Ordnerstruktur beizubehalten. Aktualisieren Sie die Pfade in *operator-deployment.yaml* sowie die Docker-Repository-Einstellungen in *operator-config.yaml*.
5. Überprüfen Sie bei Bedarf die verfügbaren Konfigurationsoptionen wie Proxy- oder private Repository-Einstellungen. Weitere Informationen finden Sie unter"Konfigurationsoptionen" .
6. Wenn Sie bereit sind, stellen Sie den Operator bereit, indem Sie das kubectl Apply-Snippet kopieren, herunterladen und ausführen.
7. Die Installation erfolgt automatisch. Wenn der Vorgang abgeschlossen ist, klicken Sie auf die Schaltfläche *Weiter*.

8. Wenn die Installation abgeschlossen ist, klicken Sie auf die Schaltfläche *Weiter*. Denken Sie daran, auch die Datei *operator-secrets.yaml* zu löschen oder sicher zu speichern.

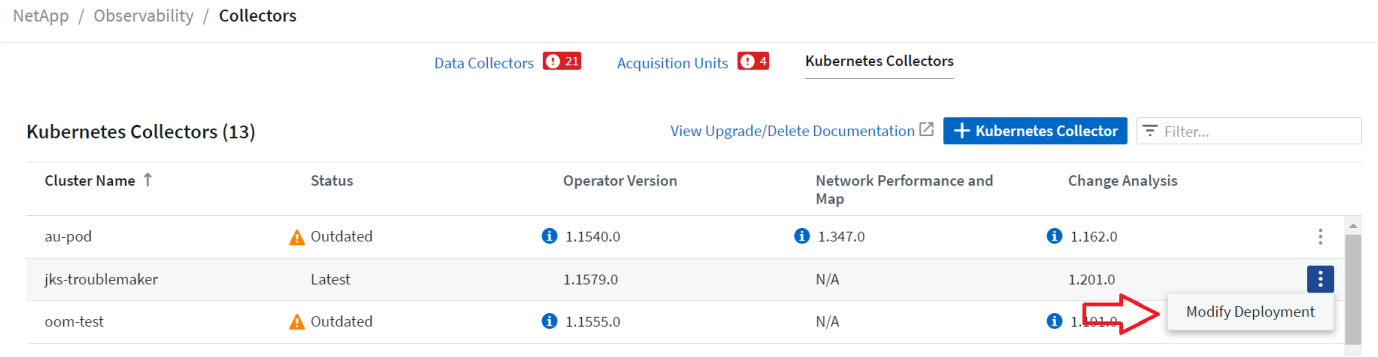
Wenn Sie ein benutzerdefiniertes Repository haben, lesen Sie überVerwenden eines benutzerdefinierten/privaten Docker-Repositorys .

Kubernetes-Überwachungskomponenten

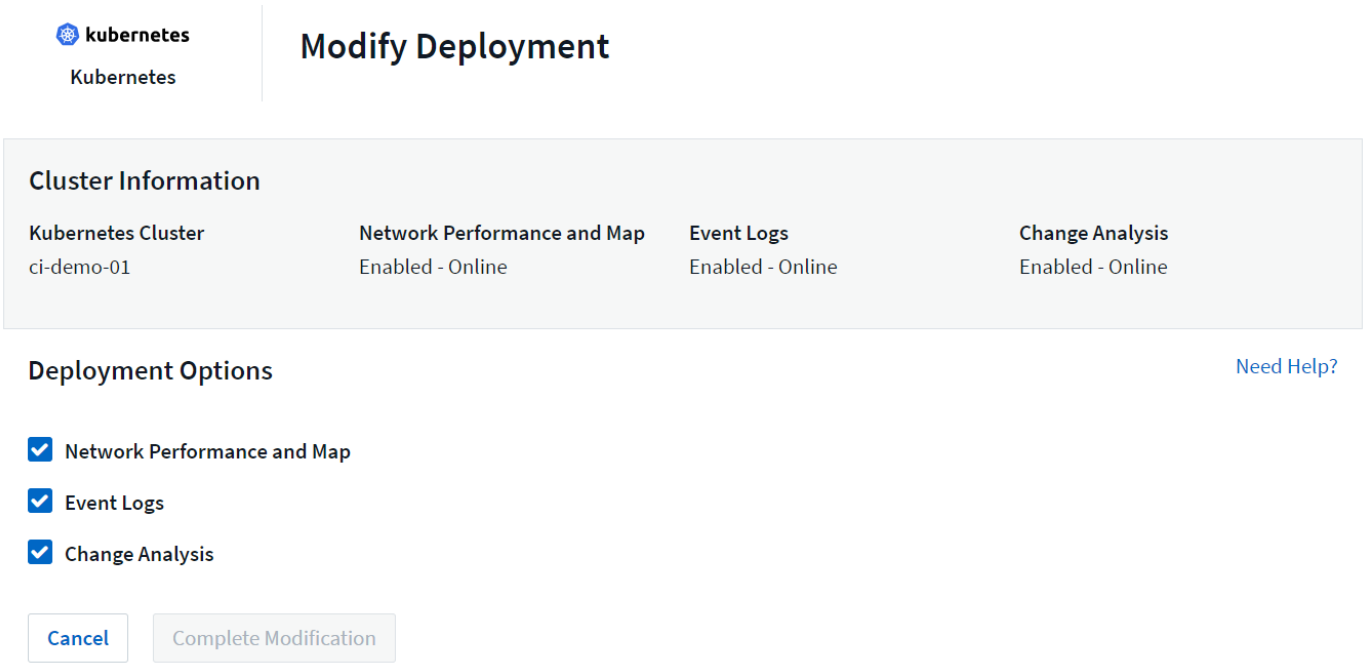
Data Infrastructure Insights Kubernetes Monitoring besteht aus vier Überwachungskomponenten:

- Clustermetriken
- Netzwerkleistung und Karte (optional)
- Ereignisprotokolle (optional)
- Änderungsanalyse (optional)

Die oben genannten optionalen Komponenten sind standardmäßig für jeden Kubernetes-Collector aktiviert. Wenn Sie entscheiden, dass Sie eine Komponente für einen bestimmten Collector nicht benötigen, können Sie sie deaktivieren, indem Sie zu **Kubernetes > Collectors** navigieren und im Drei-Punkte-Menü des Collectors auf der rechten Bildschirmseite *Bereitstellung ändern* auswählen.



Der Bildschirm zeigt den aktuellen Status jeder Komponente an und ermöglicht Ihnen, Komponenten für diesen Collector nach Bedarf zu deaktivieren oder zu aktivieren.



Upgrade auf den neuesten Kubernetes Monitoring Operator

DII-Druckknopf-Upgrades

Sie können den Kubernetes Monitoring Operator über die DII Kubernetes Collectors-Seite aktualisieren. Klicken Sie auf das Menü neben dem Cluster, den Sie aktualisieren möchten, und wählen Sie *Upgrade*. Der Betreiber überprüft die Bildsignaturen, erstellt einen Snapshot Ihrer aktuellen Installation und führt das Upgrade durch. Innerhalb weniger Minuten sollte der Status des Operators von „Upgrade läuft“ bis „Neueste“ fortschreiten. Wenn ein Fehler auftritt, können Sie für weitere Einzelheiten den Fehlerstatus auswählen und die Tabelle zur Fehlerbehebung bei Push-Button-Upgrades weiter unten zu Rate ziehen.

Push-Button-Upgrades mit privaten Repositories

Wenn Ihr Operator für die Verwendung eines privaten Repositorys konfiguriert ist, stellen Sie bitte sicher, dass alle zum Ausführen des Operators erforderlichen Bilder und deren Signaturen in Ihrem Repository verfügbar sind. Wenn während des Upgrade-Vorgangs ein Fehler aufgrund fehlender Bilder auftritt, fügen Sie diese einfach zu Ihrem Repository hinzu und versuchen Sie das Upgrade erneut. Um die Bildsignaturen in Ihr Repository hochzuladen, verwenden Sie bitte das Cosign-Tool wie folgt und stellen Sie sicher, dass Sie Signaturen für alle unter 3 angegebenen Bilder hochladen. Optional: Laden Sie die Operatorbilder in Ihr privates Repository hoch > Image Pull Snippet

```
cosign copy example.com/src:v1 example.com/dest:v1
#Example
cosign copy <DII container registry>/netapp-monitoring:<image version>
<private repository>/netapp-monitoring:<image version>
```

Rollback auf eine zuvor ausgeführte Version

Wenn Sie das Upgrade mithilfe der Funktion „Upgrade per Knopfdruck“ durchgeführt haben und innerhalb von sieben Tagen nach dem Upgrade Probleme mit der aktuellen Version des Operators auftreten, können Sie mithilfe des während des Upgrade-Vorgangs erstellten Snapshots ein Downgrade auf die zuvor ausgeführte

Version durchführen. Klicken Sie auf das Menü neben dem Cluster, für den Sie ein Rollback durchführen möchten, und wählen Sie *Rollback* aus.

Manuelle Upgrades

Stellen Sie fest, ob eine Agentenkonfiguration mit dem vorhandenen Operator vorhanden ist (wenn Ihr Namespace nicht der Standardnamespace *netapp-monitoring* ist, ersetzen Sie ihn durch den entsprechenden Namespace):

```
 kubectl -n netapp-monitoring get agentconfiguration netapp-ci-monitoring-
configuration
Wenn eine Agentenkonfiguration vorhanden ist:
```

- Installierender neueste Operator über den vorhandenen Operator.
  - Stellen Sie sicher, dass SieAbrufen der neuesten Container-Images wenn Sie ein benutzerdefiniertes Repository verwenden.

Wenn die Agentenkonfiguration nicht vorhanden ist:

- Notieren Sie sich den von Data Infrastructure Insights erkannten Clusternamen (wenn Ihr Namespace nicht der Standardnamespace „netapp-monitoring“ ist, ersetzen Sie ihn durch den entsprechenden Namespace):

```
 kubectl -n netapp-monitoring get agent -o
jsonpath='{.items[0].spec.cluster-name}'
* Erstellen Sie eine Sicherungskopie des vorhandenen Operators (wenn Ihr
Namespace nicht der Standard-Netapp-Monitoring-Namespace ist, ersetzen
Sie ihn durch den entsprechenden Namespace):
```

```
 kubectl -n netapp-monitoring get agent -o yaml > agent_backup.yaml
* <<to-remove-the-kubernetes-monitoring-operator,Deinstallieren>>der
bestehende Betreiber.
* <<installing-the-kubernetes-monitoring-operator,Installieren>>der
neueste Operator.
```

  - Verwenden Sie denselben Clusternamen.
  - Nachdem Sie die neuesten Operator-YAML-Dateien heruntergeladen haben, portieren Sie vor der Bereitstellung alle in agent_backup.yaml gefundenen Anpassungen in die heruntergeladene operator-config.yaml.
  - Stellen Sie sicher, dass SieAbrufen der neuesten Container-Images wenn Sie ein benutzerdefiniertes Repository verwenden.

Stoppen und Starten des Kubernetes-Überwachungsoperators

So stoppen Sie den Kubernetes Monitoring Operator:

```
 kubectl -n netapp-monitoring scale deploy monitoring-operator
--replicas=0
So starten Sie den Kubernetes Monitoring Operator:
```

```
kubectl -n netapp-monitoring scale deploy monitoring-operator --replicas=1
```

Deinstallation

So entfernen Sie den Kubernetes Monitoring Operator

Beachten Sie, dass der Standardnamespace für den Kubernetes Monitoring Operator „netapp-monitoring“ ist. Wenn Sie Ihren eigenen Namespace festgelegt haben, ersetzen Sie diesen Namespace in diesen und allen nachfolgenden Befehlen und Dateien.

Neuere Versionen des Monitoring-Operators können mit den folgenden Befehlen deinstalliert werden:

```
kubectl -n <NAMESPACE> delete agent -l installed-by=nkmo-<NAMESPACE>
kubectl -n <NAMESPACE> delete
clusterrole,clusterrolebinding,crd,svc,deploy,role,rolebinding,secret,sa
-l installed-by=nkmo-<NAMESPACE>
```

Wenn der Überwachungsoperator in seinem eigenen dedizierten Namespace bereitgestellt wurde, löschen Sie den Namespace:

```
 kubectl delete ns <NAMESPACE>
Hinweis: Wenn der erste Befehl „Keine Ressourcen gefunden“ zurückgibt,
befolgen Sie die folgenden Anweisungen, um ältere Versionen des
Überwachungsoperators zu deinstallieren.
```

Führen Sie die folgenden Befehle der Reihe nach aus. Abhängig von Ihrer aktuellen Installation können einige dieser Befehle die Meldung „Objekt nicht gefunden“ zurückgeben. Diese Nachrichten können bedenkenlos ignoriert werden.

```
kubectl -n <NAMESPACE> delete agent agent-monitoring-netapp
kubectl delete crd agents.monitoring.netapp.com
kubectl -n <NAMESPACE> delete role agent-leader-election-role
kubectl delete clusterrole agent-manager-role agent-proxy-role agent-
metrics-reader <NAMESPACE>-agent-manager-role <NAMESPACE>-agent-proxy-role
<NAMESPACE>-cluster-role-privileged
kubectl delete clusterrolebinding agent-manager-rolebinding agent-proxy-
rolebinding agent-cluster-admin-rolebinding <NAMESPACE>-agent-manager-
rolebinding <NAMESPACE>-agent-proxy-rolebinding <NAMESPACE>-cluster-role-
binding-privileged
kubectl delete <NAMESPACE>-psp-nkmo
kubectl delete ns <NAMESPACE>
```

Wenn zuvor eine Sicherheitskontextbeschränkung erstellt wurde:

```
kubectl delete scc telegraf-hostaccess
```

Über Kube-State-Metrics

Der NetApp Kubernetes Monitoring Operator installiert seine eigenen Kube-State-Metriken, um Konflikte mit anderen Instanzen zu vermeiden.

Informationen zu Kube-State-Metrics finden Sie unter"diese Seite" .

Konfigurieren/Anpassen des Operators

Diese Abschnitte enthalten Informationen zum Anpassen Ihrer Operatorkonfiguration, zum Arbeiten mit Proxy, zum Verwenden eines benutzerdefinierten oder privaten Docker-Repositorys oder zum Arbeiten mit OpenShift.

Konfigurationsoptionen

Die am häufigsten geänderten Einstellungen können in der benutzerdefinierten Ressource *AgentConfiguration* konfiguriert werden. Sie können diese Ressource vor der Bereitstellung des Operators bearbeiten, indem Sie die Datei *operator-config.yaml* bearbeiten. Diese Datei enthält auskommentierte Beispiele für Einstellungen. Siehe die Liste der"Verfügbare Einstellungen" für die neueste Version des Operators.

Sie können diese Ressource auch bearbeiten, nachdem der Operator bereitgestellt wurde, indem Sie den folgenden Befehl verwenden:

```
 kubectl -n netapp-monitoring edit AgentConfiguration
Um festzustellen, ob Ihre bereitgestellte Version des Operators
AgentConfiguration unterstützt, führen Sie den folgenden Befehl aus:
```

```
 kubectl get crd agentconfigurations.monitoring.netapp.com
Wenn die Meldung „Fehler vom Server (Nicht gefunden)“ angezeigt wird, muss Ihr Operator aktualisiert werden, bevor Sie die Agentenkonfiguration verwenden können.
```

Konfigurieren der Proxy-Unterstützung

Es gibt zwei Stellen, an denen Sie einen Proxy auf Ihrem Mandanten verwenden können, um den Kubernetes Monitoring Operator zu installieren. Dabei kann es sich um dasselbe oder um separate Proxy-Systeme handeln:

- Proxy, der während der Ausführung des Installationscode-Snippets (mit „curl“) benötigt wird, um das System, auf dem das Snippet ausgeführt wird, mit Ihrer Data Infrastructure Insights -Umgebung zu verbinden
- Proxy, der vom Ziel-Kubernetes-Cluster zur Kommunikation mit Ihrer Data Infrastructure Insights -Umgebung benötigt wird

Wenn Sie für einen oder beide einen Proxy verwenden, müssen Sie zur Installation des Kubernetes Operating Monitor zunächst sicherstellen, dass Ihr Proxy so konfiguriert ist, dass eine gute Kommunikation mit Ihrer Data Infrastructure Insights Umgebung möglich ist. Wenn Sie über einen Proxy verfügen und von dem Server/der VM, von dem/der Sie den Operator installieren möchten, auf Data Infrastructure Insights zugreifen können, ist Ihr Proxy wahrscheinlich richtig konfiguriert.

Legen Sie für den Proxy, der zur Installation des Kubernetes Operating Monitor verwendet wird, vor der Installation des Operators die Umgebungsvariablen *http_proxy/https_proxy* fest. Für einige Proxy-Umgebungen müssen Sie möglicherweise auch die Umgebungsvariable *no_proxy* festlegen.

Um die Variable(n) festzulegen, führen Sie **vor** der Installation des Kubernetes Monitoring Operator die folgenden Schritte auf Ihrem System aus:

1. Legen Sie die Umgebungsvariable(n) *https_proxy* und/oder *http_proxy* für den aktuellen Benutzer fest:
   a. Wenn der einzurichtende Proxy keine Authentifizierung (Benutzername/Passwort) hat, führen Sie den folgenden Befehl aus:

```
 export https_proxy=<proxy_server>:<proxy_port>
.. Wenn der einzurichtende Proxy über eine Authentifizierung (Benutzername/Passwort) verfügt, führen Sie diesen Befehl aus:
```

```
export
http_proxy=<proxy_username>:<proxy_password>@<proxy_server>:<proxy_port>
```

Damit der für Ihren Kubernetes-Cluster verwendete Proxy mit Ihrer Data Infrastructure Insights -Umgebung kommunizieren kann, installieren Sie nach dem Lesen aller dieser Anweisungen den Kubernetes Monitoring Operator.

Konfigurieren Sie den Proxy-Abschnitt der AgentConfiguration in operator-config.yaml, bevor Sie den

Kubernetes Monitoring Operator bereitstellen.

```
agent:
  ...
  proxy:
    server: <server for proxy>
    port: <port for proxy>
    username: <username for proxy>
    password: <password for proxy>

    # In the noproxy section, enter a comma-separated list of
    # IP addresses and/or resolvable hostnames that should bypass
    # the proxy
    noproxy: <comma separated list>

    isTelegrafProxyEnabled: true
    isFluentbitProxyEnabled: <true or false> # true if Events Log enabled
    isCollectorsProxyEnabled: <true or false> # true if Network
Performance and Map enabled
    isAuProxyEnabled: <true or false> # true if AU enabled
  ...
...
```

Verwenden eines benutzerdefinierten oder privaten Docker-Repositorys

Standardmäßig ruft der Kubernetes Monitoring Operator Container-Images aus dem Data Infrastructure Insights Repository ab. Wenn Sie einen Kubernetes-Cluster als Ziel für die Überwachung verwenden und dieser Cluster so konfiguriert ist, dass er nur Container-Images aus einem benutzerdefinierten oder privaten Docker-Repository oder Container-Register abruft, müssen Sie den Zugriff auf die vom Kubernetes Monitoring Operator benötigten Container konfigurieren.

Führen Sie das „Image Pull Snippet“ aus der Installationskachel des NetApp Monitoring Operator aus. Mit diesem Befehl melden Sie sich beim Data Infrastructure Insights -Repository an, rufen alle Bildabhängigkeiten für den Operator ab und melden sich vom Data Infrastructure Insights -Repository ab. Geben Sie bei der entsprechenden Aufforderung das bereitgestellte temporäre Repository-Passwort ein. Dieser Befehl lädt alle vom Bediener verwendeten Bilder herunter, auch für optionale Funktionen. Unten sehen Sie, für welche Funktionen diese Bilder verwendet werden.

Kernoperator-Funktionalität und Kubernetes-Überwachung

- NetApp-Überwachung
- ci-kube-rbac-proxy
- ci-ksm
- ci-telegraf
- Distroless-Root-Benutzer

Ereignisprotokoll

- ci-fluent-bit
- ci-kubernetes-event-exporter

Netzwerkleistung und Karte

- ci-net-observer

Übertragen Sie das Operator-Docker-Image gemäß Ihren Unternehmensrichtlinien in Ihr privates/lokales/Unternehmens-Docker-Repository. Stellen Sie sicher, dass die Bild-Tags und Verzeichnispfade zu diesen Bildern in Ihrem Repository mit denen im Data Infrastructure Insights -Repository übereinstimmen.

Bearbeiten Sie die Bereitstellung des Überwachungsoperators in operator-deployment.yaml und ändern Sie alle Bildreferenzen, um Ihr privates Docker-Repository zu verwenden.

```
image: <docker repo of the enterprise/corp docker repo>/ci-kube-rbac-
proxy:<ci-kube-rbac-proxy version>
image: <docker repo of the enterprise/corp docker repo>/netapp-
monitoring:<version>
```

Bearbeiten Sie die AgentConfiguration in operator-config.yaml, um den neuen Speicherort des Docker-Repositorys widerzuspiegeln. Erstellen Sie ein neues imagePullSecret für Ihr privates Repository. Weitere Informationen finden Sie unter *https://kubernetes.io/docs/tasks/configure-pod-container/pull-image-private-registry/*

```
agent:
  ...
  # An optional docker registry where you want docker images to be pulled
from as compared to CI's docker registry
  # Please see documentation link here:
xref:{relative_path}task_config_telegraf_agent_k8s.html#using-a-custom-or-
private-docker-repository
  dockerRepo: your.docker.repo/long/path/to/test
  # Optional: A docker image pull secret that maybe needed for your
private docker registry
  dockerImagePullSecret: docker-secret-name
```

OpenShift-Anweisungen

Wenn Sie OpenShift 4.6 oder höher verwenden, müssen Sie die AgentConfiguration in *operator-config.yaml* bearbeiten, um die Einstellung *runPrivileged* zu aktivieren:

```
# Set runPrivileged to true SELinux is enabled on your kubernetes nodes
runPrivileged: true
```

Openshift implementiert möglicherweise eine zusätzliche Sicherheitsebene, die den Zugriff auf einige Kubernetes-Komponenten blockieren kann.

Toleranzen und Makel

Die DaemonSets *netapp-ci-telegraf-ds*, *netapp-ci-fluent-bit-ds* und *netapp-ci-net-observer-l4-ds* müssen auf jedem Knoten in Ihrem Cluster einen Pod planen, um Daten auf allen Knoten korrekt zu erfassen. Der Operator wurde so konfiguriert, dass er einige bekannte **Verunreinigungen** toleriert. Wenn Sie benutzerdefinierte Taints auf Ihren Knoten konfiguriert haben und dadurch verhindern, dass Pods auf jedem Knoten ausgeführt werden, können Sie eine **Toleranz** für diese Taints erstellen."in der *AgentConfiguration*" . Wenn Sie benutzerdefinierte Taints auf alle Knoten in Ihrem Cluster angewendet haben, müssen Sie der Operatorbereitstellung auch die erforderlichen Toleranzen hinzufügen, damit der Operator-Pod geplant und ausgeführt werden kann.

Mehr über Kubernetes erfahren"Makel und Duldungen" .

Zurück zum"* Seite „NetApp Kubernetes Monitoring Operator Installation“*"

Eine Anmerkung zu Geheimnissen

Um dem Kubernetes Monitoring Operator die Berechtigung zum Anzeigen von Geheimnissen im gesamten Cluster zu entziehen, löschen Sie vor der Installation die folgenden Ressourcen aus der Datei *operator-setup.yaml*:

```
 ClusterRole/netapp-ci<namespace>-agent-secret
 ClusterRoleBinding/netapp-ci<namespace>-agent-secret
```

Wenn es sich um ein Upgrade handelt, löschen Sie auch die Ressourcen aus Ihrem Cluster:

```
 kubectl delete ClusterRole/netapp-ci-<namespace>-agent-secret-clusterrole
 kubectl delete ClusterRoleBinding/netapp-ci-<namespace>-agent-secret-
clusterrolebinding
```

Wenn die Änderungsanalyse aktiviert ist, ändern Sie die Datei *AgentConfiguration* oder *operator-config.yaml*, um den Abschnitt zur Änderungsverwaltung zu kommentieren und *kindsToIgnoreFromWatch: '"secrets"'* in den Abschnitt zur Änderungsverwaltung aufzunehmen. Beachten Sie das Vorhandensein und die Position von einfachen und doppelten Anführungszeichen in dieser Zeile.

```
change-management:
  ...
  # # A comma separated list of kinds to ignore from watching from the
default set of kinds watched by the collector
  # # Each kind will have to be prefixed by its apigroup
  # # Example: '"networking.k8s.io.networkpolicies,batch.jobs",
"authorization.k8s.io.subjectaccessreviews"'
  kindsToIgnoreFromWatch: '"secrets"'
  ...
```

Überprüfen der Bildsignaturen des Kubernetes-Überwachungsoperators

Das Image für den Operator und alle zugehörigen Images, die er bereitstellt, sind von NetApp signiert. Sie können die Images vor der Installation manuell mit dem Cosign-Tool überprüfen oder einen Kubernetes-Zulassungscontroller konfigurieren. Weitere Einzelheiten finden Sie in der"Kubernetes-Dokumentation" .

Der öffentliche Schlüssel, der zum Überprüfen der Bildsignaturen verwendet wird, ist in der Installationskachel des Überwachungsoperators unter *Optional: Laden Sie die Operatorbilder in Ihr privates Repository hoch > Öffentlicher Schlüssel der Bildsignatur* verfügbar.

Um eine Bildsignatur manuell zu überprüfen, führen Sie die folgenden Schritte aus:

1. Kopieren und führen Sie das Image Pull Snippet aus
2. Kopieren Sie das Repository-Passwort und geben Sie es ein, wenn Sie dazu aufgefordert werden.
3. Speichern Sie den öffentlichen Schlüssel der Bildsignatur (dii-image-signing.pub im Beispiel).
4. Überprüfen Sie die Bilder mit Cosign. Siehe das folgende Beispiel für die Verwendung von Cosign

```
$ cosign verify --key dii-image-signing.pub --insecure-ignore-sct
--insecure-ignore-tlog <repository>/<image>:<tag>
Verification for <repository>/<image>:<tag> --
The following checks were performed on each of these signatures:
  - The cosign claims were validated
  - The signatures were verified against the specified public key
[{"critical":{"identity":{"docker-
reference":"<repository>/<image>"},"image":{"docker-manifest-
digest":"sha256:<hash>"},"type":"cosign container image
signature"},"optional":null}]
```

Fehlerbehebung

Wenn beim Einrichten des Kubernetes Monitoring Operators Probleme auftreten, können Sie Folgendes versuchen:

Problem:	Versuchen Sie Folgendes:
Ich sehe keinen Hyperlink/keine Verbindung zwischen meinem Kubernetes Persistent Volume und dem entsprechenden Back-End-Speichergerät. Mein Kubernetes Persistent Volume wird mit dem Hostnamen des Speicherservers konfiguriert.	Befolgen Sie die Schritte zum Deinstallieren des vorhandenen Telegraf-Agenten und installieren Sie anschließend den neuesten Telegraf-Agenten neu. Sie müssen Telegraf Version 2.0 oder höher verwenden und Ihr Kubernetes-Clusterspeicher muss aktiv von Data Infrastructure Insights überwacht werden.

Problem:	Versuchen Sie Folgendes:
Ich sehe in den Protokollen Meldungen, die den folgenden ähneln: E0901 15:21:39.962145 1 reflector.go:178] k8s.io/kube-state-metrics/internal/store/builder.go:352: *v1.MutatingWebhookConfiguration konnte nicht aufgelistet werden: Der Server konnte die angeforderte Ressource nicht finden. E0901 15:21:43.168161 1 reflector.go:178] k8s.io/kube-state-metrics/internal/store/builder.go:352: *v1.Lease konnte nicht aufgelistet werden: Der Server konnte die angeforderte Ressource nicht finden (get leases.coordination.k8s.io) usw.	Diese Meldungen können auftreten, wenn Sie kube-state-metrics Version 2.0.0 oder höher mit Kubernetes-Versionen unter 1.20 ausführen. So erhalten Sie die Kubernetes-Version: *kubectl version* So erhalten Sie die kube-state-metrics-Version: *kubectl get deploy/kube-state-metrics -o jsonpath='{..image}'* Um diese Meldungen zu verhindern, können Benutzer ihre kube-state-metrics-Bereitstellung ändern, um die folgenden Leases zu deaktivieren: *mutatingwebhookconfigurations validatingwebhookconfigurations volumeattachments resources* Genauer gesagt können sie das folgende CLI-Argument verwenden: resources=certificatesigningrequests,configmaps,cronjobs,daemonsets, deployments,endpoints,horizontalpodautoscalers,ingresses,jobs,limitranges, namespaces,networkpolicies,nodes,persistentvolumeclaims,persistentvolumes, poddisruptionbudgets,pods,replicasets,replicationcontrollers,resourcequotas, secrets,services,statefulsets,storageclasses Die Standardressourcenliste ist: „Zertifikatsignaturanforderungen, Konfigurationszuordnungen, Cronjobs, Daemonsets, Bereitstellungen, Endpunkte, horizontale Pod-Autoskalierer, Ingresses, Jobs, Leases, Grenzwertbereiche, mutierende Webhookkonfigurationen, Namespaces, Netzwerkrichtlinien, Knoten, persistente Volumeansprüche, persistente Volumes, Pod-Unterbrechungsbudgets, Pods, Replikatsets, Replikationscontroller, Ressourcenkontingente, Geheimnisse, Dienste, Statefulsets, Speicherklassen, validierende Webhookkonfigurationen, Volumeanhänge“

Problem:	Versuchen Sie Folgendes:
Ich sehe Fehlermeldungen von Telegraf, die den folgenden ähneln, aber Telegraf wird gestartet und ausgeführt: 11. Okt. 14:23:41 ip-172-31-39-47 systemd[1]: Der Plugin-gesteuerte Server-Agent zum Melden von Metriken in InfluxDB wurde gestartet. 11. Okt. 14:23:41 ip-172-31-39-47 telegraf[1827]: time="2021-10-11T14:23:41Z" level=error msg="Cache-Verzeichnis konnte nicht erstellt werden. /etc/telegraf/.cache/snowflake, err: mkdir /etc/telegraf/.ca che: Zugriff verweigert. Ignoriert\n" func="gosnowflake.(*defaultLogger).Errorf" file="log.go:120" 11. Okt. 14:23:41 ip-172-31-39-47 telegraf[1827]: time="2021-10-11T14:23:41Z" level=error msg="Öffnen fehlgeschlagen. Ignoriert. Öffnen Sie /etc/telegraf/.cache/snowflake/ocsp_response_cache.json: keine solche Datei oder kein solches Verzeichnis\n" func="gosnowflake.(*defaultLogger).Errorf" file="log.go:120" 11. Okt. 14:23:41 ip-172-31-39-47 telegraf[1827]: 2021-10-11T14:23:41Z I! Telegraf 1.19.3 wird gestartet	Dies ist ein bekanntes Problem. Siehe"Dieser GitHub-Artikel" für weitere Details. Solange Telegraf läuft, können Benutzer diese Fehlermeldungen ignorieren.
Auf Kubernetes melden meine Telegraf-Pods den folgenden Fehler: „Fehler beim Verarbeiten der Mountstats-Informationen: Mountstats-Datei konnte nicht geöffnet werden: /hostfs/proc/1/mountstats, Fehler: Öffnen von /hostfs/proc/1/mountstats: Berechtigung verweigert“	Wenn SELinux aktiviert ist und erzwungen wird, verhindert es wahrscheinlich, dass die Telegraf-Pods auf die Datei /proc/1/mountstats auf dem Kubernetes-Knoten zugreifen können. Um diese Einschränkung zu umgehen, bearbeiten Sie die Agentenkonfiguration und aktivieren Sie die Einstellung „runPrivileged“. Weitere Einzelheiten finden Sie in den OpenShift-Anweisungen.
Auf Kubernetes meldet mein Telegraf ReplicaSet-Pod den folgenden Fehler: [inputs.prometheus] Fehler im Plugin: Schlüsselpaar /etc/kubernetes/pki/etcd/server.crt konnte nicht geladen werden:/etc/kubernetes/pki/etcd/server.key: öffne /etc/kubernetes/pki/etcd/server.crt: keine solche Datei oder kein solches Verzeichnis	Der Telegraf ReplicaSet-Pod soll auf einem Knoten ausgeführt werden, der als Master oder für etcd bestimmt ist. Wenn der ReplicaSet-Pod auf einem dieser Knoten nicht ausgeführt wird, werden diese Fehler angezeigt. Überprüfen Sie, ob Ihre Master-/etcd-Knoten Verunreinigungen aufweisen. Wenn dies der Fall ist, fügen Sie die erforderlichen Toleranzen zum Telegraf ReplicaSet, telegraf-rs, hinzu. Bearbeiten Sie beispielsweise das ReplicaSet … kubectl edit rs telegraf-rs … und fügen Sie der Spezifikation die entsprechenden Toleranzen hinzu. Starten Sie dann den ReplicaSet-Pod neu.

Problem:	Versuchen Sie Folgendes:
Ich habe eine PSP/PSA-Umgebung. Betrifft dies meinen Überwachungsbetreiber?	Wenn Ihr Kubernetes-Cluster mit Pod Security Policy (PSP) oder Pod Security Admission (PSA) ausgeführt wird, müssen Sie auf den neuesten Kubernetes Monitoring Operator aktualisieren. Befolgen Sie diese Schritte, um auf den aktuellen Operator mit Unterstützung für PSP/PSA zu aktualisieren: 1. Deinstallieren der vorherige Überwachungsoperator: kubectl delete agent agent-monitoring-netapp -n netapp-monitoring kubectl delete ns netapp-monitoring kubectl delete crd agents.monitoring.netapp.com kubectl delete clusterrole agent-manager-role agent-proxy-role agent-metrics-reader kubectl delete clusterrolebinding agent-manager-rolebinding agent-proxy-rolebinding agent-cluster-admin-rolebinding 2. Installieren die neueste Version des Überwachungsoperators.
Beim Versuch, den Operator bereitzustellen, sind mir Probleme begegnet, und ich verwende PSP/PSA.	1. Bearbeiten Sie den Agenten mit dem folgenden Befehl: kubectl -n <name-space> edit agent 2. Markieren Sie „security-policy-enabled“ als „false“. Dadurch werden die Pod-Sicherheitsrichtlinien und die Pod-Sicherheitszulassung deaktiviert und dem Operator die Bereitstellung ermöglicht. Bestätigen Sie mit den folgenden Befehlen: kubectl get psp (sollte anzeigen, dass die Pod-Sicherheitsrichtlinie entfernt wurde) kubectl get all -n <namespace>
grep -i psp (sollte anzeigen, dass nichts gefunden wurde)	„ImagePullBackoff“-Fehler aufgetreten
Diese Fehler können auftreten, wenn Sie über ein benutzerdefiniertes oder privates Docker-Repository verfügen und den Kubernetes Monitoring Operator noch nicht so konfiguriert haben, dass es ordnungsgemäß erkannt wird. Mehr lesen Informationen zur Konfiguration für benutzerdefinierte/private Repos.	Ich habe ein Problem mit der Bereitstellung meines Überwachungsoperators und die aktuelle Dokumentation hilft mir nicht bei der Lösung.

Problem:	Versuchen Sie Folgendes:

Erfassen oder notieren Sie die Ausgabe der folgenden Befehle und wenden Sie sich an das technische Supportteam.
 	
`kubectl -n netapp-monitoring get all`
`kubectl -n netapp-monitoring describe all`
`kubectl -n netapp-monitoring logs <monitoring-operator-pod> --all -containers=true`
`kubectl -n netapp-monitoring logs <telegraf-pod> --all -containers=true`
	Net-Observer-Pods (Workload Map) im Operator-Namespace befinden sich in CrashLoopBackOff

Diese Pods entsprechen dem Workload Map-Datensammler für die Netzwerkbeobachtung. Versuchen Sie Folgendes: • Überprüfen Sie die Protokolle eines der Pods, um die Mindestkernelversion zu bestätigen. Beispiel: ---- {"ci-tenant-id":"Ihre Mandanten-ID","collector-cluster":"Ihr K8S-Clustername","environment":"prod","level":"error","msg":"Validierung fehlgeschlagen. Grund: Kernelversion 3.10.0 ist niedriger als die Mindestkernelversion 4.18.0","time":"2022-11-09T08:23:08Z"} ---- • Net-Observer-Pods erfordern mindestens die Linux-Kernelversion 4.18.0. Überprüfen Sie die Kernelversion mit dem Befehl „uname -r“ und stellen Sie sicher, dass sie >= 4.18.0 ist	Pods werden im Operator-Namespace ausgeführt (Standard: Netapp-Monitoring), aber in der Benutzeroberfläche werden keine Daten für die Workload-Map oder Kubernetes-Metriken in Abfragen angezeigt.
Überprüfen Sie die Zeiteinstellung auf den Knoten des K8S-Clusters. Für eine genaue Prüfung und Datenberichterstattung wird dringend empfohlen, die Zeit auf dem Agent-Computer mithilfe des Network Time Protocol (NTP) oder Simple Network Time Protocol (SNTP) zu synchronisieren.	Einige der Net-Observer-Pods im Operator-Namespace befinden sich im Status „Ausstehend“
Net-Observer ist ein DaemonSet und führt in jedem Knoten des K8S-Clusters einen Pod aus. • Beachten Sie den Pod, der sich im Status „Ausstehend“ befindet, und prüfen Sie, ob ein Ressourcenproblem für die CPU oder den Speicher vorliegt. Stellen Sie sicher, dass im Knoten genügend Speicher und CPU verfügbar sind.	Unmittelbar nach der Installation des Kubernetes Monitoring Operator wird mir in meinen Protokollen Folgendes angezeigt: [inputs.prometheus] Fehler im Plug-In: Fehler beim Senden der HTTP-Anforderung an http://kube-state-metrics.<namespace>.svc.cluster.local:8080/metrics: Get http://kube-state-metrics.<namespace>.svc.cluster.local:8080/metrics: dial tcp: lookup kube-state-metrics.<namespace>.svc.cluster.local: no such host

Problem:	Versuchen Sie Folgendes:
Diese Meldung wird normalerweise nur angezeigt, wenn ein neuer Operator installiert wird und der *telegraf-rs*-Pod vor dem *ksm*-Pod aktiv ist. Diese Nachrichten sollten aufhören, sobald alle Pods ausgeführt werden.	Ich sehe keine erfassten Metriken für die in meinem Cluster vorhandenen Kubernetes-CronJobs.
Überprüfen Sie Ihre Kubernetes-Version (d. h. `kubectl version`). Wenn es sich um v1.20.x oder niedriger handelt, ist dies eine erwartete Einschränkung. Die mit dem Kubernetes Monitoring Operator bereitgestellte Version von kube-state-metrics unterstützt nur v1.CronJob. Bei Kubernetes 1.20.x und darunter befindet sich die CronJob-Ressource unter v1beta.CronJob. Aus diesem Grund kann kube-state-metrics die CronJob-Ressource nicht finden.	Nach der Installation des Operators treten die Telegraf-DS-Pods in CrashLoopBackOff ein und die Pod-Protokolle zeigen „su: Authentifizierungsfehler“ an.
Bearbeiten Sie den Telegraf-Abschnitt in *AgentConfiguration* und setzen Sie *dockerMetricCollectionEnabled* auf „false“. Weitere Einzelheiten finden Sie in der Betriebsanleitung des Betreibers."Konfigurationsoptionen" . … Spezifikation: … Telegraf: … - Name: Docker-Ausführungsmodus: - DaemonSet-Ersetzungen: - Schlüssel: DOCKER_UNIX_SOCK_PLACEHOLDER-Wert: unix:///run/docker.sock … …	In meinen Telegraf-Protokollen werden immer wieder Fehlermeldungen angezeigt, die den folgenden ähneln: E! [Agent] Fehler beim Schreiben in outputs.http: Post "https://<tenant_url>/rest/v1/lake/ingest/influxdb": Kontextfrist überschritten (Client.Timeout beim Warten auf Header überschritten)
Bearbeiten Sie den Telegraf-Abschnitt in *AgentConfiguration* und erhöhen Sie *outputTimeout* auf 10 s. Weitere Einzelheiten finden Sie in der Betriebsanleitung des Betreibers."Konfigurationsoptionen" .	Mir fehlen *involvedobject*-Daten für einige Ereignisprotokolle.
Stellen Sie sicher, dass Sie die Schritte in der"Berechtigungen" Abschnitt oben.	Warum werden zwei Überwachungsoperator-Pods ausgeführt, einer mit dem Namen netapp-ci-monitoring-operator-<pod> und der andere mit dem Namen monitoring-operator-<pod>?
Ab dem 12. Oktober 2023 hat Data Infrastructure Insights den Operator überarbeitet, um unseren Benutzern einen besseren Service zu bieten. Damit diese Änderungen vollständig übernommen werden können, müssen SieEntfernen Sie den alten Operator Undinstallieren Sie die neue .	Meine Kubernetes-Ereignisse wurden unerwartet nicht mehr an Data Infrastructure Insights gemeldet.
Rufen Sie den Namen des Event-Exporter-Pods ab: `` `kubectl -n netapp-monitoring get pods ``	grep event-exporter

Problem:	Versuchen Sie Folgendes:
awk '{print $1}'	sed 's/event-exporter./event-exporter/'` Es sollte entweder „netapp-ci-event-exporter“ oder „event-exporter“ sein. Bearbeiten Sie als Nächstes den Überwachungsagenten `kubectl -n netapp-monitoring edit agent` und legen Sie den Wert für LOG_FILE so fest, dass er den entsprechenden Event-Exporter-Pod-Namen widerspiegelt, der im vorherigen Schritt gefunden wurde. Genauer gesagt sollte LOG_FILE entweder auf "/var/log/containers/netapp-ci-event-exporter.log" oder "/var/log/containers/event-exporter*.log" gesetzt werden. …. fluent-bit: … - name: event-exporter-ci substitutions: - key: LOG_FILE values: - /var/log/containers/netapp-ci-event-exporter*.log … …. Alternativ kann man auchdeinstallieren UndNeuinstallation der Agent.
Ich sehe, dass vom Kubernetes Monitoring Operator bereitgestellte Pods aufgrund unzureichender Ressourcen abstürzen.	Siehe den Kubernetes Monitoring Operator"Konfigurationsoptionen" um die CPU- und/oder Speichergrenzen nach Bedarf zu erhöhen.
Ein fehlendes Image oder eine ungültige Konfiguration führte dazu, dass die netapp-ci-kube-state-metrics-Pods nicht gestartet werden konnten oder nicht bereit waren. Jetzt steckt das StatefulSet fest und Konfigurationsänderungen werden nicht auf die Netapp-CI-Kube-State-Metrics-Pods angewendet.	Das StatefulSet ist in einem"gebrochen" Zustand. Nachdem Sie alle Konfigurationsprobleme behoben haben, führen Sie einen Bounce der Netapp-CI-Kube-State-Metrics-Pods durch.
netapp-ci-kube-state-metrics-Pods können nach der Ausführung eines Kubernetes Operator-Upgrades nicht gestartet werden und lösen ErrImagePull aus (das Abrufen des Images schlägt fehl).	Versuchen Sie, die Pods manuell zurückzusetzen.
Bei der Protokollanalyse werden für meinen Kubernetes-Cluster Meldungen vom Typ „Ereignis verworfen, da es älter ist als maxEventAgeSeconds“ beobachtet.	Ändern Sie die Operator-Agentenkonfiguration und erhöhen Sie *event-exporter-maxEventAgeSeconds* (z. B. auf 60 s), *event-exporter-kubeQPS* (z. B. auf 100) und *event-exporter-kubeBurst* (z. B. auf 500). Weitere Einzelheiten zu diesen Konfigurationsoptionen finden Sie im"Konfigurationsoptionen" Seite.

Problem:	Versuchen Sie Folgendes:
Telegraf warnt vor unzureichendem sperrbaren Speicher oder stürzt ab.	Versuchen Sie, das Limit des sperrbaren Speichers für Telegraf im zugrunde liegenden Betriebssystem/Knoten zu erhöhen. Wenn eine Erhöhung des Limits keine Option ist, ändern Sie die NKMO-Agentenkonfiguration und setzen Sie *unprotected* auf *true*. Dadurch wird Telegraf angewiesen, keinen Versuch zu unternehmen, gesperrte Speicherseiten zu reservieren. Dies kann zwar ein Sicherheitsrisiko darstellen, da entschlüsselte Geheimnisse möglicherweise auf die Festplatte ausgelagert werden, ermöglicht jedoch die Ausführung in Umgebungen, in denen die Reservierung gesperrten Speichers nicht möglich ist. Weitere Informationen zu den *ungeschützten* Konfigurationsoptionen finden Sie im"Konfigurationsoptionen" Seite.
Ich sehe Warnmeldungen von Telegraf, die etwa wie folgt aussehen: *W! [inputs.diskio] Der Datenträgername für „vdc“ konnte nicht ermittelt werden: Fehler beim Lesen von /dev/vdc: keine solche Datei oder kein solches Verzeichnis*	Für den Kubernetes Monitoring Operator sind diese Warnmeldungen harmlos und können ignoriert werden. Alternativ können Sie den Abschnitt „Telegraf“ in der AgentConfiguration bearbeiten und *runDsPrivileged* auf „true“ setzen. Weitere Einzelheiten finden Sie im"Konfigurationsoptionen des Betreibers" .

Problem:	Versuchen Sie Folgendes:

Mein Fluent-Bit-Pod schlägt mit den folgenden Fehlern fehl: [2024/10/16 14:16:23] [Fehler] [/src/fluent-bit/plugins/in_tail/tail_fs_inotify.c:360 errno=24] Zu viele offene Dateien [2024/10/16 14:16:23] [Fehler] Initialisierung der Eingabe tail.0 fehlgeschlagen [2024/10/16 14:16:23] [Fehler] [Engine] Initialisierung der Eingabe fehlgeschlagen	Versuchen Sie, Ihre *fsnotify*-Einstellungen in Ihrem Cluster zu ändern:
	`sudo sysctl fs.inotify.max_user_instances (take note of setting)`
	`sudo sysctl fs.inotify.max_user_instances=<something larger than current setting>`
	`sudo sysctl fs.inotify.max_user_watches (take note of setting)`
	`sudo sysctl fs.inotify.max_user_watches=<something larger than current setting>`
	Starten Sie Fluent-bit neu.
	Hinweis: Um diese Einstellungen auch nach einem Neustart des Knotens dauerhaft zu halten, müssen Sie die folgenden Zeilen in */etc/sysctl.conf* einfügen.
	`fs.inotify.max_user_instances=<something larger than current setting>`
	`fs.inotify.max_user_watches=<something larger than current setting>`

Problem:	Versuchen Sie Folgendes:
Die Telegraf DS-Pods melden Fehler im Zusammenhang mit dem Kubernetes-Eingabe-Plugin, das keine HTTP-Anfragen stellen kann, da das TLS-Zertifikat nicht validiert werden kann. Zum Beispiel: E! [inputs.kubernetes] Fehler im Plugin: Fehler beim Senden einer HTTP-Anfrage an"<a href="https://<kubelet_IP>:10250/stats/summary": " class="bare">https://<kubelet_IP>:10250/stats/summary": Erhalten"<a href="https://<kubelet_IP>:10250/stats/summary": " class="bare">https://<kubelet_IP>:10250/stats/summary": tls: Zertifikat konnte nicht überprüft werden: x509: Zertifikat für <kubelet_IP> kann nicht validiert werden, da es keine IP-SANs enthält	Dies tritt auf, wenn das Kubelet selbstsignierte Zertifikate verwendet und/oder das angegebene Zertifikat die <kubelet_IP> nicht in der Liste „Subject Alternative Name“ des Zertifikats enthält. Um dieses Problem zu lösen, kann der Benutzer die"Agentenkonfiguration" , und setzen Sie *telegraf:insecureK8sSkipVerify* auf *true*. Dadurch wird das Telegraf-Eingabe-Plugin so konfiguriert, dass die Überprüfung übersprungen wird. Alternativ kann der Benutzer das Kubelet konfigurieren für"serverTLSBootstrap" , wodurch eine Zertifikatsanforderung von der API „certificates.k8s.io“ ausgelöst wird.

Weitere Informationen finden Sie in der"Support" Seite oder in der"Datensammler-Supportmatrix" .

Konfigurationsoptionen für den Kubernetes-Überwachungsoperator

Der "Kubernetes-Überwachungsoperator" bietet umfangreiche Anpassungsmöglichkeiten über die AgentConfiguration-Datei. Sie können Ressourcenlimits, Erfassungsintervalle, Proxy-Einstellungen, Toleranzen und komponentenspezifische Einstellungen konfigurieren, um die Überwachung Ihrer Kubernetes-Umgebung zu optimieren. Nutzen Sie diese Optionen, um Telegraf, Kube-State-Metrics, die Protokollerfassung, die Workload-Zuordnung, das Änderungsmanagement und andere Überwachungskomponenten anzupassen.

In der folgenden Tabelle sind die möglichen Optionen für die Datei *AgentConfiguration* aufgeführt:

Komponente	Option	Beschreibung
Agent		Konfigurationsoptionen, die allen Komponenten gemeinsam sind, die der Betreiber installieren kann. Diese können als „globale“ Optionen betrachtet werden.
	dockerRepo	Eine DockerRepo-Überschreibung, um Bilder aus den privaten Docker-Repositorys des Kunden statt aus dem Docker-Repository von Data Infrastructure Insights abzurufen. Standardmäßig wird das Docker-Repository von Data Infrastructure Insights verwendet.
	dockerImagePullSecret	Optional: Ein Geheimnis für das private Repository des Kunden.

Komponente	Option	Beschreibung
	Clustername	Freitextfeld, das einen Cluster über alle Kundencluster hinweg eindeutig identifiziert. Dies sollte innerhalb eines Data Infrastructure Insights Mandanten eindeutig sein. Standardmäßig wird der vom Kunden in der Benutzeroberfläche im Feld „Clustername“ eingegebene Wert verwendet.
	Proxy-Format: Proxy: Server: Port: Benutzername: Passwort: noProxy: isTelegrafProxyEnabled: isAuProxyEnabled: isFluentbitProxyEnabled: isCollectorProxyEnabled:	Optional zum Festlegen des Proxys. Dies ist in der Regel der Unternehmensbevollmächtigte des Kunden.
Telegraf		Konfigurationsoptionen, die die Telegraf-Installation des Operators anpassen können
	Sammlungsintervall	Intervall für die Messwerterfassung in Sekunden (max. 60 s)
	dsCpuLimit	CPU-Limit für Telegraf DS
	dsMemLimit	Speicherlimit für Telegraf DS
	dsCpuRequest	CPU-Anforderung für Telegraf DS
	dsMemRequest	Speicheranforderung für Telegraf DS
	rsCpuLimit	CPU-Limit für Telegraf RS
	rsMemLimit	Speicherlimit für Telegraf RS
	rsCpuRequest	CPU-Anforderung für Telegraf RS
	rsMemRequest	Speicheranforderung für Telegraf RS
	runPrivileged	Führen Sie den *telegraf-mountstats-poller*-Container des Telegraf-DaemonSets im privilegierten Modus aus. Setzen Sie dies auf „true“, wenn SELinux auf Ihren Kubernetes-Knoten aktiviert ist.
	runDsPrivileged	Setzen Sie runDsPrivileged auf „true“, um den Telegraf-Container des Telegraf-DaemonSets im privilegierten Modus auszuführen.
	Batchgröße	Sehen"Telegraf-Konfigurationsdokumentation"
	Pufferlimit	Sehen"Telegraf-Konfigurationsdokumentation"
	Rundenintervall	Sehen"Telegraf-Konfigurationsdokumentation"
	SammlungJitter	Sehen"Telegraf-Konfigurationsdokumentation"
	Präzision	Sehen"Telegraf-Konfigurationsdokumentation"
	Spülintervall	Sehen"Telegraf-Konfigurationsdokumentation"
	FlushJitter	Sehen"Telegraf-Konfigurationsdokumentation"

Komponente	Option	Beschreibung
	Ausgabe-Timeout	Sehen"Telegraf-Konfigurationsdokumentation"
	dsToleranzen	zusätzliche Toleranzen für Telegraf-DS.
	rsToleranzen	zusätzliche Toleranzen für Telegraf-RS.
	skipProcessorsAfterAggregators	Sehen"Telegraf-Konfigurationsdokumentation"
	ungeschützt	Sehen Sie dies "bekanntes Telegraf-Problem" . Die Einstellung *unprotected* weist den Kubernetes Monitoring Operator an, Telegraf mit dem `--unprotected` Flagge.
	insecureK8sSkipVerify	Wenn Telegraf das Zertifikat aufgrund fehlender IP-SANs nicht überprüfen kann, versuchen Sie, die Überprüfung zu überspringen
Kube-State-Metriken		Konfigurationsoptionen, mit denen die Installation der Kube-Statusmetriken des Operators angepasst werden kann
	CPU-Limit	CPU-Limit für die Bereitstellung von Kube-State-Metrics
	memLimit	Speicherlimit für die Bereitstellung von Kube-State-Metrics
	CPU-Anforderung	CPU-Anforderung für die Bereitstellung von Kube-Statusmetriken
	memRequest	Mem-Anforderung für die Bereitstellung von Kube-Statusmetriken
	Ressourcen	eine durch Kommas getrennte Liste der zu erfassenden Ressourcen. Beispiel: Cronjobs, Daemonsets, Bereitstellungen, Ingresses, Jobs, Namespaces, Knoten, persistente Volumeansprüche, persistente Volumes, Pods, Replikatsets, Ressourcenkontingente, Dienste, Statefulsets
	Duldungen	Zusätzliche Toleranzen für Kube-State-Metrics.
	Etiketten	eine durch Kommas getrennte Liste von Ressourcen, für die kube-state-metrics Labels erfassen soll Beispiel: cronjobs=[*],daemonsets=[*],deployments=[*],ingresses=[*],jobs=[*],namespaces=[*],nodes=[*],persistentvolumeclaims=[*],persistentvolumes=[*],pods=[*],replicasets=[*],resourcequotas=[*],services=[*],statefulsets=[*]
Protokolle		Konfigurationsoptionen, mit denen die Protokollerfassung und Installation des Operators angepasst werden kann
	readFromHead	true/false, soll Fluent Bit das Protokoll vom Kopf lesen
	Time-out	Timeout in Sekunden

Komponente	Option	Beschreibung
	dnsMode	TCP/UDP, Modus für DNS
	Fluent-Bit-Toleranzen	zusätzliche Toleranzen für fluent-bit-ds.
	Ereignis-Exporter-Toleranzen	zusätzliche Toleranzen für den Ereignisexporteur.
	event-exporter-maxEventAgeSeconds	maximales Ereignisalter des Ereignisexporteurs. Sehen https://github.com/jkroepke/resmoio-kubernetes-event-exporter
	Fluent-Bit-ContainerLogPath	Standardmäßig mountet das Fluentbit DaemonSet die Hostpfade /var/log und /var/lib/docker/containers, um auf die Kubernetes-Containerprotokolle zuzugreifen/sie zu lesen. Wenn Kubernetes so konfiguriert wurde, dass Containerprotokolle an einem nicht standardmäßigen Speicherort abgelegt werden, verwenden Sie diese Option, um das Fluentbit-DaemonSet so zu ändern, dass der nicht standardmäßige Pfad bereitgestellt wird.
Arbeitslastkarte		Konfigurationsoptionen, mit denen die Workload-Map-Erfassung und -Installation des Operators angepasst werden kann.
	CPU-Limit	CPU-Limit für Net Observer DS
	memLimit	Speicherlimit für Net Observer DS
	CPU-Anforderung	CPU-Anforderung für Net Observer DS
	memRequest	Mem-Anforderung für Net Observer DS
	metricAggregationInterval	Metrikaggregationsintervall in Sekunden
	bpfPollIntervall	BPF-Polling-Intervall in Sekunden
	enableDNSLookup	true/false, DNS-Suche aktivieren
	l4-Toleranzen	net-observer-l4-ds zusätzliche Toleranzen.
	runPrivileged	true/false – Setzen Sie runPrivileged auf „true“, wenn SELinux auf Ihren Kubernetes-Knoten aktiviert ist.
Änderungsmanagement		Konfigurationsoptionen für Kubernetes Change Management und Analyse
	CPU-Limit	CPU-Limit für change-observer-watch-rs
	memLimit	Mem-Limit für Change-Observer-Watch-RS
	CPU-Anforderung	CPU-Anforderung für change-observer-watch-rs
	memRequest	Mem-Anforderung für Change-Observer-Watch-RS
	ArbeitslastFehlerdeklarationsintervallSekunden	Intervall in Sekunden, nach dem eine nicht erfolgreiche Bereitstellung einer Arbeitslast als fehlgeschlagen markiert wird
	ArbeitslastDeployAggrIntervalSeconds	Häufigkeit, mit der Workloadbereitstellungen kombiniert und gesendet werden (in Sekunden)

Komponente	Option	Beschreibung
	nonWorkloadDeployAggrIntervalSeconds	Häufigkeit, mit der Nicht-Workload-Bereitstellungen kombiniert und gesendet werden (in Sekunden)
	termsToRedact	Eine Reihe von regulären Ausdrücken, die in Umgebungsnamen und Datenzuordnungen verwendet werden und deren Wert redigiert wird. Beispielbegriffe: „pwd“, „Passwort“, „Token“, „API-Schlüssel“, „API-Schlüssel“, „JWT“.
	zusätzlicheKindeZuBeobachten	Eine durch Kommas getrennte Liste zusätzlicher Arten, die aus dem Standardsatz der vom Collector überwachten Arten beobachtet werden sollen
	Arten, die von der Überwachung ignoriert werden sollen	Eine durch Kommas getrennte Liste von Arten, die aus dem vom Collector überwachten Standardsatz von Arten ignoriert werden sollen
	logRecordAggrIntervalSeconds	Häufigkeit, mit der Protokolldatensätze vom Collector an CI gesendet werden
	Uhrentoleranzen	change-observer-watch-ds zusätzliche Toleranzen. Nur abgekürztes einzeiliges Format. Beispiel: „{key: taint1, operator: Exists, effect: NoSchedule},{key: taint2, operator: Exists, effect: NoExecute}“

Beispieldatei für AgentConfiguration

Unten sehen Sie ein Beispiel für eine *AgentConfiguration*-Datei.

```
apiVersion: monitoring.netapp.com/v1alpha1
kind: AgentConfiguration
metadata:
  name: netapp-ci-monitoring-configuration
  namespace: "netapp-monitoring"
  labels:
    installed-by: nkmo-netapp-monitoring

spec:
  # # You can modify the following fields to configure the operator.
  # # Optional settings are commented out and include default values for
reference
  # #   To update them, uncomment the line, change the value, and apply
the updated AgentConfiguration.
  agent:
    # # [Required Field] A uniquely identifiable user-friendly
clustername.
    # # clusterName must be unique across all clusters in your Data
Infrastructure Insights environment.
    clusterName: "my_cluster"
```

```
    # # Proxy settings. The proxy that the operator should use to send
metrics to Data Infrastructure Insights.
    # # Please see documentation here: https://docs.netapp.com/us-
en/cloudinsights/task_config_telegraf_agent_k8s.html#configuring-proxy-
support
    # proxy:
    #   server:
    #   port:
    #   noproxy:
    #   username:
    #   password:
    #   isTelegrafProxyEnabled:
    #   isFluentbitProxyEnabled:
    #   isCollectorsProxyEnabled:

    # # [Required Field] By default, the operator uses the CI repository.
    # # To use a private repository, change this field to your repository
name.
    # # Please see documentation here: https://docs.netapp.com/us-
en/cloudinsights/task_config_telegraf_agent_k8s.html#using-a-custom-or-
private-docker-repository
    dockerRepo: 'docker.c01.cloudinsights.netapp.com'
    # # [Required Field] The name of the imagePullSecret for dockerRepo.
    # # If you are using a private repository, change this field from
'netapp-ci-docker' to the name of your secret.
    dockerImagePullSecret: 'netapp-ci-docker'

    # # Allow the operator to automatically rotate its ApiKey before
expiration.
    # tokenRotationEnabled: 'true'
    # # Number of days before expiration that the ApiKey should be
rotated. This must be less than the total ApiKey duration.
    # tokenRotationThresholdDays: '30'

  telegraf:
    # # Settings to fine-tune metrics data collection. Telegraf config
names are included in parenthesis.
    # # See
https://github.com/influxdata/telegraf/blob/master/docs/CONFIGURATION.md#a
gent

    # # The default time telegraf will wait between inputs for all plugins
(interval). Max=60
    # collectionInterval: '60s'
    # # Maximum number of records per output that telegraf will write in
one batch (metric_batch_size).
```

```
    # batchSize: '10000'
    # # Maximum number of records per output that telegraf will cache
pending a successful write (metric_buffer_limit).
    # bufferLimit: '150000'
    # # Collect metrics on multiples of interval (round_interval).
    # roundInterval: 'true'
    # # Each plugin waits a random amount of time between the scheduled
collection time and that time + collection_jitter before collecting inputs
(collection_jitter).
    # collectionJitter: '0s'
    # # Collected metrics are rounded to the precision specified. When set
to "0s" precision will be set by the units specified by interval
(precision).
    # precision: '0s'
    # # Time telegraf will wait between writing outputs (flush_interval).
Max=collectionInterval
    # flushInterval: '60s'
    # # Each output waits a random amount of time between the scheduled
write time and that time + flush_jitter before writing outputs
(flush_jitter).
    # flushJitter: '0s'
    # # Timeout for writing to outputs (timeout).
    # outputTimeout: '5s'

    # # telegraf-ds CPU/Mem limits and requests.
    # # See https://kubernetes.io/docs/concepts/configuration/manage-
resources-containers/
    # dsCpuLimit: '750m'
    # dsMemLimit: '800Mi'
    # dsCpuRequest: '100m'
    # dsMemRequest: '500Mi'

    # # telegraf-rs CPU/Mem limits and requests.
    # rsCpuLimit: '3'
    # rsMemLimit: '4Gi'
    # rsCpuRequest: '100m'
    # rsMemRequest: '500Mi'

    # # Skip second run of processors after aggregators
    # skipProcessorsAfterAggregators: 'true'

    # # telegraf additional tolerations. Use the following abbreviated
single line format only.
    # # Inspect telegraf-rs/-ds to view tolerations which are always
present.
    # # Example: '{key: taint1, operator: Exists, effect:
```

```
NoSchedule},{key: taint2, operator: Exists, effect: NoExecute}'
    # dsTolerations: ''
    # rsTolerations: ''


    # If telegraf warns of insufficient lockable memory, try increasing
the limit of lockable memory for Telegraf in the underlying operating
system/node.  If increasing the limit is not an option, set this to true
to instruct Telegraf to not attempt to reserve locked memory pages.  While
this might pose a security risk as decrypted secrets might be swapped out
to disk, it allows for execution in environments where reserving locked
memory is not possible.
    # unprotected: 'false'

    # # Run the telegraf DaemonSet's telegraf-mountstats-poller container
in privileged mode.  Set runPrivileged to true if SELinux is enabled on
your Kubernetes nodes.
    # runPrivileged: '{{
.Values.telegraf_installer.kubernetes.privileged_mode }}'

    # # Set runDsPrivileged to true to run the telegraf DaemonSet's
telegraf container in privileged mode
    # runDsPrivileged: '{{
.Values.telegraf_installer.kubernetes.ds.privileged_mode }}'

    # # Collect container Block IO metrics.
    # dsBlockIOEnabled: 'true'

    # # Collect NFS IO metrics.
    # dsNfsIOEnabled: 'true'

    # # Collect kubernetes.system_container metrics and objects in the
kube-system|cattle-system namespaces for managed kubernetes clusters (EKS,
AKS, GKE, managed Rancher).  Set this to true if you want collect these
metrics.
    # managedK8sSystemMetricCollectionEnabled: 'false'

    # # Collect kubernetes.pod_volume (pod ephemeral storage) metrics.
Set this to true if you want to collect these metrics.
    # podVolumeMetricCollectionEnabled: 'false'

    # # Declare Rancher cluster as managed.  Set this to true if your
Rancher cluster is managed as opposed to on-premise.
    # isManagedRancher: 'false'

    # # If telegraf-rs fails to start due to being unable to find the etcd
crt and key, manually specify the appropriate path here.
```

```
    # rsHostEtcdCrt: ''
    # rsHostEtcdKey: ''

  # kube-state-metrics:
    # # kube-state-metrics CPU/Mem limits and requests.
    # cpuLimit: '500m'
    # memLimit: '1Gi'
    # cpuRequest: '100m'
    # memRequest: '500Mi'

    # # Comma-separated list of resources to enable.
    # # See resources in https://github.com/kubernetes/kube-state-
metrics/blob/main/docs/cli-arguments.md
    # resources:
'cronjobs,daemonsets,deployments,ingresses,jobs,namespaces,nodes,persisten
tvolumeclaims,persistentvolumes,pods,replicasets,resourcequotas,services,s
tatefulsets'

    # # Comma-separated list of metrics to enable.
    # # See metric-allowlist in https://github.com/kubernetes/kube-state-
metrics/blob/main/docs/cli-arguments.md
    # metrics:
'kube_cronjob_created,kube_cronjob_status_active,kube_cronjob_labels,kube_
daemonset_created,kube_daemonset_status_current_number_scheduled,kube_daem
onset_status_desired_number_scheduled,kube_daemonset_status_number_availab
le,kube_daemonset_status_number_misscheduled,kube_daemonset_status_number_
ready,kube_daemonset_status_number_unavailable,kube_daemonset_status_obser
ved_generation,kube_daemonset_status_updated_number_scheduled,kube_daemons
et_metadata_generation,kube_daemonset_labels,kube_deployment_status_replic
as,kube_deployment_status_replicas_available,kube_deployment_status_replic
as_unavailable,kube_deployment_status_replicas_updated,kube_deployment_sta
tus_observed_generation,kube_deployment_spec_replicas,kube_deployment_spec
_paused,kube_deployment_spec_strategy_rollingupdate_max_unavailable,kube_d
eployment_spec_strategy_rollingupdate_max_surge,kube_deployment_metadata_g
eneration,kube_deployment_labels,kube_deployment_created,kube_job_created,
kube_job_owner,kube_job_status_active,kube_job_status_succeeded,kube_job_s
tatus_failed,kube_job_labels,kube_job_status_start_time,kube_job_status_co
mpletion_time,kube_namespace_created,kube_namespace_labels,kube_namespace_
status_phase,kube_node_info,kube_node_labels,kube_node_role,kube_node_spec
_unschedulable,kube_node_created,kube_persistentvolume_capacity_bytes,kube
_persistentvolume_status_phase,kube_persistentvolume_labels,kube_persisten
tvolume_info,kube_persistentvolume_claim_ref,kube_persistentvolumeclaim_ac
cess_mode,kube_persistentvolumeclaim_info,kube_persistentvolumeclaim_label
s,kube_persistentvolumeclaim_resource_requests_storage_bytes,kube_persiste
ntvolumeclaim_status_phase,kube_pod_info,kube_pod_start_time,kube_pod_comp
letion_time,kube_pod_owner,kube_pod_labels,kube_pod_status_phase,kube_pod_
```

```
status_ready,kube_pod_status_scheduled,kube_pod_container_info,kube_pod_co
ntainer_status_waiting,kube_pod_container_status_waiting_reason,kube_pod_c
ontainer_status_running,kube_pod_container_state_started,kube_pod_containe
r_status_terminated,kube_pod_container_status_terminated_reason,kube_pod_c
ontainer_status_last_terminated_reason,kube_pod_container_status_ready,kub
e_pod_container_status_restarts_total,kube_pod_overhead_cpu_cores,kube_pod
_overhead_memory_bytes,kube_pod_created,kube_pod_deletion_timestamp,kube_p
od_init_container_info,kube_pod_init_container_status_waiting,kube_pod_ini
t_container_status_waiting_reason,kube_pod_init_container_status_running,k
ube_pod_init_container_status_terminated,kube_pod_init_container_status_te
rminated_reason,kube_pod_init_container_status_last_terminated_reason,kube
_pod_init_container_status_ready,kube_pod_init_container_status_restarts_t
otal,kube_pod_status_scheduled_time,kube_pod_status_unschedulable,kube_pod
_spec_volumes_persistentvolumeclaims_readonly,kube_pod_container_resource_
requests_cpu_cores,kube_pod_container_resource_requests_memory_bytes,kube_
pod_container_resource_requests_storage_bytes,kube_pod_container_resource_
requests_ephemeral_storage_bytes,kube_pod_container_resource_limits_cpu_co
res,kube_pod_container_resource_limits_memory_bytes,kube_pod_container_res
ource_limits_storage_bytes,kube_pod_container_resource_limits_ephemeral_st
orage_bytes,kube_pod_init_container_resource_limits_cpu_cores,kube_pod_ini
t_container_resource_limits_memory_bytes,kube_pod_init_container_resource_
limits_storage_bytes,kube_pod_init_container_resource_limits_ephemeral_sto
rage_bytes,kube_pod_init_container_resource_requests_cpu_cores,kube_pod_in
it_container_resource_requests_memory_bytes,kube_pod_init_container_resour
ce_requests_storage_bytes,kube_pod_init_container_resource_requests_epheme
ral_storage_bytes,kube_replicaset_status_replicas,kube_replicaset_status_r
eady_replicas,kube_replicaset_status_observed_generation,kube_replicaset_s
pec_replicas,kube_replicaset_metadata_generation,kube_replicaset_labels,ku
be_replicaset_created,kube_replicaset_owner,kube_resourcequota,kube_resour
cequota_created,kube_service_info,kube_service_labels,kube_service_created
,kube_service_spec_type,kube_statefulset_status_replicas,kube_statefulset_
status_replicas_current,kube_statefulset_status_replicas_ready,kube_statef
ulset_status_replicas_updated,kube_statefulset_status_observed_generation,
kube_statefulset_replicas,kube_statefulset_metadata_generation,kube_statef
ulset_created,kube_statefulset_labels,kube_statefulset_status_current_revi
sion,kube_statefulset_status_update_revision,kube_node_status_capacity,kub
e_node_status_allocatable,kube_node_status_condition,kube_pod_container_re
source_requests,kube_pod_container_resource_limits,kube_pod_init_container
_resource_limits,kube_pod_init_container_resource_requests'

    # # Comma-separated list of Kubernetes label keys that will be used in
the resources' labels metric.
    # # See metric-labels-allowlist in https://github.com/kubernetes/kube-
state-metrics/blob/main/docs/cli-arguments.md
    # labels:
'cronjobs=[*],daemonsets=[*],deployments=[*],ingresses=[*],jobs=[*],namesp
```

```
aces=[*],nodes=[*],persistentvolumeclaims=[*],persistentvolumes=[*],pods=[
*],replicasets=[*],resourcequotas=[*],services=[*],statefulsets=[*]'

    # # kube-state-metrics additional tolerations. Use the following
abbreviated single line format only.
    # # No tolerations are applied by default
    # # Example: '{key: taint1, operator: Exists, effect:
NoSchedule},{key: taint2, operator: Exists, effect: NoExecute}'
    # tolerations: ''

    # # kube-state-metrics shards.  Increase the number of shards for
larger clusters if telegraf RS pod(s) experience collection timeouts
    # shards: '2'

  # # Settings for the Events Log feature.
  # logs:
    # # Set runPrivileged to true if Fluent Bit fails to start, trying to
open/create its database.
    # runPrivileged: 'false'

    # # If Fluent Bit should read new files from the head, not tail.
    # # See Read_from_Head in
https://docs.fluentbit.io/manual/pipeline/inputs/tail
    # readFromHead: "true"

    # # Network protocol that Fluent Bit should use for DNS: "UDP" or
"TCP".
    # dnsMode: "UDP"

    # # DNS resolver that Fluent Bit should use: "LEGACY" or "ASYNC"
    # fluentBitDNSResolver: "LEGACY"

    # # Logs additional tolerations. Use the following abbreviated single
line format only.
    # # Inspect fluent-bit-ds to view tolerations which are always
present. No tolerations are applied by default for event-exporter.
    # # Example: '{key: taint1, operator: Exists, effect:
NoSchedule},{key: taint2, operator: Exists, effect: NoExecute}'
    # fluent-bit-tolerations: ''
    # event-exporter-tolerations: ''

    # # event-exporter CPU/Mem limits and requests.
    # # See https://kubernetes.io/docs/concepts/configuration/manage-
resources-containers/
    # event-exporter-cpuLimit: '500m'
    # event-exporter-memLimit: '1Gi'
```

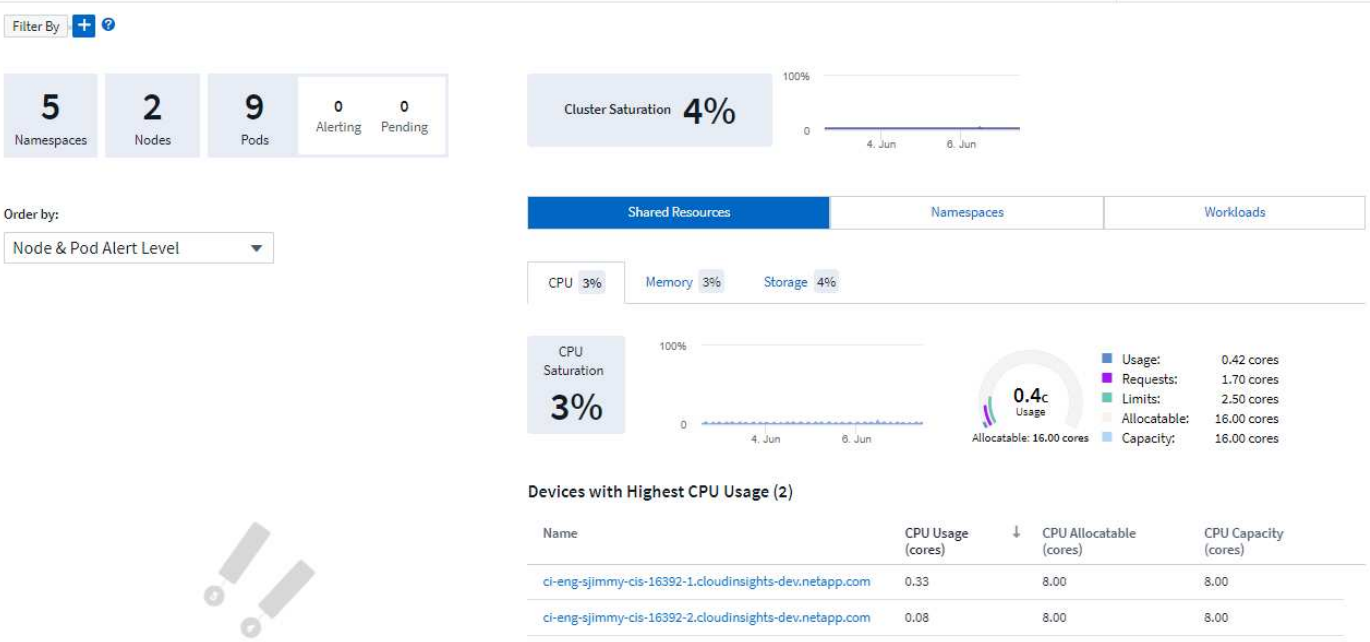
```
    # event-exporter-cpuRequest: '50m'
    # event-exporter-memRequest: '100Mi'

    # # event-exporter max event age.
    # # See https://github.com/jkroepke/resmoio-kubernetes-event-exporter
    # event-exporter-maxEventAgeSeconds: '10'

    # # event-exporter client-side throttling
    # # Set kubeBurst to roughly match your events per minute and
kubeQPS=kubeBurst/5
    # # See https://github.com/resmoio/kubernetes-event-
exporter#troubleshoot-events-discarded-warning
    # event-exporter-kubeQPS: 20
    # event-exporter-kubeBurst: 100

    # # fluent-bit CPU/Mem limits and requests.
    # # See https://kubernetes.io/docs/concepts/configuration/manage-
resources-containers/
    # fluent-bit-cpuLimit: '500m'
    # fluent-bit-memLimit: '1Gi'
    # fluent-bit-cpuRequest: '50m'
    # fluent-bit-memRequest: '100Mi'

    # By default, the Fluentbit DaemonSet will mount the /var/log and
/var/lib/docker/containers host paths to access/read the
    # Kubernetes container logs.  If Kubernetes has been configured to
place container logs in a non-default location, use
    # this option to modify the Fluentbit DaemonSet to mount the non-
default path.
    # fluent-bit-containerLogPath

  # # Settings for the Network Performance and Map feature.
  # workload-map:
    # # netapp-ci-net-observer-l4-ds CPU/Mem limits and requests.
    # # See https://kubernetes.io/docs/concepts/configuration/manage-
resources-containers/
    # cpuLimit: '500m'
    # memLimit: '500Mi'
    # cpuRequest: '100m'
    # memRequest: '500Mi'

    # # Metric aggregation interval in seconds. Min=30, Max=120
    # metricAggregationInterval: '60'

    # # Interval for bpf polling. Min=3, Max=15
    # bpfPollInterval: '8'
```

```
    # # Enable performing reverse DNS lookups on observed IPs.
    # enableDNSLookup: 'true'

    # # netapp-ci-net-observer-l4-ds additional tolerations. Use the
following abbreviated single line format only.
    # # Inspect netapp-ci-net-observer-l4-ds to view tolerations which are
always present.
    # # Example: '{key: taint1, operator: Exists, effect:
NoSchedule},{key: taint2, operator: Exists, effect: NoExecute}'
    # l4-tolerations: ''

    # # Set runPrivileged to true if SELinux is enabled on your Kubernetes
nodes.
    # # Note: In OpenShift environments, this is set to true
automatically.
    # runPrivileged: 'false'

  # change-management:
    # # change-observer-watch-rs CPU/Mem limits and requests.
    # # See https://kubernetes.io/docs/concepts/configuration/manage-
resources-containers/
    # cpuLimit: '1'
    # memLimit: '1Gi'
    # cpuRequest: '500m'
    # memRequest: '500Mi'

    # # Interval after which a non-successful deployment of a workload
will be marked as failed, in seconds
    # workloadFailureDeclarationIntervalSeconds: '30'

    # # Frequency at which workload deployments are combined and sent, in
seconds
    # workloadDeployAggrIntervalSeconds: '300'

    # # Frequency at which non-workload deployments are combined and sent,
in seconds
    # nonWorkloadDeployAggrIntervalSeconds: '15'

    # # A set of regular expressions used in env names and data maps whose
value will be redacted
    # termsToRedact: '"pwd", "password", "token", "apikey", "api-key",
"api_key", "jwt", "accesskey", "access_key", "access-key", "ca-file",
"key-file", "cert", "cafile", "keyfile", "tls", "crt", "salt",
".dockerconfigjson", "auth", "secret"'

    # # A comma separated list of additional kinds to watch from the
```

```
default set of kinds watched by the collector
    # # Each kind will have to be prefixed by its apigroup
    # # Example: '"authorization.k8s.io.subjectaccessreviews"'
    # additionalKindsToWatch: ''

    # # A comma separated list of additional field paths whose diff is
ignored as part of change analytics. This list in addition to the default
set of field paths ignored by the collector.
    # # Example: '"metadata.specTime", "data.status"'
    # additionalFieldsDiffToIgnore: ''

    # # A comma separated list of kinds to ignore from watching from the
default set of kinds watched by the collector
    # # Each kind will have to be prefixed by its apigroup
    # # Example: '"networking.k8s.io.networkpolicies,batch.jobs",
"authorization.k8s.io.subjectaccessreviews"'
    # kindsToIgnoreFromWatch: ''

    # # Frequency with which log records are sent to CI from the collector
    # logRecordAggrIntervalSeconds: '20'

    # # change-observer-watch-ds additional tolerations. Use the following
abbreviated single line format only.
    # # Inspect change-observer-watch-ds to view tolerations which are
always present.
    # # Example: '{key: taint1, operator: Exists, effect:
NoSchedule},{key: taint2, operator: Exists, effect: NoExecute}'
    # watch-tolerations: ''
```

Kubernetes-Cluster-Detailseite

Auf der Detailseite des Kubernetes-Clusters wird eine detaillierte Übersicht über Ihren Kubernetes-Cluster angezeigt.



Anzahl der Namespaces, Knoten und Pods

Die Zählungen oben auf der Seite zeigen Ihnen die Gesamtzahl der Namespaces, Knoten und Pods im Cluster sowie die Anzahl der Popds, die derzeit Alarm schlagen und ausstehen.

Gemeinsam genutzte Ressourcen und Sättigung

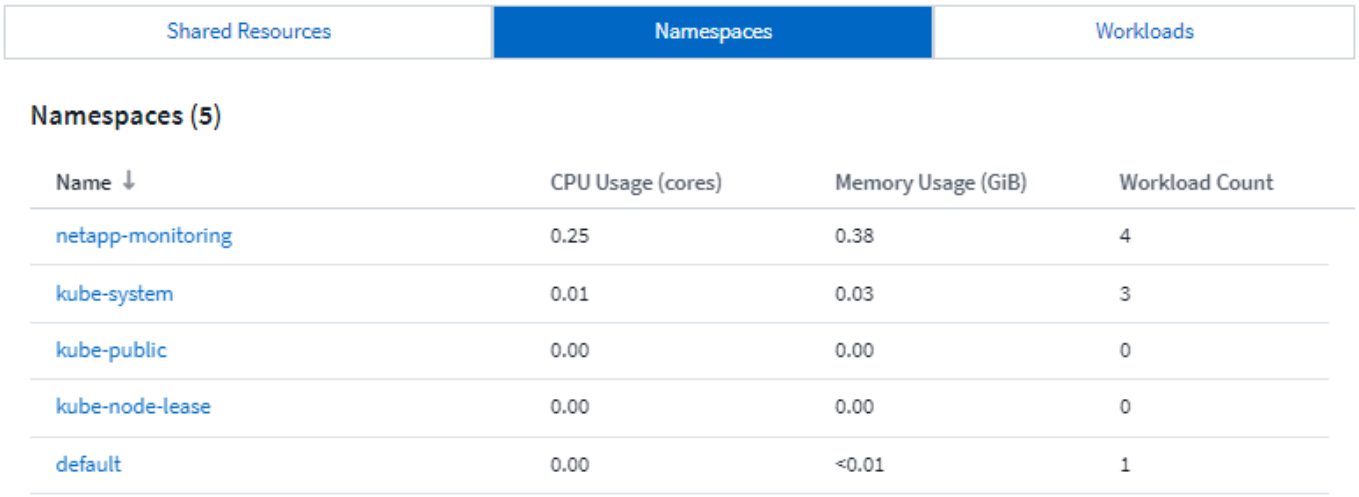
Oben rechts auf der Detailseite wird Ihre Clustersättigung als aktueller Prozentsatz sowie ein Diagramm angezeigt, das den aktuellen Trend im Zeitverlauf zeigt. Die Clustersättigung ist die höchste CPU-, Speicher- oder Speichersättigung zu jedem Zeitpunkt.

Darunter zeigt die Seite standardmäßig die Nutzung **gemeinsam genutzter Ressourcen** mit Registerkarten für CPU, Arbeitsspeicher und Speicherplatz. Jede Registerkarte zeigt den Sättigungsprozentsatz und den Trend im Zeitverlauf mit zusätzlichen Nutzungsdetails. Beim Speicher ist der angezeigte Wert der höhere der beiden Werte für Backend- und Dateisystemsättigung, die unabhängig voneinander berechnet werden.

Die Geräte mit der höchsten Nutzung werden unten in einer Tabelle angezeigt. Klicken Sie auf einen beliebigen Link, um diese Geräte zu erkunden.

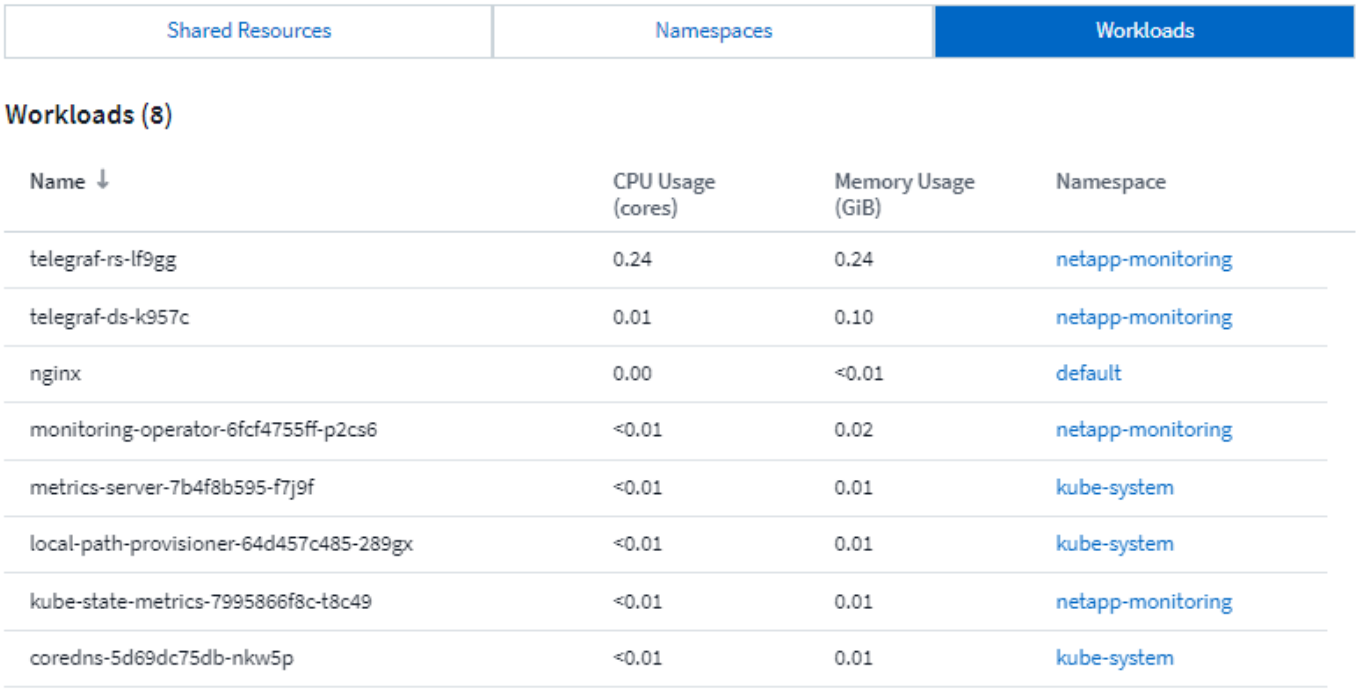
Namensräume

Auf der Registerkarte „Namespaces“ wird eine Liste aller Namespaces in Ihrer Kubernetes-Umgebung angezeigt, die die CPU- und Speicherauslastung sowie die Anzahl der Workloads in jedem Namespace anzeigt. Klicken Sie auf die Namenslinks, um die einzelnen Namespaces zu erkunden.



Arbeitslasten

Ebenso wird auf der Registerkarte „Workloads“ eine Liste der Workloads in jedem Namespace angezeigt, wobei auch hier die CPU- und Speicherauslastung angezeigt wird. Durch Klicken auf die Namespace-Links gelangen Sie zu den einzelnen Links.



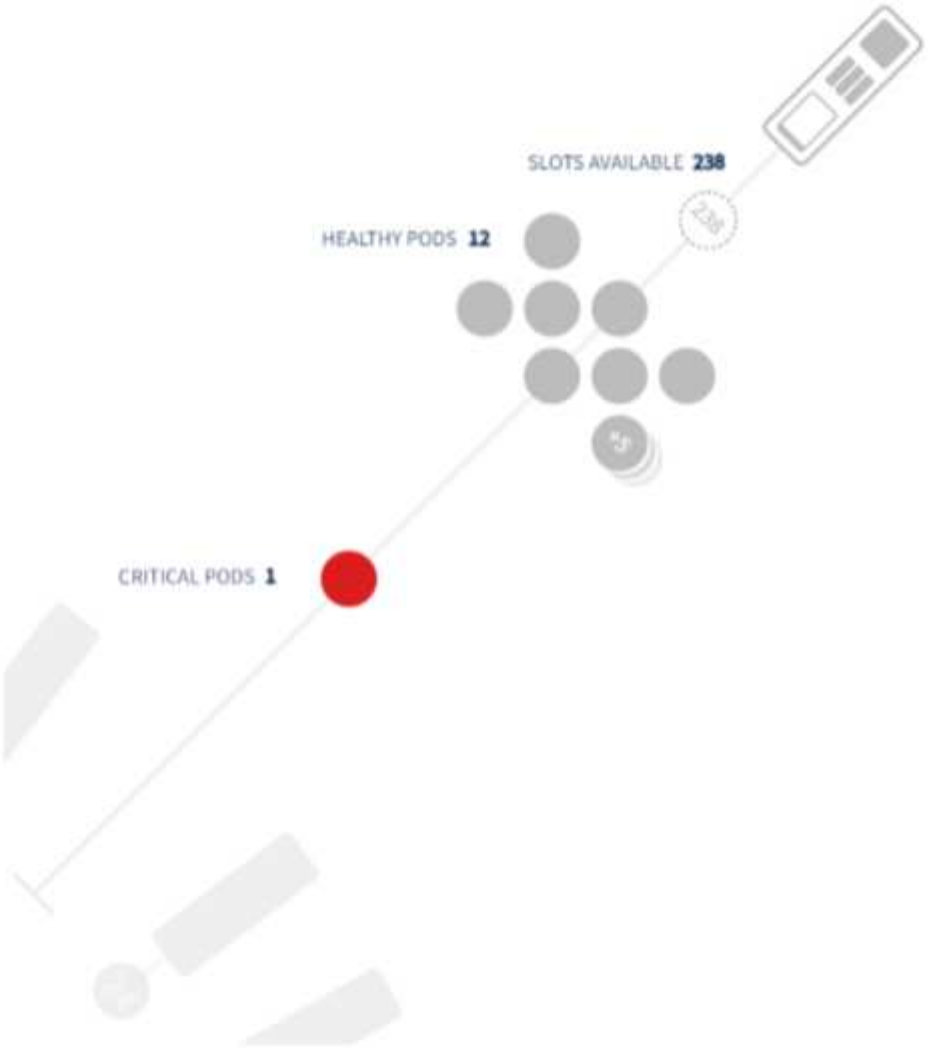
Das Cluster-„Rad“

Der Cluster-Abschnitt „Rad“ bietet auf einen Blick Informationen zum Zustand von Knoten und Pods, die Sie für weitere Informationen genauer untersuchen können. Wenn Ihr Cluster mehr Knoten enthält, als in diesem Bereich der Seite angezeigt werden können, können Sie das Rad mit den verfügbaren Schaltflächen drehen.

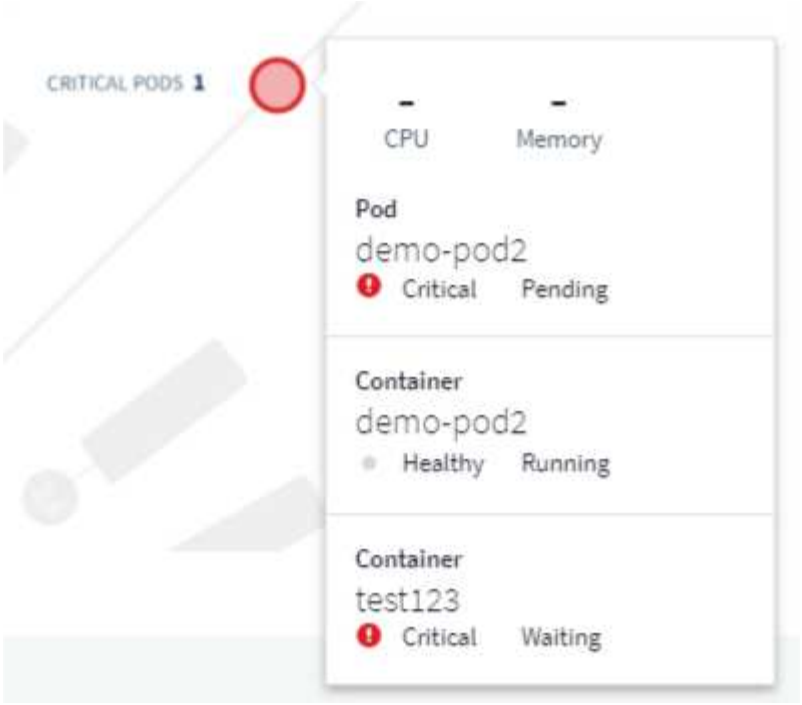
Alarmierende Pods oder Knoten werden rot angezeigt. „Warnbereiche“ werden orange angezeigt. Nicht geplante (d. h. nicht verbundene) Pods werden in der unteren Ecke des Cluster-„Rads“ angezeigt.

Wenn Sie mit der Maus über einen Pod (Kreis) oder Knoten (Balken) fahren, wird die Ansicht des Knotens erweitert.

Wenn Sie in dieser Ansicht auf den Pod oder Knoten klicken, wird die erweiterte Knotenansicht vergrößert.



Von hier aus können Sie mit der Maus über ein Element fahren, um Details zu diesem Element anzuzeigen. Wenn Sie in diesem Beispiel beispielsweise mit der Maus über den kritischen Pod fahren, werden Details zu diesem Pod angezeigt.



Sie können Informationen zu Dateisystem, Speicher und CPU anzeigen, indem Sie mit der Maus über die Knotenelemente fahren.

Ein Hinweis zu den Messgeräten

Die Speicher- und CPU-Anzeigen zeigen drei Farben an, da sie die *Nutzung* im Verhältnis zur *zuweisbaren Kapazität* und zur *Gesamtkapazität* anzeigen.

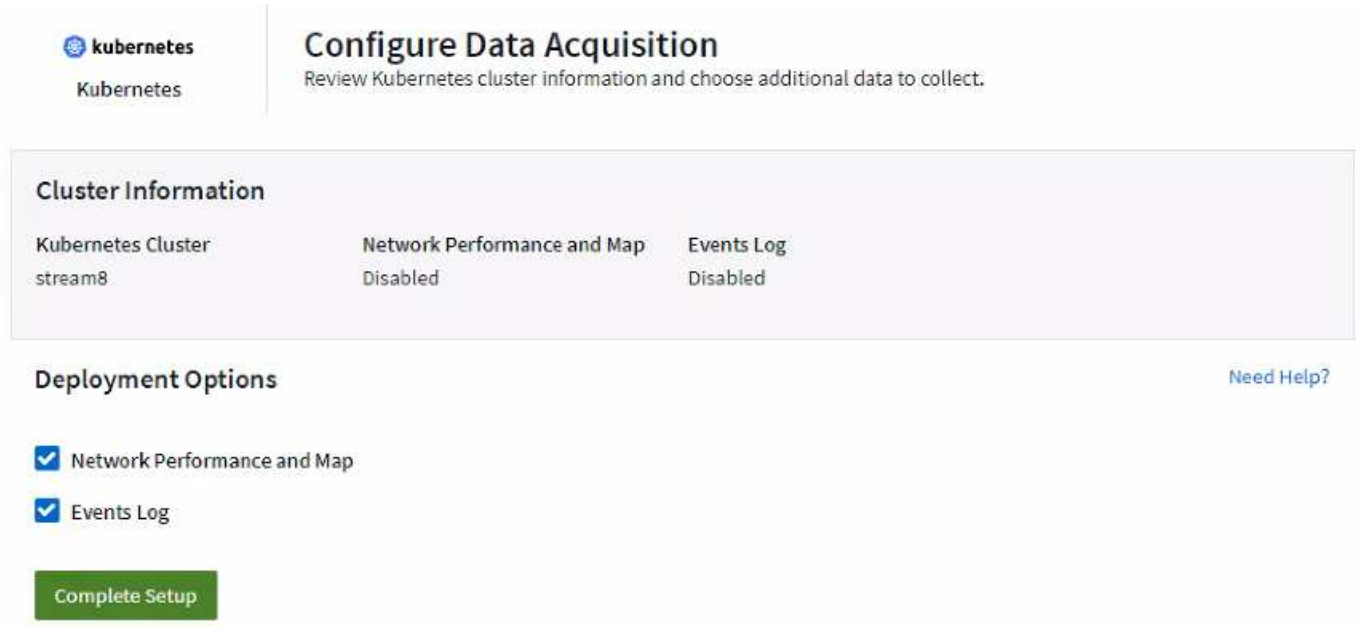
Überwachung und Zuordnung der Kubernetes-Netzwerkleistung

Die Funktion „Netzwerkleistungsüberwachung und -zuordnung“ von Kubernetes vereinfacht die Fehlerbehebung durch die Zuordnung von Abhängigkeiten zwischen Diensten (auch Workloads genannt) und bietet Echtzeit-Einblicke in Latenzen und Anomalien der Netzwerkleistung, um Leistungsprobleme zu erkennen, bevor sie sich auf Benutzer auswirken. Diese Funktion hilft Unternehmen, die Gesamtkosten durch die Analyse und Prüfung von Kubernetes-Verkehrsflüssen zu senken.

Hauptfunktionen: • Die Workload Map stellt Kubernetes-Workload-Abhängigkeiten und -Flows dar und hebt Netzwerk- und Leistungsprobleme hervor. • Überwachen Sie den Netzwerkverkehr zwischen Kubernetes-Pods, Workloads und Knoten; identifizieren Sie die Quelle von Verkehrs- und Latenzproblemen. • Reduzieren Sie die Gesamtkosten, indem Sie den eingehenden, ausgehenden, regions- und zonenübergreifenden Netzwerkverkehr analysieren.

Voraussetzungen

Bevor Sie die Kubernetes-Netzwerkleistungsüberwachung und -karte verwenden können, müssen Sie Folgendes konfiguriert haben:"NetApp Kubernetes Monitoring Operator" um diese Option zu aktivieren. Aktivieren Sie während der Bereitstellung des Operators das Kontrollkästchen „Netzwerkleistung und Karte“, um die Funktion zu aktivieren. Sie können diese Option auch aktivieren, indem Sie zu einer Kubernetes-Landingpage navigieren und „Bereitstellung ändern“ auswählen.



Monitore

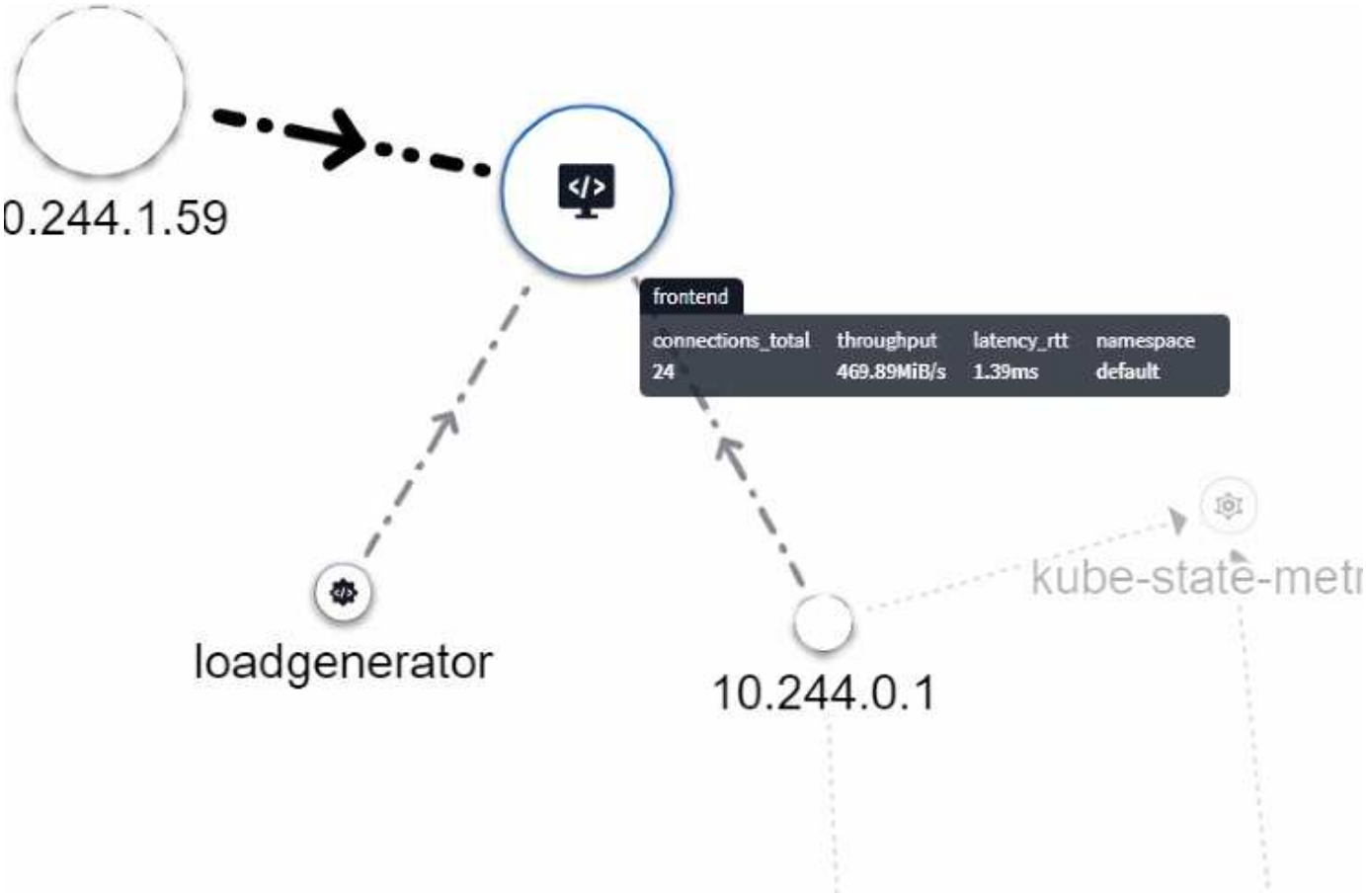
Die Workload Map verwendet"Monitore" um Informationen abzuleiten. Data Infrastructure Insights bietet eine Reihe von standardmäßigen Kubernetes-Monitoren (beachten Sie, dass diese standardmäßig *angehalten* sein können). Sie können die gewünschten Monitore *fortsetzen* (d. h. aktivieren) oder benutzerdefinierte Monitore für Kubernetes-Objekte erstellen, die auch von der Workload Map verwendet werden.

Sie können Data Infrastructure Insights -Metrikwarnungen für alle der folgenden Objekttypen erstellen. Stellen Sie sicher, dass die Daten nach dem Standardobjekttyp gruppiert sind.

- kubernetes.workload
- kubernetes.daemonset
- kubernetes.deployment
- kubernetes.cronjob
- kubernetes.job
- kubernetes.replicaset
- kubernetes.statefulset
- kubernetes.pod
- kubernetes.network_traffic_l4

Die Karte

Die Karte zeigt Dienste/Workloads und ihre Beziehungen zueinander. Pfeile zeigen die Verkehrsrichtung an. Wenn Sie mit der Maus über eine Arbeitslast fahren, werden zusammenfassende Informationen zu dieser Arbeitslast angezeigt, wie Sie in diesem Beispiel sehen können:



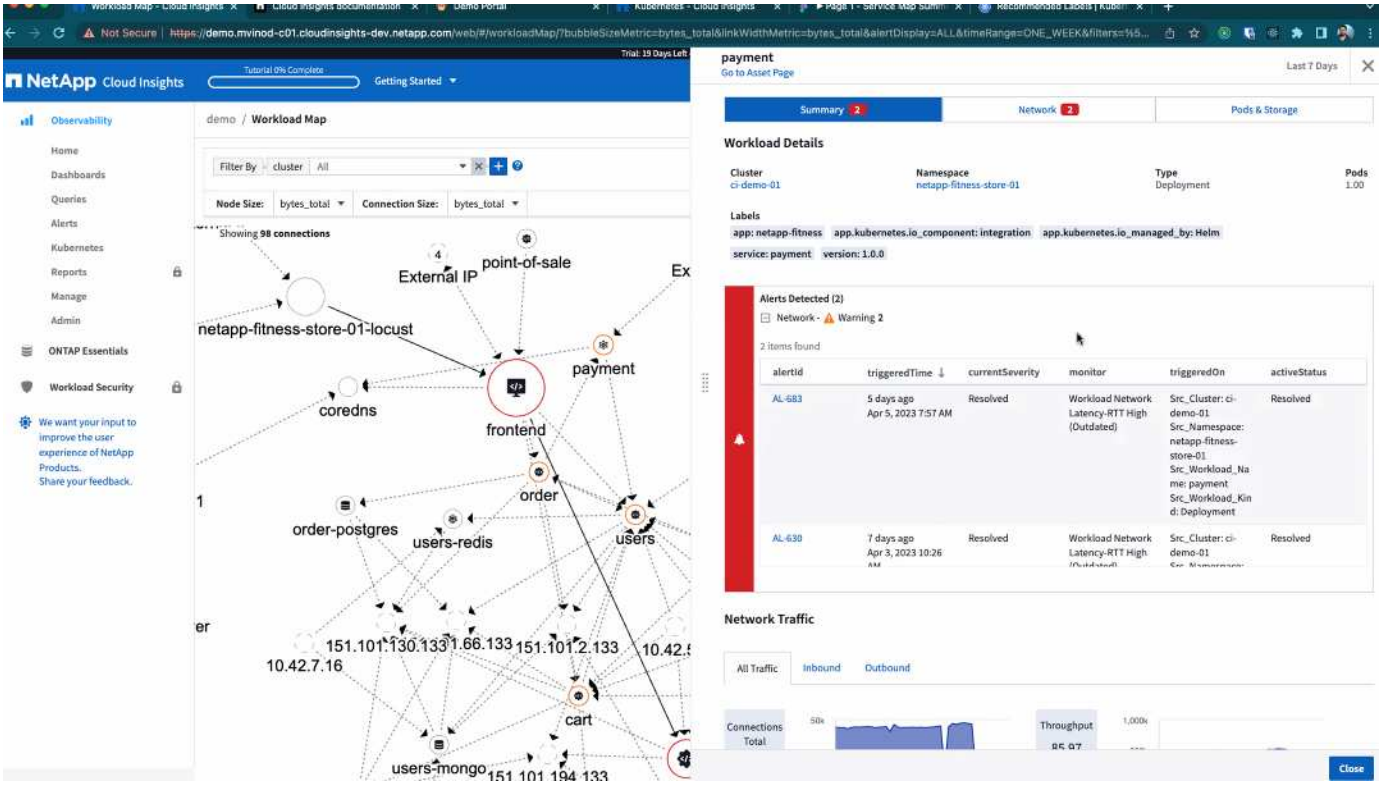
Die Symbole in den Kreisen stellen unterschiedliche Servicetypen dar. Beachten Sie, dass Symbole nur sichtbar sind, wenn die darunter liegenden ObjekteEtiketten .

Die Größe jedes Kreises gibt die Knotengröße an. Beachten Sie, dass diese Größen relativ sind. Die Zoomstufe Ihres Browsers oder die Bildschirmgröße können die tatsächliche Kreisgröße beeinflussen. Auf die gleiche Weise bietet Ihnen der Verkehrslinienstil einen Überblick über die Verbindungsgröße. Fette durchgezogene Linien stehen für hohen Verkehr, während hell gepunktete Linien für geringeren Verkehr stehen.

Die Zahlen in den Kreisen geben die Anzahl der externen Verbindungen an, die derzeit vom Dienst verarbeitet werden.

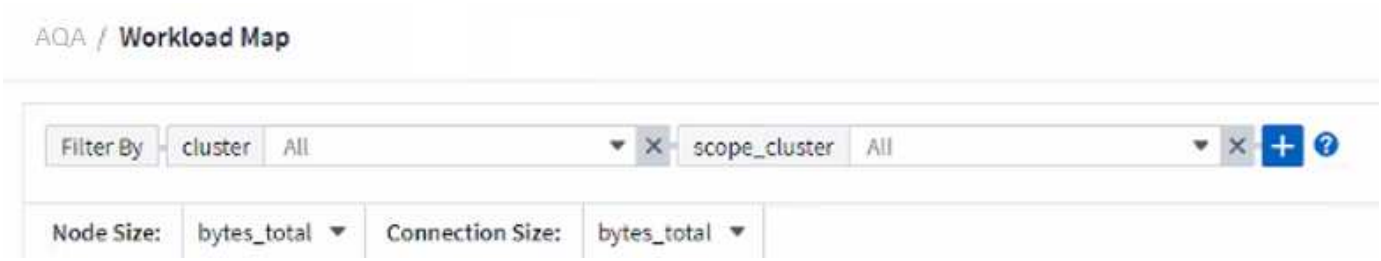
Arbeitslastdetails und Warnungen

Farbig angezeigte Kreise weisen auf eine Warnung oder einen Alarm der kritischen Stufe für die Arbeitslast hin. Bewegen Sie den Mauszeiger über den Kreis, um eine Zusammenfassung des Problems anzuzeigen, oder klicken Sie auf den Kreis, um ein Slideout-Fenster mit weiteren Details zu öffnen.

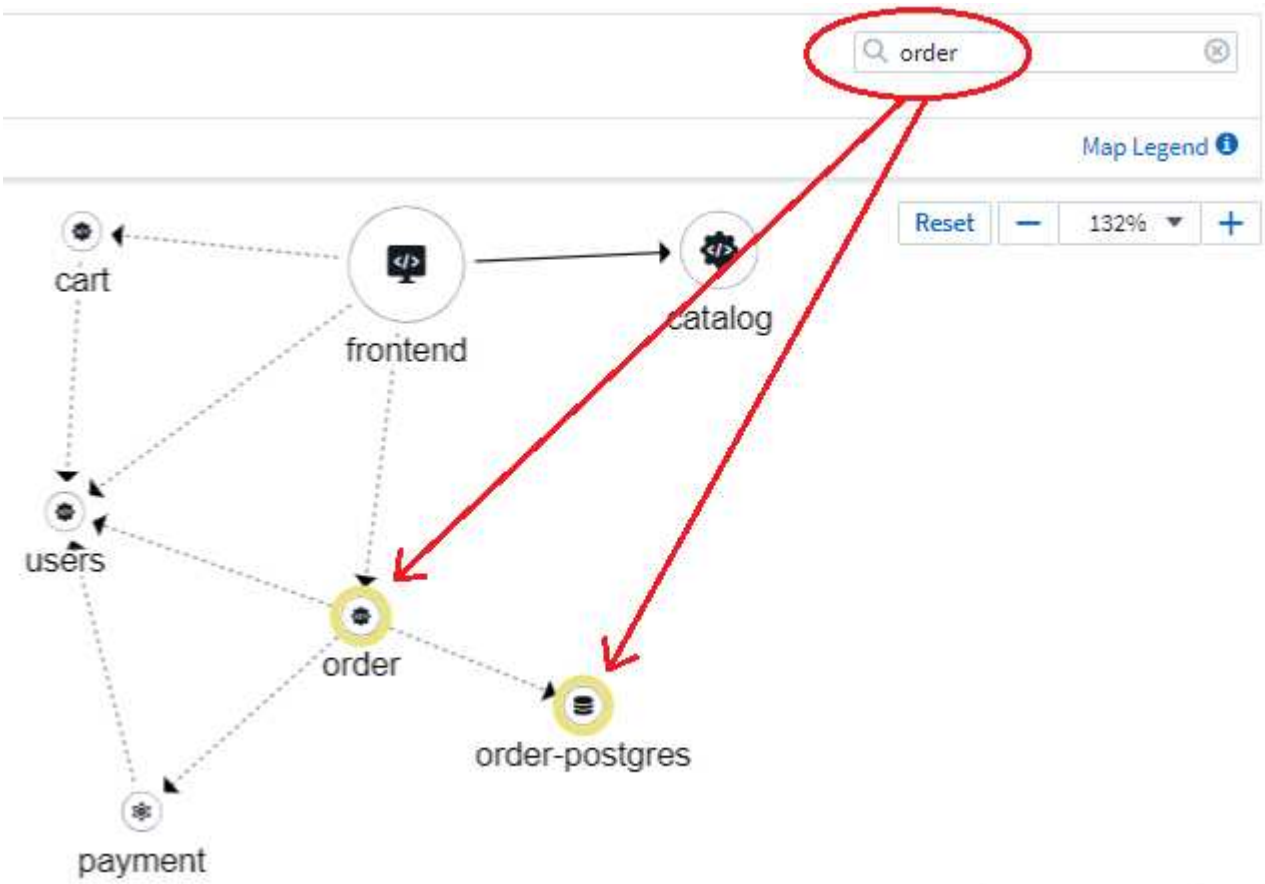


Suchen und Filtern

Wie bei anderen Data Infrastructure Insights Funktionen können Sie ganz einfach Filter festlegen, um sich auf die gewünschten spezifischen Objekte oder Workload-Attribute zu konzentrieren.



Ebenso werden durch die Eingabe einer Zeichenfolge in das Feld *Suchen* passende Workloads hervorgehoben.



Arbeitslastbezeichnungen

Arbeitslastbeschriftungen sind erforderlich, wenn die Karte die angezeigten Arbeitslasttypen identifizieren soll (d. h. die Kreissymbole). Die Bezeichnungen werden wie folgt abgeleitet:

- Name des ausgeführten Dienstes/der ausgeführten Anwendung in allgemeinen Begriffen
- Wenn die Quelle ein Pod ist:
  - Das Label wird vom Workload-Label des Pods abgeleitet
  - Erwartete Bezeichnung für die Arbeitslast: app.kubernetes.io/component
  - Referenz des Etikettennamens: https://kubernetes.io/docs/concepts/overview/working-with-objects/common-labels/
  - Empfohlene Etiketten:
    - Frontend

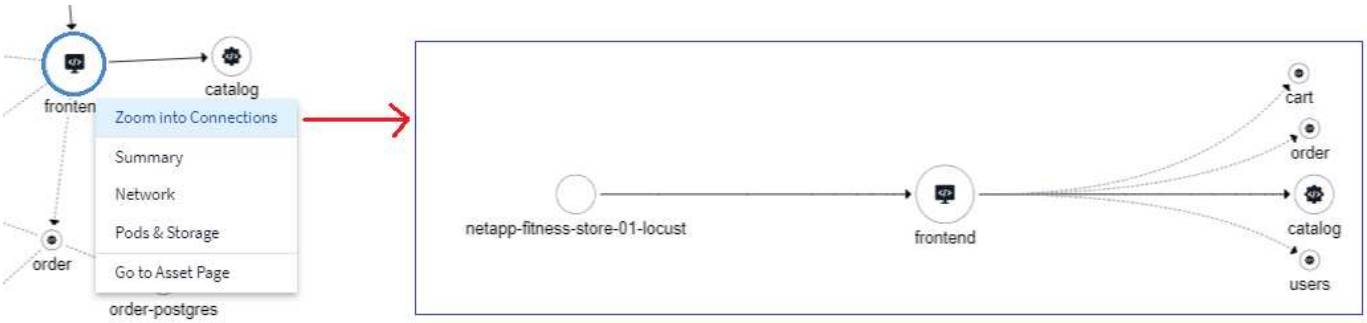
- Backend
- Datenbank
- Cache
- Warteschlange
- Kafka

- Wenn die Quelle außerhalb des Kubernetes-Clusters liegt:
  - Data Infrastructure Insights versucht, den DNS-aufgelösten Namen zu analysieren, um den Diensttyp zu extrahieren.

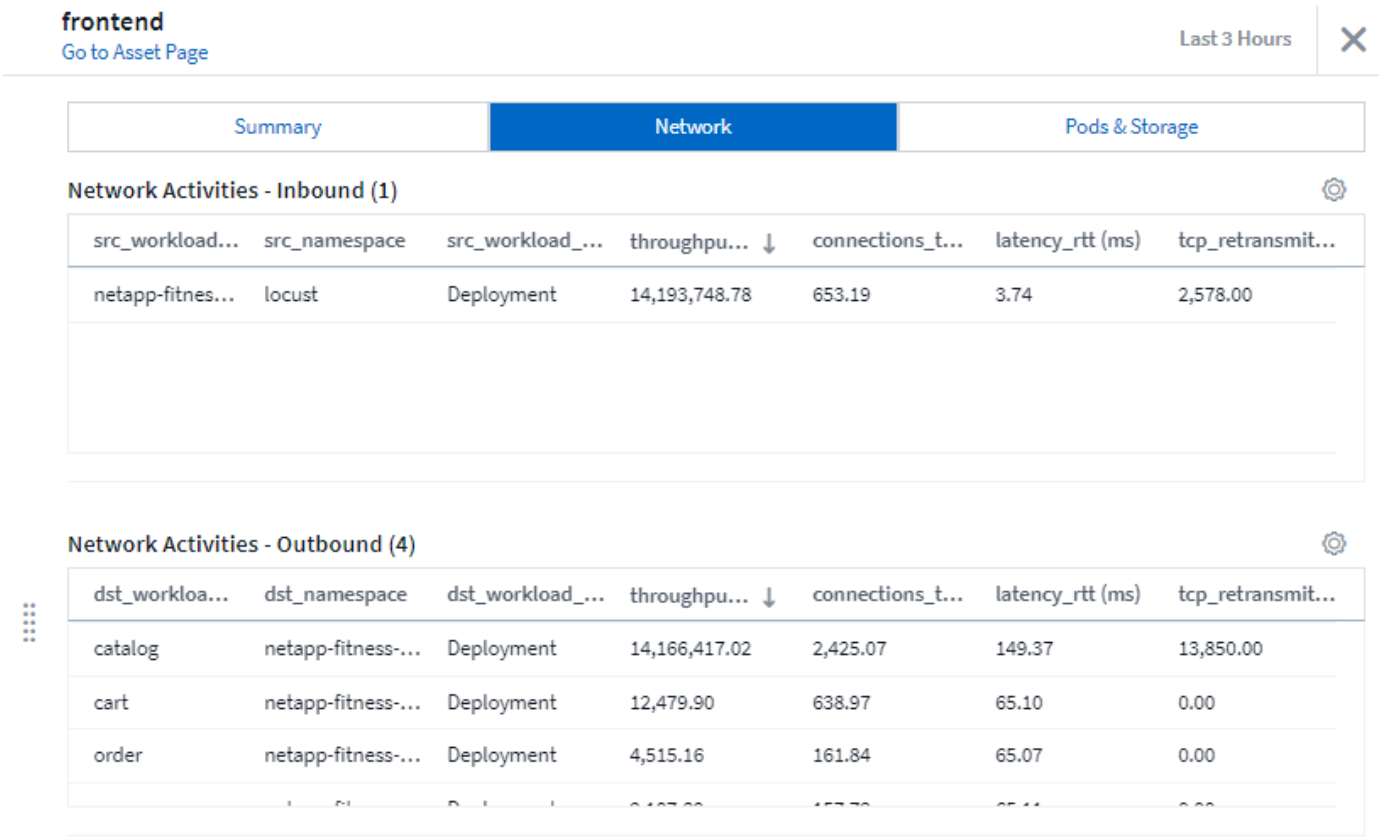
    Beispielsweise wird bei einem DNS-aufgelösten Namen von *s3.eu-north-1.amazonaws.com* der aufgelöste Name analysiert, um *s3* als Diensttyp zu erhalten.

Tauchen Sie tief ein

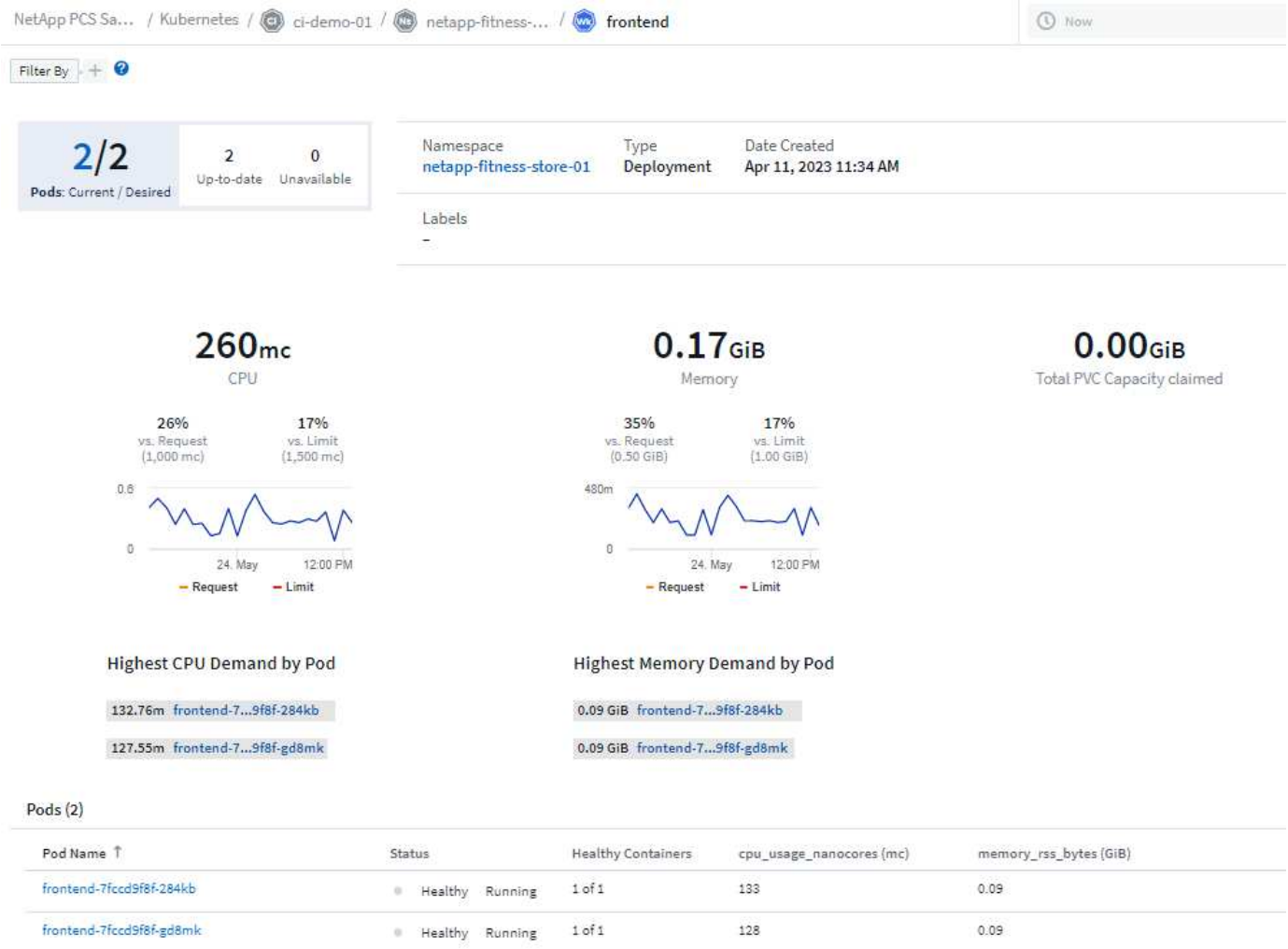
Wenn Sie mit der rechten Maustaste auf eine Arbeitslast klicken, werden Ihnen zusätzliche Optionen zur weiteren Erkundung angezeigt. Von hier aus können Sie beispielsweise hineinzoomen, um die Verbindungen für diese Arbeitslast anzuzeigen.



Oder Sie können das Detail-Slideout-Panel öffnen, um die Registerkarten „Zusammenfassung“, „Netzwerk“ oder „Pod & Speicher“ direkt anzuzeigen.



Wenn Sie abschließend „Zur Asset-Seite gehen“ auswählen, wird die detaillierte Asset-Landingpage für die Arbeitslast geöffnet.



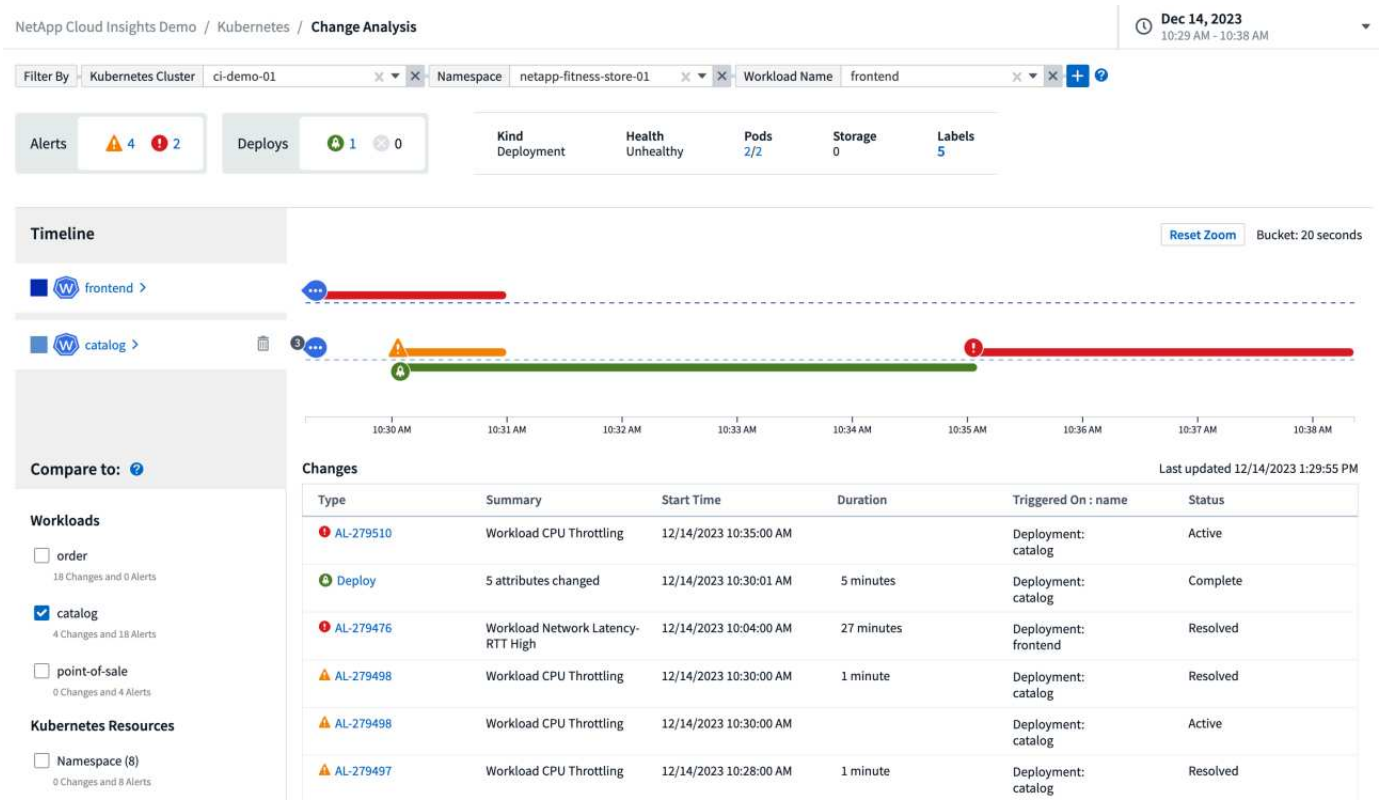
Kubernetes-Änderungsanalyse

Kubernetes Change Analytics bietet Ihnen eine umfassende Ansicht der jüngsten Änderungen an Ihrer K8s-Umgebung. Sie haben jederzeit Zugriff auf Warnmeldungen und den Bereitstellungsstatus. Mit Change Analytics können Sie jede Bereitstellungs- und Konfigurationsänderung verfolgen und mit dem Zustand und der Leistung der Dienste, Infrastruktur und Cluster von K8s korrelieren.

Wie hilft die Änderungsanalyse?

- In Kubernetes-Umgebungen mit mehreren Mandanten kann es aufgrund falsch konfigurierter Änderungen zu Ausfällen kommen. Change Analytics hilft dabei, indem es einen einzigen Bereich bereitstellt, in dem der Zustand von Workloads und Konfigurationsänderungen angezeigt und korreliert werden kann. Dies kann bei der Fehlerbehebung in dynamischen Kubernetes-Umgebungen hilfreich sein.

Um Kubernetes Change Analytics anzuzeigen, navigieren Sie zu **Kubernetes > Änderungsanalyse**.



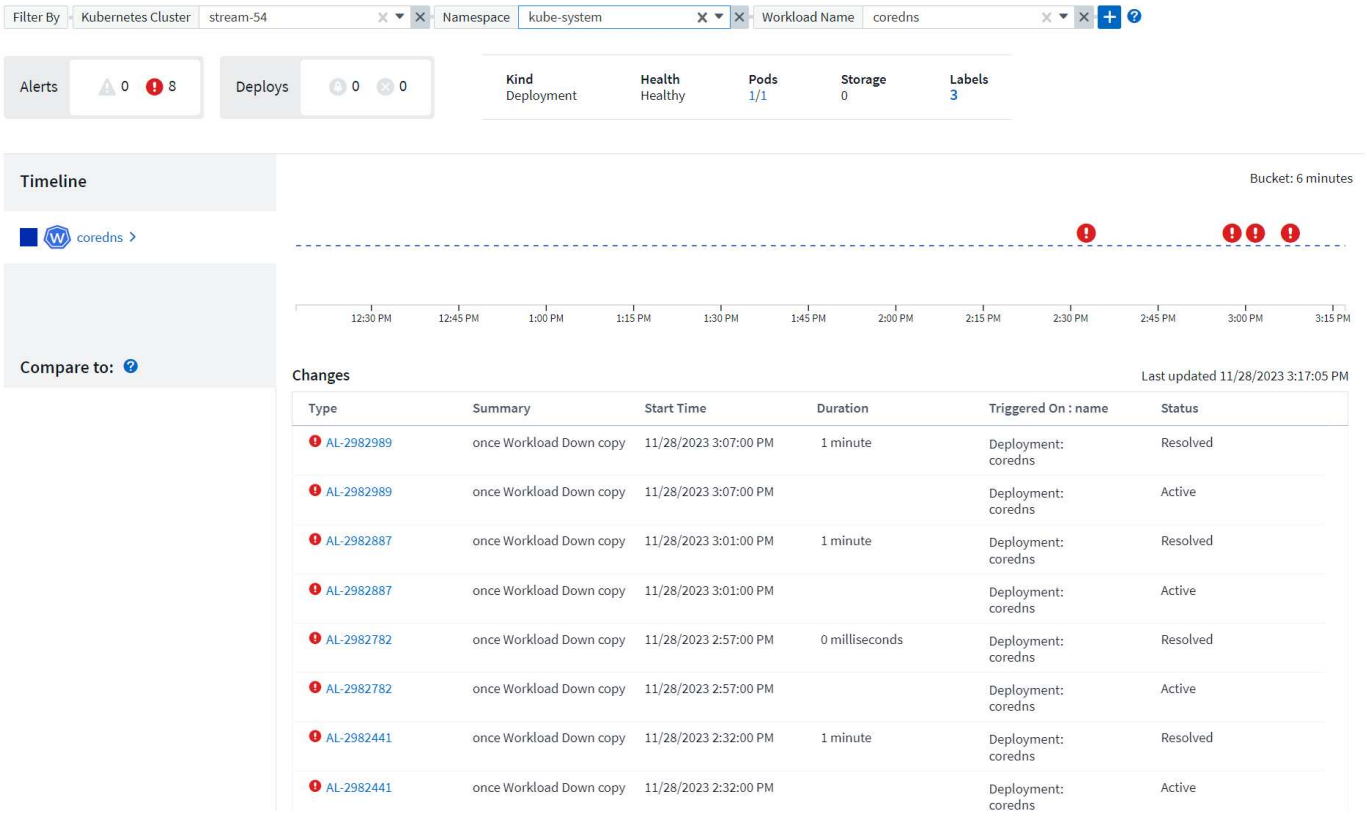
.

Die Seite wird automatisch basierend auf dem aktuell ausgewählten Data Infrastructure Insights -Zeitraum aktualisiert. Kleinere Zeiträume bedeuten eine häufigere Bildschirmaktualisierung.

Filtern

Wie bei allen Funktionen von Data Infrastructure Insights ist das Filtern der Änderungsliste intuitiv: Geben Sie oben auf der Seite Werte für Ihren Kubernetes-Cluster, Namespace oder Workload ein oder wählen Sie diese aus oder fügen Sie Ihre eigenen Filter hinzu, indem Sie die Schaltfläche {+] auswählen.

Wenn Sie auf einen bestimmten Cluster, Namespace und Workload (zusammen mit allen anderen von Ihnen festgelegten Filtern) filtern, wird Ihnen eine Zeitleiste mit Bereitstellungen und Warnungen für diesen Workload in diesem Namespace auf diesem Cluster angezeigt. Zoomen Sie weiter hinein, indem Sie im Diagramm klicken und ziehen, um sich auf einen spezifischeren Zeitbereich zu konzentrieren.

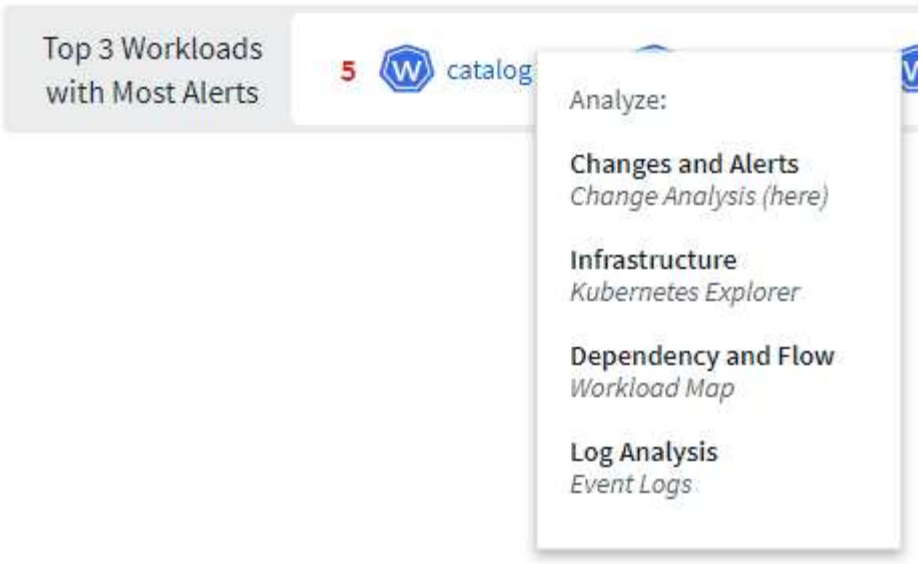


Schnellstatus

Unterhalb des Filterbereichs befinden sich eine Reihe von Indikatoren auf hoher Ebene. Links steht die Anzahl der Alarme (Warnung und Kritisch). Diese Zahl umfasst sowohl *aktive* als auch *gelöste* Warnungen. Um nur *aktive* Warnungen anzuzeigen, legen Sie einen Filter für „Status“ fest und wählen Sie „Aktiv“.

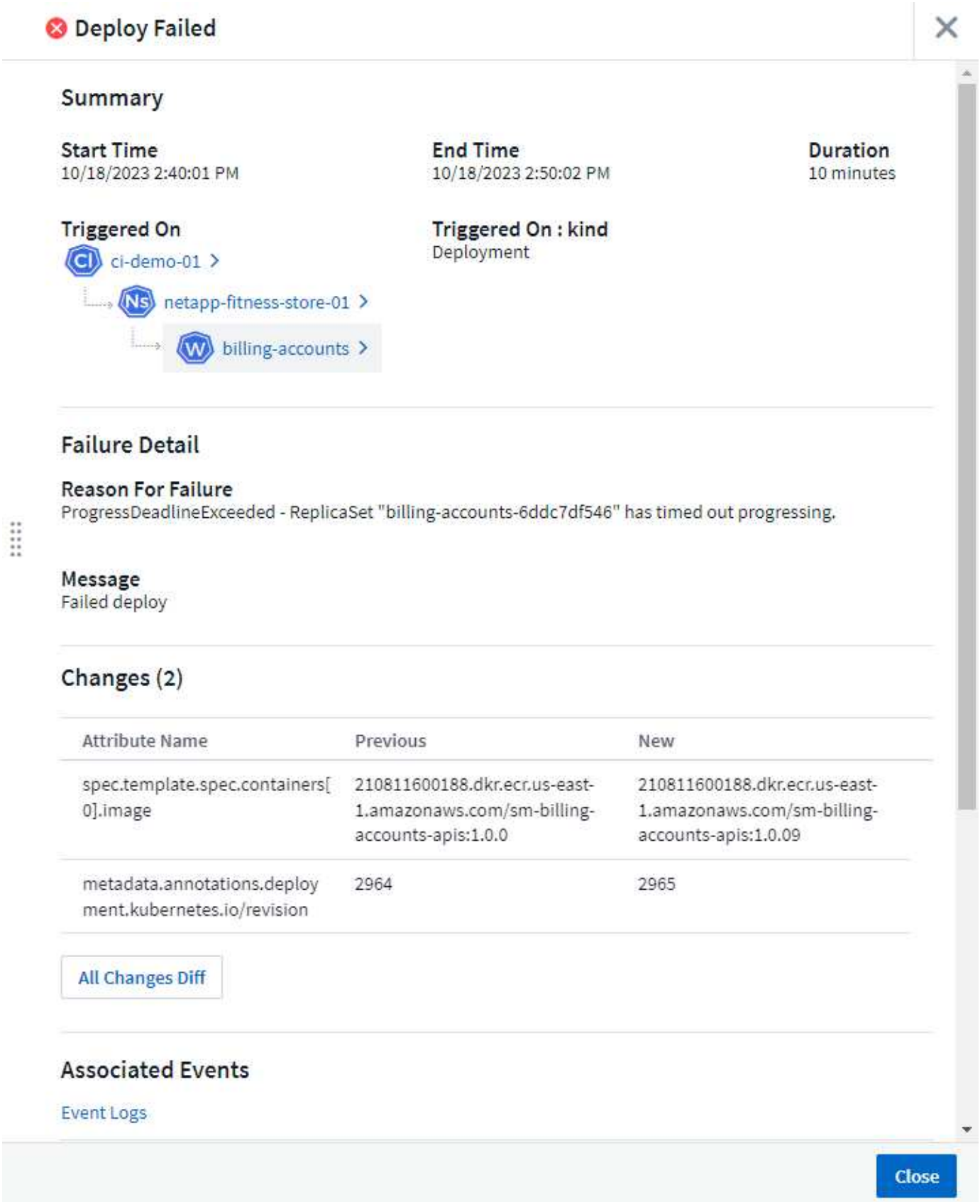
Der Bereitstellungsstatus wird hier ebenfalls angezeigt. Auch hier wird standardmäßig die Anzahl der gestarteten, abgeschlossenen und fehlgeschlagenen Bereitstellungen angezeigt. Um nur *fehlgeschlagene* Bereitstellungen anzuzeigen, legen Sie einen Filter für „Status“ fest und wählen Sie „Fehlgeschlagen“ aus.

Als nächstes folgen die drei Workloads mit den meisten Warnungen. Die rote Zahl neben jeder Arbeitslast gibt die Anzahl der Warnungen an, die mit dieser Arbeitslast in Zusammenhang stehen. Klicken Sie auf den Workload-Link, um Ihre Infrastruktur (Kubernetes Explorer), Abhängigkeiten (Workload Map) oder Protokollanalyse (Ereignisprotokolle) zu erkunden.



Detailbereich

Wenn Sie eine Änderung in der Liste auswählen, wird ein Fenster geöffnet, in dem die Änderung ausführlicher beschrieben wird. Wenn Sie beispielsweise eine fehlgeschlagene Bereitstellung auswählen, wird eine Zusammenfassung der Bereitstellung mit Start- und Endzeit, Dauer und Auslöseort der Bereitstellung sowie Links zum Durchsuchen dieser Ressourcen angezeigt. Außerdem werden der Grund für den Fehler, alle damit verbundenen Änderungen und alle zugehörigen Ereignisse angezeigt.



Durch Auswahl einer Warnung werden ebenfalls Details zur Warnung bereitgestellt, darunter der Monitor, der die Warnung ausgelöst hat, sowie ein Diagramm mit einer visuellen Zeitleiste für die Warnung.

ONTAP Essentials

ONTAP Essentials ist eine Reihe von Dashboards und Workflows, die detaillierte Übersichten über Ihre ONTAP -Bestände und -Workloads bieten. Bei der Arbeit mit ONTAP Essentials werden Ihnen möglicherweise die folgenden Begriffe angezeigt:

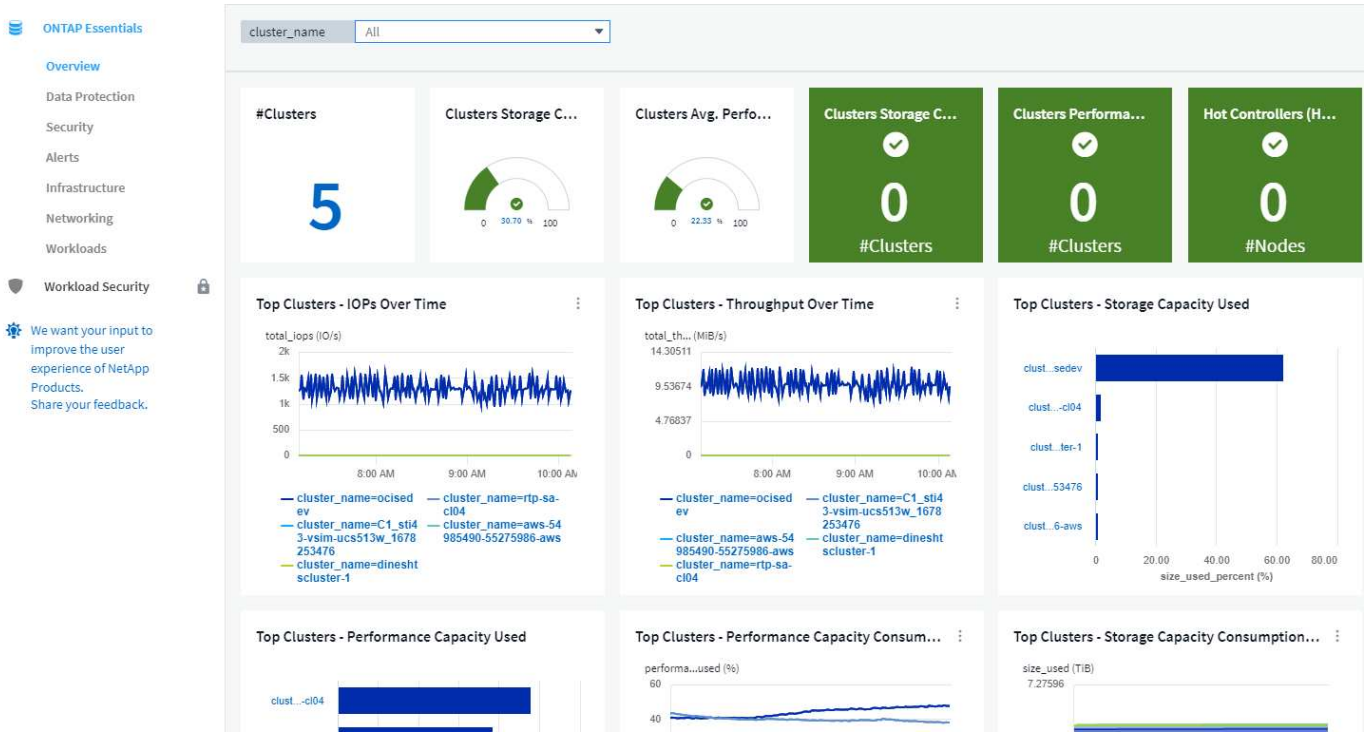
- Infrastruktur/Inventar: Objekte, die Speicher-/Netzwerkdienste für Benutzerdaten bereitstellen
- Workloads: Objekte, die Benutzern eine Schnittstelle zum Lesen/Schreiben von Daten bieten.
- Datenschutz: Objekte, die mit NetApp Datenschutztechnologien geschützt werden können

Weitere Begriffe und Definitionen im Zusammenhang mit ONTAP finden Sie im"ONTAP-Datensammler" Dokumentation.

ONTAP Essentials erfordert mindestens einen funktionierenden ONTAP Datensammler mit Daten, die innerhalb der letzten sieben Tage erfasst wurden.

Überblick

Um mit der Erkundung zu beginnen, wählen Sie * ONTAP Essentials* aus dem Hauptmenü „Data Infrastructure Insights“ .



Das Dashboard **Übersicht** zeigt nützliche Informationen an, beispielsweise die Anzahl der Cluster auf Ihrem Mandanten mit ihrer Gesamtkapazität und den Leistungsprozentsätzen. Sie erhalten außerdem Prognosedaten zur voraussichtlichen Anzahl von Tagen, bis die Speicherkapazität oder Leistungskapazität nicht mehr ausreicht. Wenn außerdem Controller in Ihrer Infrastruktur mit einer CPU-Auslastung von über 65 % laufen – und Ihr Cluster im Falle eines Failovers möglicherweise gefährdet –, werden diese von ONTAP Essentials als „Hot“-Controller angezeigt.

Aussagekräftige Diagramme geben Ihnen einen Einblick in die Leistung im Zeitverlauf sowie eine

Aufschlüsselung der Kapazitätsauslastung. Jedes dieser Diagramme oder Datenpunkte kann als Ausgangspunkt für Erkundungen oder Untersuchungen verwendet werden.

Hinweis: Eine „Tage bis zur vollständigen Befüllung“-Zahl von „0“ (Null) gibt an, dass die geschätzte Anzahl der Tage bis zur vollständigen Befüllung mehr als 90 Tage beträgt. Mit anderen Worten: Es besteht nicht die Gefahr, dass Ihren Systemen in absehbarer Zeit der Speicherplatz ausgeht.

Datensicherung

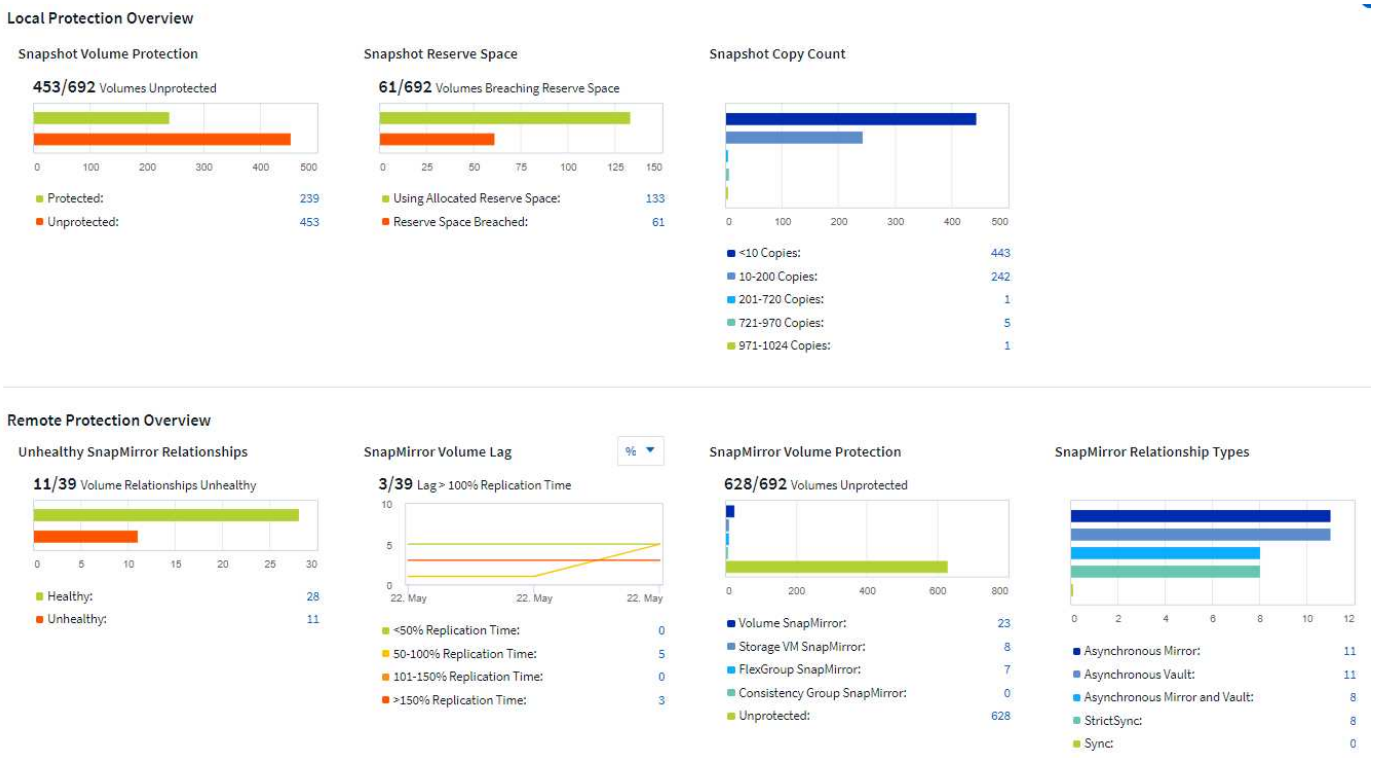
Auf der Seite **Datenschutz** wird der Status von Volumes angezeigt, die durch **Snapshot-Kopien** oder * SnapMirror Richtlinien* geschützt sind.

Im Abschnitt „Übersicht über den lokalen Schutz“ enthalten die Diagramme die folgenden Informationen zu Volumes, die durch Snapshot-Kopien geschützt sind:

- Die Anzahl der durch Snapshot-Kopien geschützten und nicht geschützten Volumes.
- Die Anzahl der Volumes, die den reservierten Speicherplatz für die Snapshot-Kopien verwenden oder überschreiten.
- Die Anzahl der Volumes in bestimmten Bereichen der Snapshot-Kopienanzahl (d. h. weniger als 10 Kopien, 10 bis 200 usw.).

Im Abschnitt „Übersicht zum Remote-Schutz“ enthalten die Diagramme Informationen zu den durch SnapMirror -Richtlinien geschützten Volumes:

- Die Anzahl der gesunden und ungesunden SnapMirror -Beziehungen.
- Die Anzahl der SnapMirror -Beziehungen, bei denen basierend auf dem Verzögerungsstatus eine Verzögerung des Recovery Point Objectives (RPO) auftritt.
- Die Anzahl der durch SnapMirror Volume-Schutztypen geschützten Beziehungen, wie Volume SnapMirror, SVMDR-Beziehungen, FlexGroup SnapMirror -Beziehungen, SnapMirror Business Continuity (SMBC) Consistency Group-Beziehungen sowie ungeschützte Volumes.
- Die Anzahl der durch die SnapMirror Beziehungstypen geschützten Beziehungen wie Asynchronous Mirror, Asynchronous Vault, Asynchronous MirrorVault, StrictSync und Sync.



Das Raster „Cluster“ unten auf der Seite enthält Details zu folgenden Punkten:

- Volumes, die nicht durch Snapshots geschützt sind.
- Volumes überschreiten den reservierten Speicherplatz für Snapshots.
- Bei Volumes, die nicht durch Snapmirror-Richtlinien und Snapmirror-Beziehungen geschützt sind, kommt es zu Verzögerungen.
- Ungesunde SnapMirror -Beziehungen.

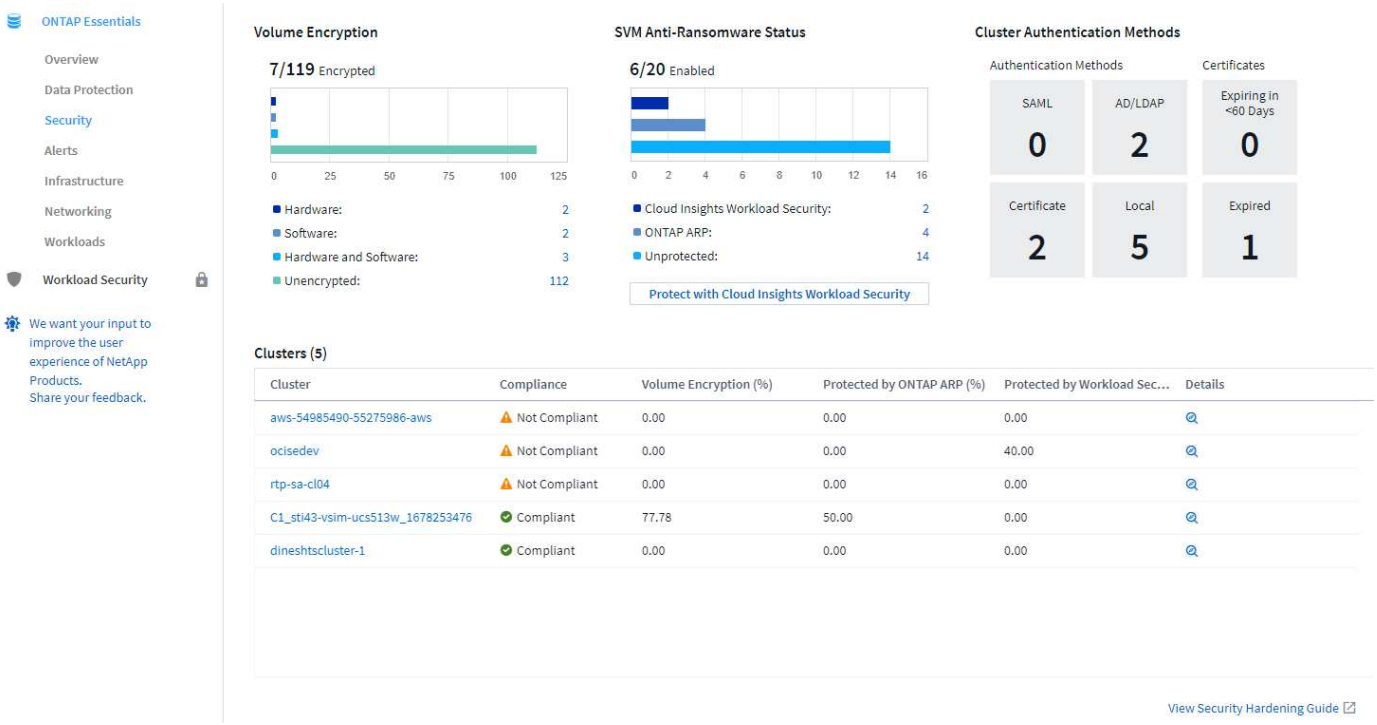
Clusters (6)

Cluster	Volumes Not Protected by Snapshots ↓	Volumes Breaching Snapshot Reserve Space	Volumes Not Protected by SnapMirror	SnapMirror Relationships Experiencing Lag	Unhealthy SnapMirror Relationships
rtp-sa-cl01	304	1	393	0	1
umeng-aff300-01-02	123	20	160	1	3
annapook-vsim12	7	4	7	0	3
C1_sti11-vsim-ucs574m_168327	0	0	0	0	0
C1_sti43-vsim-ucs513w_167825	0	0	0	0	0
ci-cs-fas8060-01-02	0	0	0	0	0

Sicherheit

Das Sicherheits-Dashboard bietet Ihnen einen sofortigen Überblick über Ihre aktuelle Sicherheitslage und zeigt Diagramme zur Hardware- und Software-Volume-Verschlüsselung, zum Anti-Ransomware-Status und zu Cluster-Authentifizierungsmethoden. Die Sicherheitskriterien werden auf Grundlage der Empfehlungen bewertet, die in der"* NetApp Security Hardening Guide für ONTAP 9*" .

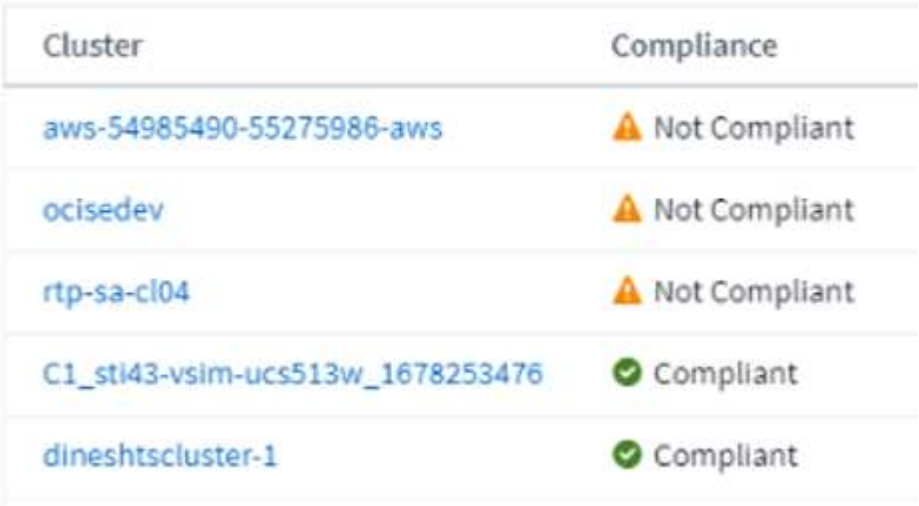
Wählen Sie eine der Verschlüsselungs- oder Anti-Ransomware-Funktionen aus, um Ihre Umgebung genauer zu untersuchen.



Das ONTAP Essentials Security-Dashboard überwacht Ihre Umgebung, um den Cluster-Compliance-Status zu ermitteln. Weitere Informationen finden Sie im"Cluster-Compliance-Kategorien" um mehr zu erfahren. ONTAP Essentials verwendet die folgenden Monitore, um die Konformität zu bestimmen:

Monitorname	Attributname (wird in den Clusterdetails angezeigt)	Attributkonformer Wert
FIPS-Modus deaktiviert	FIPS-Modus	Ermöglicht
Cluster Unsichere Chiffren für SSH	Sichere SSH-Einstellungen	Ja
Telnet-Protokoll aktiviert	Telnet	Deaktiviert
Remote Shell aktiviert	Remote-Shell	Deaktiviert
Standardmäßiger lokaler Administratorbenutzer aktiviert	Standard-Administratorbenutzer	Deaktiviert
MD5-gehashtes Passwort	MD5 im Einsatz	Nein
Cluster-Peer-Kommunikation nicht verschlüsselt	Cluster-Peering	Verschlüsselt/ Kein Peer
AutoSupport HTTPS-Transport deaktiviert	AutoSupport mit HTTPS	Ja
Es sind keine NTP-Server konfiguriert	Netzwerkzeitprotokoll	Konfiguriert
Die Anzahl der NTP-Server ist niedrig	Netzwerkzeitprotokoll	Konfiguriert
Cluster-Anmeldebanner deaktiviert	Login-Banner	Ermöglicht
Protokollweiterleitung nicht verschlüsselt	Verschlüsselte Protokollweiterleitung	Ja

Beachten Sie, dass bei deaktiviertem Monitor in den Clusterdetails für das entsprechende Sicherheitskonformitätsattribut der Wert „Nicht aktiviert“ angezeigt wird.

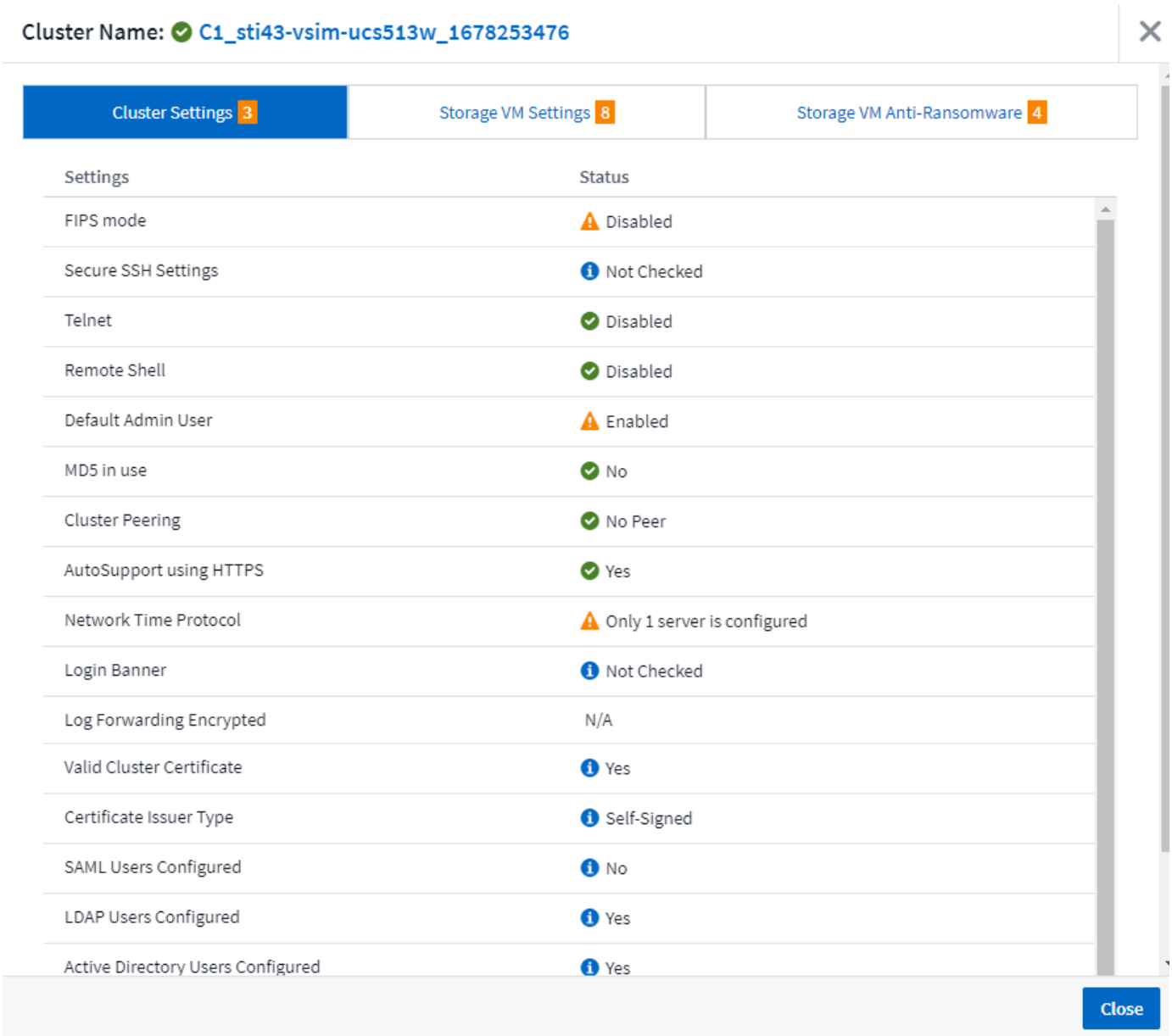


Bei SVMs werden im Sicherheits-Dashboard die folgenden Monitore angezeigt:

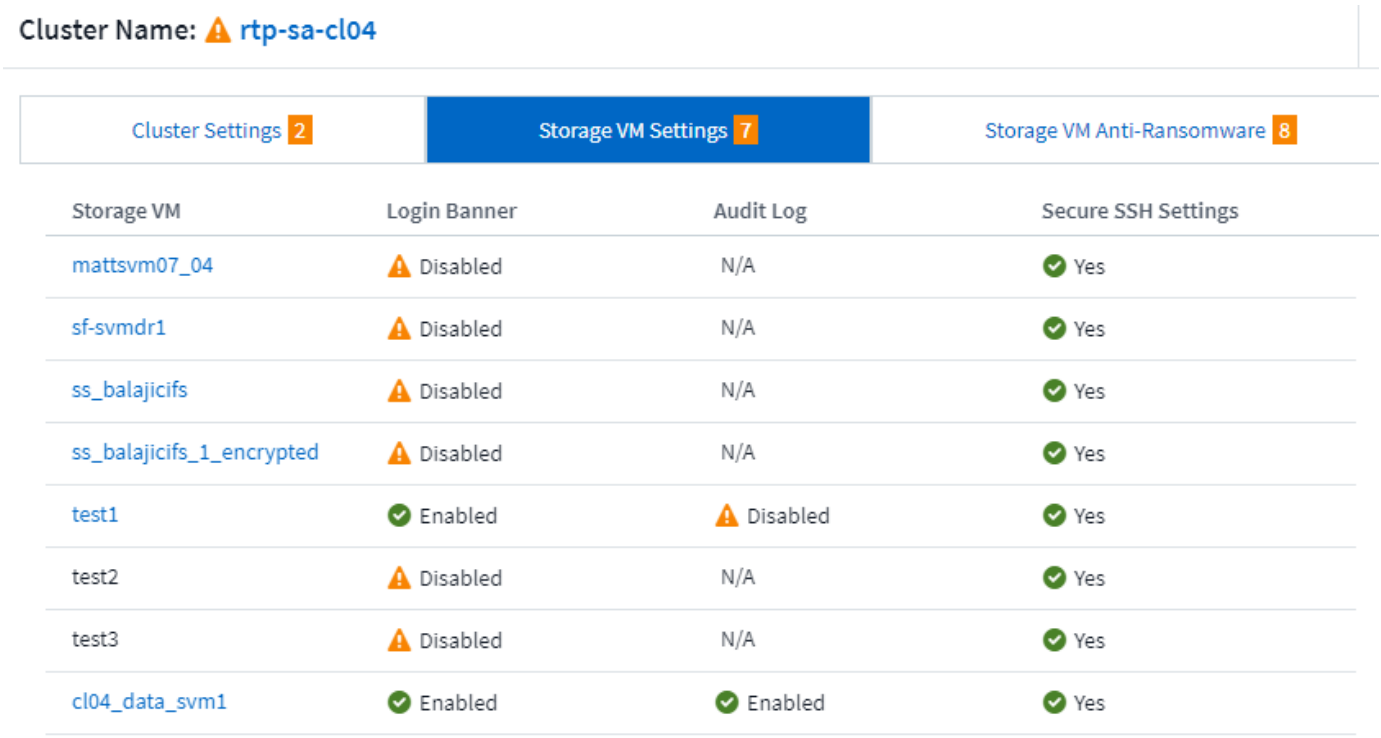
Monitorname	**Attributname (wird in den Storage-VM-Einstellungen angezeigt)**	**Attributkonformer Wert**
Unsichere Verschlüsselungsverfahren für Storage-VMs für SSH	Sichere SSH-Einstellungen	Ja
Storage VM-Anmeldebanner deaktiviert	Login-Banner	Ermöglicht
Speicher-VM-Auditprotokoll deaktiviert	Prüfprotokoll	Ermöglicht

Wählen Sie in der Clusterliste für jeden Cluster „Details anzeigen“ aus, um ein ausziehbares Fenster zu öffnen, das Ihnen die aktuellen Einstellungen für „Cluster“, „Speicher-VM“ oder „Anti-Ransomware“ anzeigt.

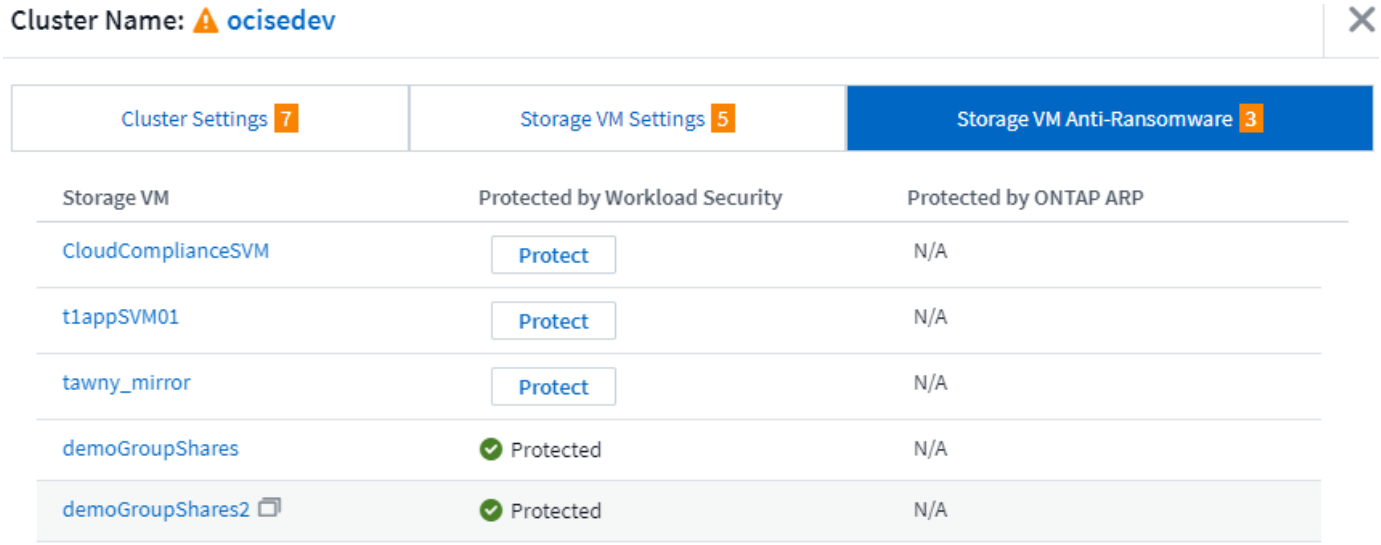
Zu den Clusterdetails gehören Verbindungsstatus, Zertifikatsinformationen und mehr:



Die Details der Speicher-VM zeigen Audit- und SSH-Informationen:

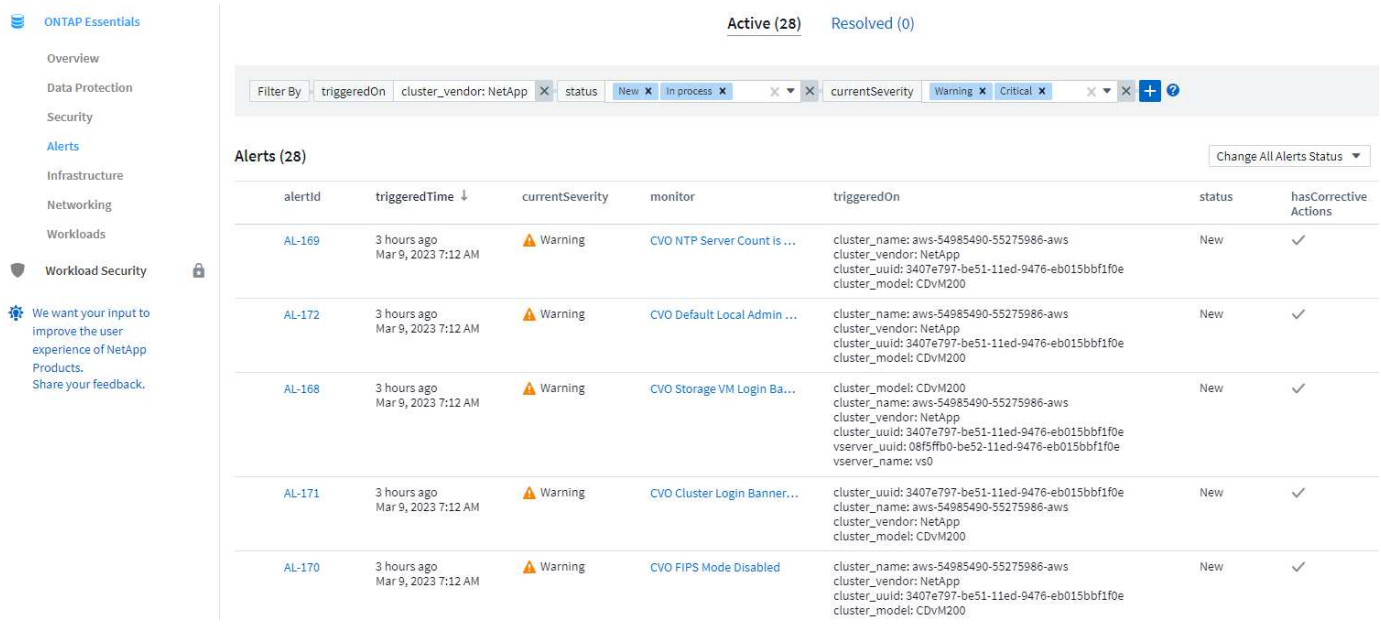


Anti-Ransomware-Details zeigen, ob eine Speicher-VM durch ONTAPs Anti-Ransomware-Schutz oder Data Infrastructure Insights Workload Security geschützt ist. Beachten Sie, dass in der Spalte ONTAP ARP der aktuelle Status des integrierten Anti-Ransomware-Schutzes von ONTAP angezeigt wird, der auf dem ONTAP -System konfiguriert ist. Die Workload-Sicherheit von Data Infrastructure Insights kann durch Auswahl von „Schützen“ in dieser Spalte aktiviert
werden.



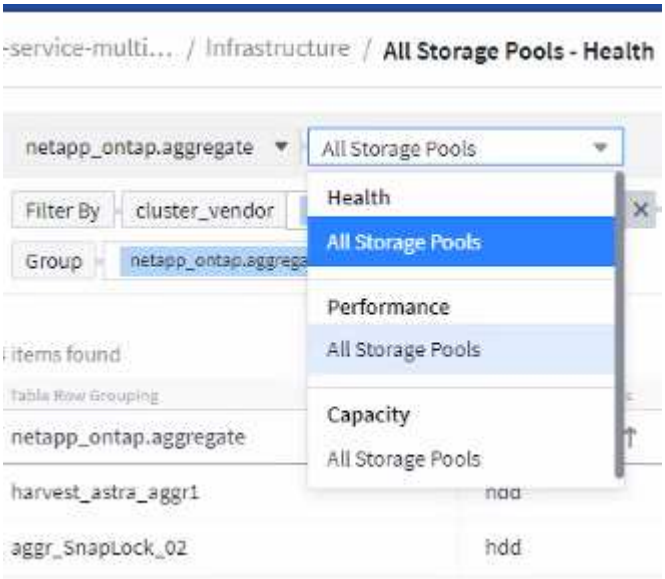
Warnungen

Hier können Sie die aktiven Warnungen Ihres Mandanten anzeigen und schnell auf potenzielle Probleme eingehen. Wählen Sie die Registerkarte „Gelöst“ aus, um behobene Warnungen anzuzeigen.

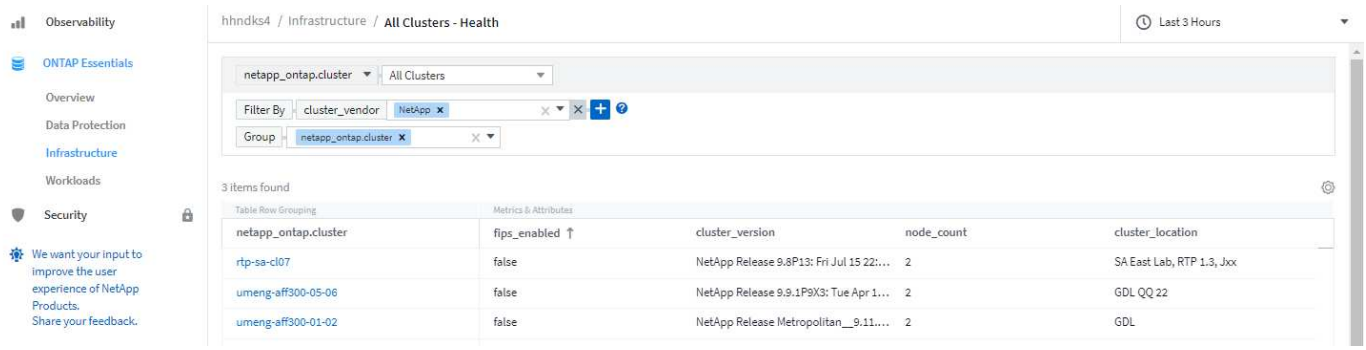


Infrastruktur

Auf der Seite „ONTAP Essentials **Infrastruktur**“ erhalten Sie mithilfe vorgefertigter (und dennoch weiter anpassbarer) Abfragen für alle grundlegenden ONTAP Objekte einen Überblick über den Zustand und die Leistung des Clusters. Wählen Sie den Objekttyp aus, den Sie untersuchen möchten (Cluster, Speicherpool usw.), und entscheiden Sie, ob Sie Informationen zum Zustand oder zur Leistung anzeigen möchten. Setzen Sie Filter, um tiefer in einzelne Systeme einzutauchen.

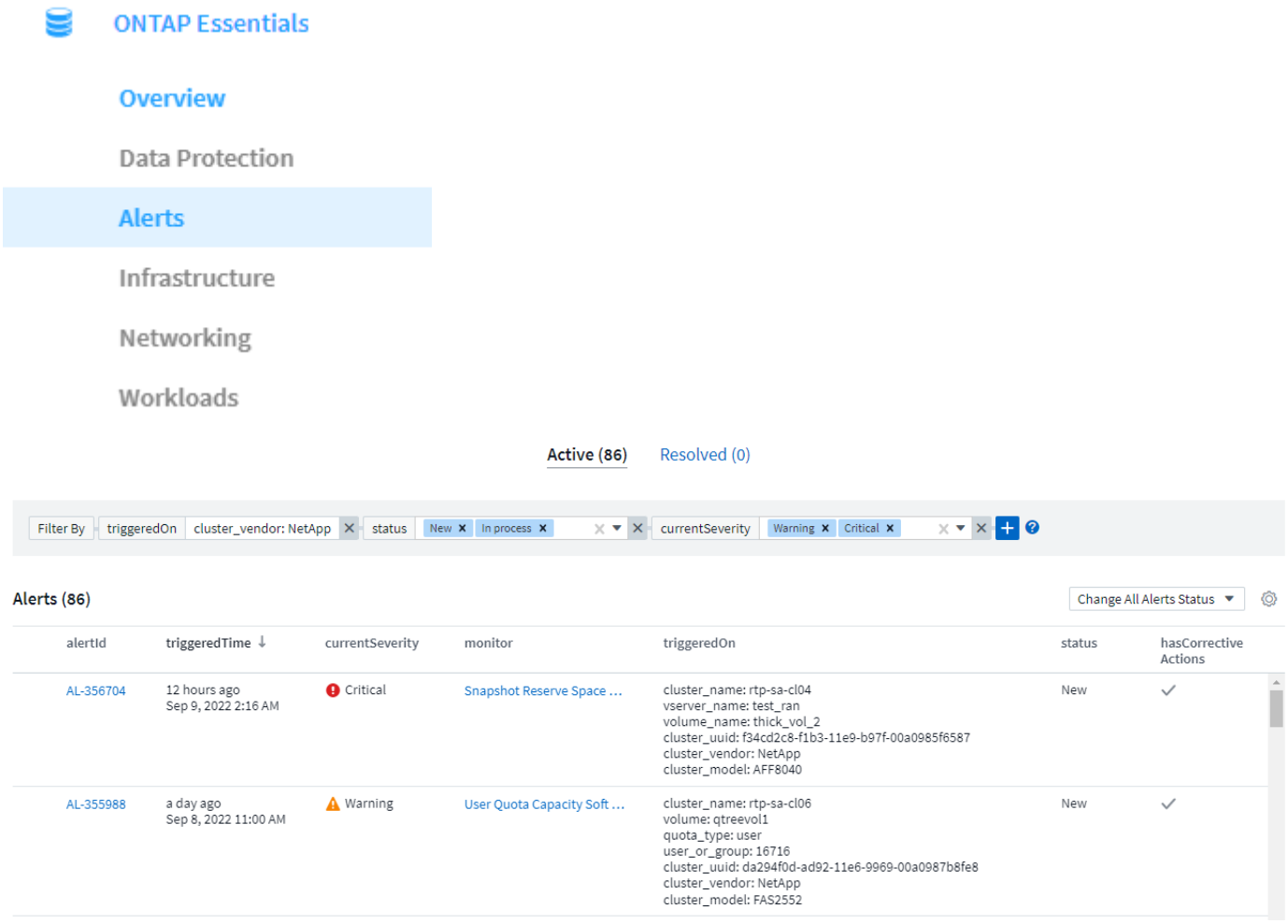


Infrastrukturseite mit Cluster-Integrität:



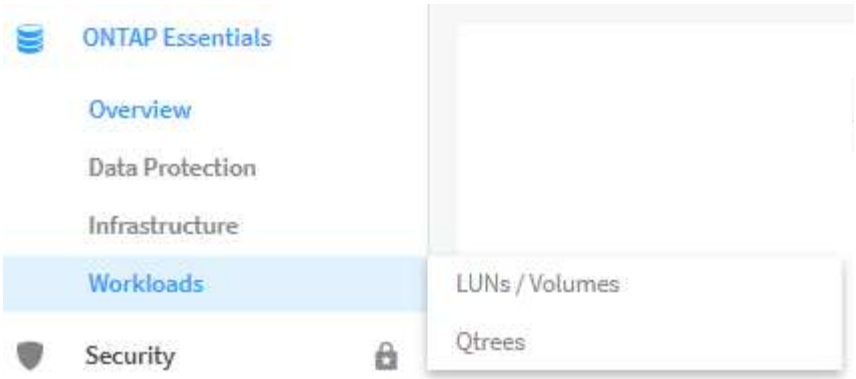
Vernetzung

ONTAP Essentials Networking bietet Ihnen Einblicke in Ihre FC-, NVME FC-, Ethernet- und iSCSI-Infrastruktur. Auf diesen Seiten können Sie Dinge wie Ports in Ihren Clustern und deren Knoten erkunden.



Arbeitslasten

Zeigen Sie Workloads auf LUNs/Volumes, NFS- oder SMB-Freigaben oder Qtrees auf Ihrem Mandanten an und erkunden Sie diese.



netapp_ontap.lun | All LUNs

Filter By | cluster_vendor | NetApp

Group | netapp_ontap.lun

13 items found

Table Row Grouping	Metrics & Attributes								
netapp_ontap.lun	total_late... ↑	total_iops (IO/s)	total_through...	size (B)	size_used (B)	volume	vserver_name	aggregate_name	node
/vol/ste/ste	0.00	0.00	0.00	53,694,627,840....	0.00	ste	vs_test	umeng_aff300...	ui
/vol/kubebug/kubebuglun1	0.00	0.00	0.00	85,905,637,376....	1,489,985,536.00	kubebug	vs_test	umeng_aff300...	ui
/vol/trident_pvc_3ef5a87c_4149_44e8_8113...	0.00	0.00	0.00	1,073,741,824.00	0.00	trident_pvc_3e...	vs_test	umeng_aff300...	ui
/vol/trident_pvc_0bf4ffd4_3f11_4d63_aa01_...	0.00	0.00	0.00	1,073,741,824.00	0.00	trident_pvc_0b...	vs_test	umeng_aff300...	ui
/vol/NSLM_VOL_LUN_1597772263794/matts...	0.00	0.00	0.00	1,073,741,824.00	0.00	NSLM_VOL_LU...	VMware_test	aggr_data_01_...	rt
/vol/mattlun12345/mattlun12345	0.00	0.00	0.00	1,073,741,824.00	0.00	mattlun12345	VMware_test	aggr_data_01_...	rt
/vol/kubebug1/kubebuglun2	0.00	0.00	0.00	85,904,826,368....	0.00	kubebug1	vs_test	umeng_aff300...	ui
/vol/trident_pvc_d66d7f51_a623_4fc3_8cda...	0.00	0.00	0.00	1,073,741,824.00	0.00	trident_pvc_d6...	vs_test	umeng_aff300...	ui
/vol/Rah/Rah	0.00	0.00	0.00	57,576,960.00	0.00	Rah	vs_test	umeng_aff300...	ui
/vol/chap_test_lun_vol/chap_test_lun	0.00	0.00	0.00	107,374,182,40...	0.00	chap_test_lun_...	VMware_test	aggr_data_01_...	rt
/vol/windows_iscsi_example/windows_iscsi...	0.00	0.00	1.04	1,073,741,824.00	10,911,744.00	windows_iscsi...	VMware_test	aggr_data_01_...	rt
/vol/vol_test/lun1	0.04	0.10	0.00	1,073,741,824.00	0.00	vol_test	vs_test	umeng_aff300...	ui
/vol/osc_iscsi_vol01/osc_iscsi_vol01	2.11	116.83	2,737,374.33	4,398,046,511,1...	2,535,381,008,3...	osc_iscsi_vol01	osc	umeng_aff300...	ui

Admin und andere Aufgaben

API für Data Infrastructure Insights

Die Data Infrastructure Insights API ermöglicht NetApp Kunden und unabhängigen Softwareanbietern (ISVs) , Data Infrastructure Insights in andere Anwendungen wie CMDBs oder andere Ticketsysteme zu integrieren.

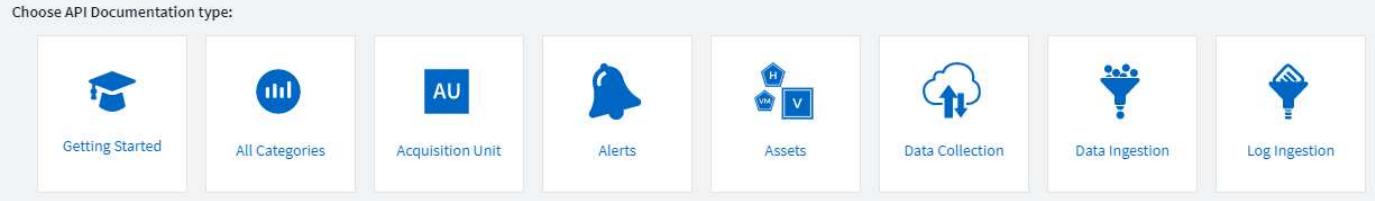
Data Infrastructure Insights"Feature-Set-Rolle" bestimmt, auf welche APIs Sie zugreifen können. Die Rollen „Benutzer“ und „Gast“ verfügen über weniger Berechtigungen als die Rolle „Administrator“. Wenn Sie beispielsweise in Monitor und Optimize die Administratorrolle haben, in Reporting jedoch die Benutzerrolle, können Sie alle API-Typen außer Data Warehouse verwalten.

Voraussetzungen für den API-Zugriff

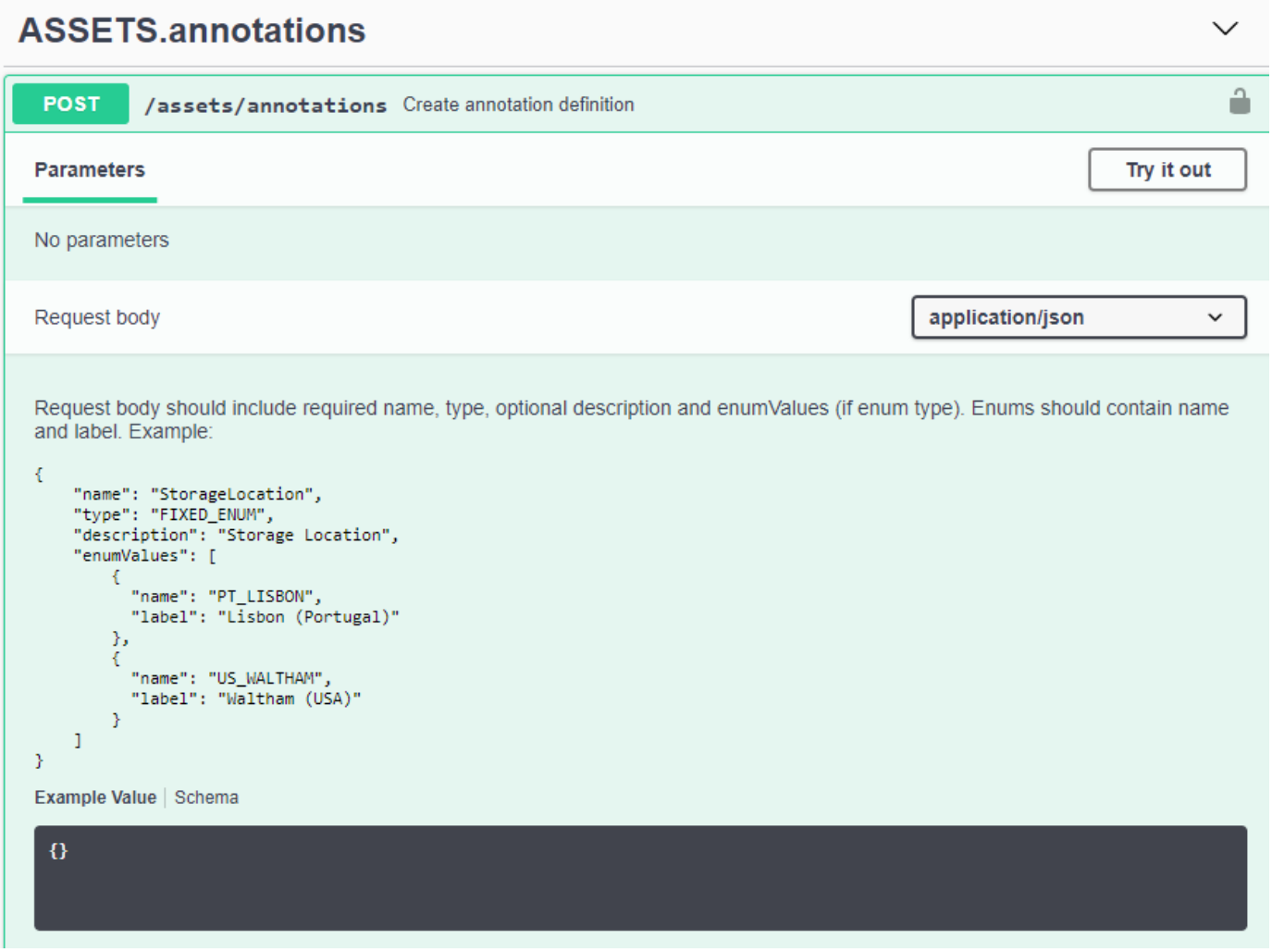
- Zum Gewähren des Zugriffs wird ein API-Zugriffstokenmodell verwendet.
- Die API-Token-Verwaltung wird von Data Infrastructure Insights -Benutzern mit der Administratorrolle durchgeführt.

API-Dokumentation (Swagger)

Die neuesten API-Informationen finden Sie, indem Sie sich bei Data Infrastructure Insights anmelden und zu **Admin > API-Zugriff** navigieren. Klicken Sie auf den Link **API-Dokumentation**.



Die API-Dokumentation basiert auf Swagger und bietet eine kurze Beschreibung und Nutzungsinformationen zur API. Sie können sie in Ihrem Mandanten ausprobieren. Je nach Ihrer Benutzerrolle und/oder Data Infrastructure Insights -Edition können die für Sie verfügbaren API-Typen variieren.



API-Zugriffstoken

Bevor Sie die Data Infrastructure Insights API verwenden, müssen Sie ein oder mehrere **API-Zugriffstoken** erstellen. Zugriffstoken werden für bestimmte API-Typen verwendet und können Lese- und/oder Schreibberechtigungen erteilen. Sie können auch das Ablaufdatum für jedes Zugriffstoken festlegen. Alle APIs unter den angegebenen Typen sind für das Zugriffstoken gültig. Für jedes Token ist weder ein Benutzername noch ein Passwort erforderlich.

So erstellen Sie ein Zugriffstoken:

- Klicken Sie auf **Admin > API-Zugriff**
- Klicken Sie auf **+API-Zugriffstoken**
  - Geben Sie den Tokennamen ein
  - API-Typen auswählen
  - Geben Sie die für diesen API-Zugriff erteilten Berechtigungen an
  - Token-Ablauf festlegen

Ihr Token steht Ihnen während des Erstellungsprozesses nur zum Kopieren in die Zwischenablage und zum Speichern zur Verfügung. Token können nach ihrer Erstellung nicht abgerufen werden. Es wird daher dringend empfohlen, das Token zu kopieren und an einem sicheren Ort zu speichern. Sie werden aufgefordert, auf die Schaltfläche **API-Zugriffstoken kopieren** zu klicken, bevor Sie den Bildschirm zur Token-Erstellung schließen können.

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

Token gewähren aus Kundensicht allgemeinen Zugriff auf APIs und verwalten den Zugriff auf APIs im Rahmen ihres eigenen Mandanten. Kundenadministratoren können diese Token ohne direkte Beteiligung des Back-End-Personals von Data Infrastructure Insights erteilen und widerrufen.

Die Anwendung erhält ein Zugriffstoken, nachdem ein Benutzer den Zugriff erfolgreich authentifiziert und autorisiert hat, und übergibt das Zugriffstoken dann als Anmeldeinformation, wenn sie die Ziel-API aufruft. Das übergebene Token informiert die API darüber, dass der Inhaber des Tokens autorisiert wurde, auf die API zuzugreifen und bestimmte Aktionen auszuführen, die durch den bei der Autorisierung gewährten Umfang festgelegt sind.

Der HTTP-Header, an den das Zugriffstoken übergeben wird, ist **X-CloudInsights-ApiKey:**.

Verwenden Sie beispielsweise Folgendes, um Speicherressourcen abzurufen:

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

Auf den Swagger-Seiten finden Sie Beispiele speziell für die API, die Sie verwenden möchten.

API-Typ

Die Data Infrastructure Insights API ist kategoriebasiert und enthält derzeit die folgenden Typen:

- Der Typ ASSETS enthält Asset-, Abfrage- und Such-APIs.
  - Assets: Listen Sie Objekte der obersten Ebene auf und rufen Sie ein bestimmtes Objekt oder eine Objekthierarchie ab.
  - Abfrage: Rufen Sie Data Infrastructure Insights -Abfragen ab und verwalten Sie sie.
  - Importieren: Annotationen oder Anwendungen importieren und Objekten zuordnen
  - Suche: Suchen Sie ein bestimmtes Objekt, ohne die eindeutige ID oder den vollständigen Namen des Objekts zu kennen.
- Der Typ DATA COLLECTION wird zum Abrufen und Verwalten von Datensammlern verwendet.
- Der Typ DATA INGESTION wird zum Abrufen und Verwalten von Aufnahmedaten und benutzerdefinierten Metriken verwendet, beispielsweise von Telegraf-Agenten
- LOG INGESTION dient zum Abrufen und Verwalten von Protokolldaten

Im Laufe der Zeit werden möglicherweise weitere Typen und/oder APIs verfügbar. Die aktuellsten API-Informationen finden Sie im"API Swagger-Dokumentation" .

Beachten Sie, dass die API-Typen, auf die ein Benutzer Zugriff hat, auch von der"Benutzerrolle" Sie verfügen

über jeden Data Infrastructure Insights Funktionssatz (Überwachung, Workload-Sicherheit, Berichterstellung).

Bestandsdurchlauf

In diesem Abschnitt wird beschrieben, wie Sie eine Hierarchie von Data Infrastructure Insights -Objekten durchlaufen.

Objekte der obersten Ebene

Einzelne Objekte werden in Anfragen durch eine eindeutige URL (in JSON „self“ genannt) identifiziert und erfordern die Kenntnis des Objekttyps und der internen ID. Für einige der Objekte der obersten Ebene (Hosts, Speicher usw.) bietet die REST-API Zugriff auf die gesamte Sammlung.

Das allgemeine Format einer API-URL ist:

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

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

Untergeordnete Elemente und zugehörige Objekte

Objekte der obersten Ebene, wie z. B. Speicher, können zum Durchlaufen anderer untergeordneter und verwandter Objekte verwendet werden. Um beispielsweise alle Datenträger für einen bestimmten Speicher abzurufen, verketten Sie die Speicher-URL „self“ mit „/disks“, zum Beispiel:

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

Erweitert

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

Der einzige gemeinsame Erweiterungsparameter ist *expands*. Die Antwort enthält eine Liste aller verfügbaren spezifischen Erweiterungen für das Objekt.

Wenn Sie beispielsweise Folgendes anfordern:

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

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

Jede Erweiterung enthält Daten, eine URL oder beides. Der Expand-Parameter unterstützt mehrere und verschachtelte Attribute, zum Beispiel:

```
 https://<tenant>/rest/v1/assets/storages/2782?expand=performance,storageR
esources.storage
Mit „Erweitern“ können Sie viele verwandte Daten in einer Antwort
einbringen.  NetApp empfiehlt, nicht zu viele Informationen auf einmal
anzufordern, da dies zu Leistungseinbußen führen kann.
```

Um dies zu verhindern, können Anfragen für Sammlungen der obersten Ebene nicht erweitert werden. Sie können beispielsweise nicht für alle Speicherobjekte gleichzeitig erweiterte Daten anfordern. Clients müssen die Objektliste abrufen und dann bestimmte Objekte zum Erweitern auswählen.

Leistungsdaten

Leistungsdaten werden über viele Geräte hinweg als separate Stichproben erfasst. Jede Stunde (Standardeinstellung) aggregiert und fasst Data Infrastructure Insights Leistungsbeispiele zusammen.

Die API ermöglicht den Zugriff sowohl auf die Beispiele als auch auf die zusammengefassten Daten. Für ein Objekt mit Leistungsdaten ist eine Leistungszusammenfassung als *expand=performance* verfügbar. Zeitreihen zur Leistungshistorie sind über verschachtelte *expand=performance.history* verfügbar.

Beispiele für Leistungsdatenobjekte sind:

- Speicherleistung
- Speicherpoolleistung
- PortPerformance
- DiskPerformance

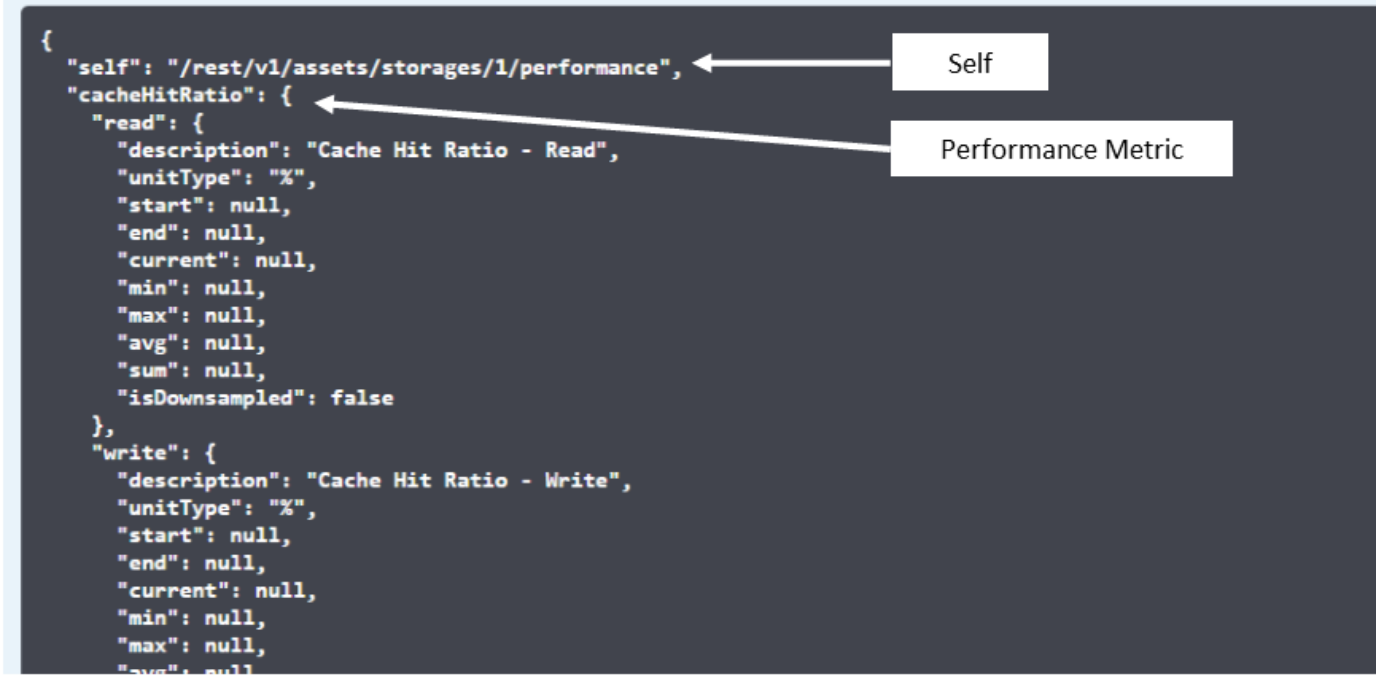
Eine Leistungsmetrik hat eine Beschreibung und einen Typ und enthält eine Sammlung von Leistungszusammenfassungen. Zum Beispiel Latenz, Verkehr und Rate.

Eine Leistungszusammenfassung enthält eine Beschreibung, eine Einheit, eine Beispielstartzeit, eine Beispielendzeit und eine Sammlung zusammengefasster Werte (aktuell, Min., Max., Durchschnitt usw.), die aus einem einzelnen Leistungsindikator über einen Zeitraum (1 Stunde, 24 Stunden, 3 Tage usw.) berechnet wurden.

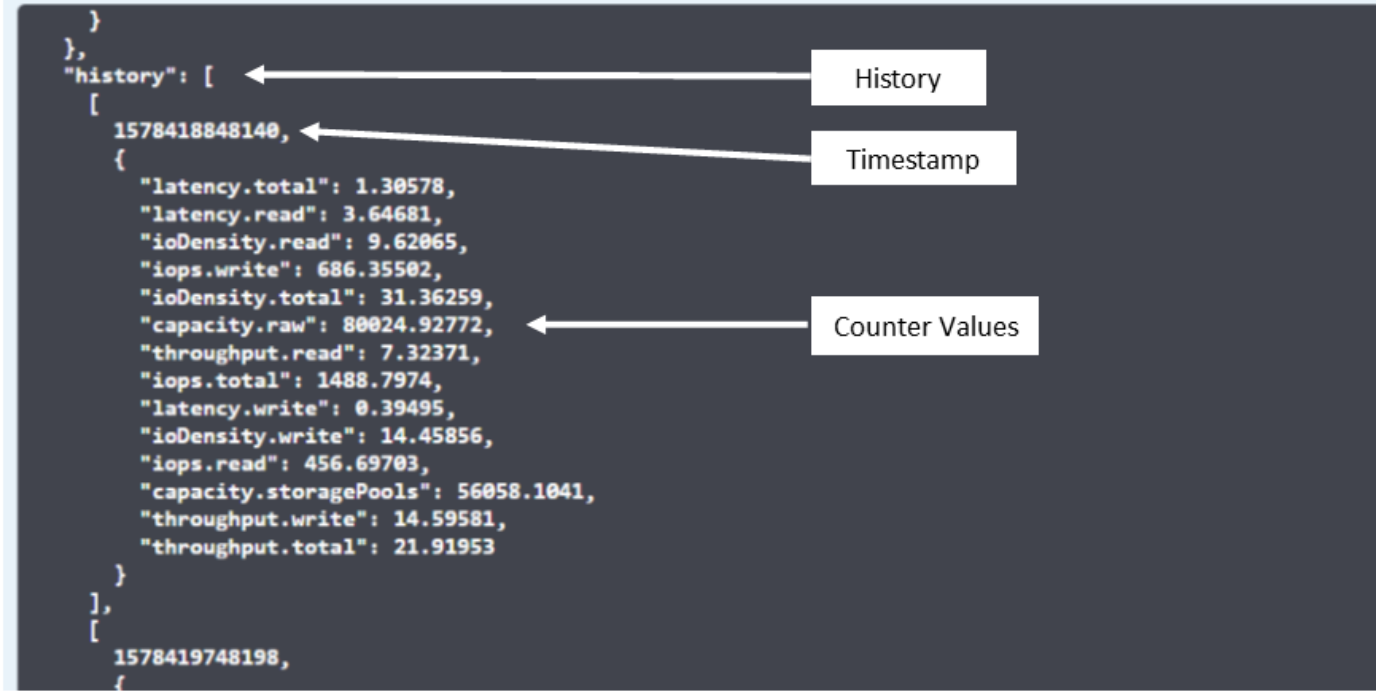
https://tenant.cloudinsights.netapp.com/rest/v1/assets/storages/1/performance?expand=history

Details

Response body



Response body



Das resultierende Leistungsdatenwörterbuch enthält die folgenden Schlüssel:

- „self“ ist die eindeutige URL des Objekts

- „History“ ist die Liste der Paare aus Zeitstempel und Zuordnung der Zählerwerte
- Jeder andere Wörterbuchschlüssel („diskThroughput“ usw.) ist der Name einer Leistungsmetrik.

Jeder Leistungsdatenobjekttyp verfügt über einen einzigartigen Satz von Leistungsmetriken. Beispielsweise unterstützt das Leistungsobjekt „Virtuelle Maschine“ „diskThroughput“ als Leistungsmetrik. Jede unterstützte Leistungsmetrik gehört zu einer bestimmten „Leistungskategorie“, die im Metrikwörterbuch dargestellt wird. Data Infrastructure Insights unterstützt mehrere Leistungsmetriktypen, die weiter unten in diesem Dokument aufgeführt sind. Jedes Leistungsmetrikwörterbuch verfügt außerdem über das Feld „Beschreibung“, das eine für Menschen lesbare Beschreibung dieser Leistungsmetrik und eine Reihe von Leistungszusammenfassungszählereinträgen enthält.

Der Leistungszusammenfassungszähler ist die Zusammenfassung der Leistungszähler. Es werden typische aggregierte Werte wie Min., Max. und Durchschnitt für einen Zähler sowie der zuletzt beobachtete Wert, der Zeitbereich für zusammengefasste Daten, der Einheitentyp für den Zähler und Schwellenwerte für Daten angezeigt. Nur Schwellenwerte sind optional; die restlichen Attribute sind obligatorisch.

Für die folgenden Zählertypen sind Leistungszusammenfassungen verfügbar:

- Lesen – Zusammenfassung für Lesevorgänge
- Schreiben – Zusammenfassung für Schreibvorgänge
- Gesamt – Zusammenfassung aller Vorgänge. Es kann höher sein als die einfache Summe aus Lesen und Schreiben und es können auch andere Operationen enthalten sein.
- Gesamtmaximum – Zusammenfassung aller Vorgänge. Dies ist der maximale Gesamtwert im angegebenen Zeitraum.

Objektleistungsmetriken

Die API kann detaillierte Metriken für Objekte auf Ihrem Mandanten zurückgeben, zum Beispiel:

- Speicherleistungsmetriken wie IOPS (Anzahl der Eingabe-/Ausgabeanforderungen pro Sekunde), Latenz oder Durchsatz.
- Switch-Leistungsmetriken, wie etwa Verkehrsauslastung, BB Credit Zero-Daten oder Portfehler.

Siehe die"API Swagger-Dokumentation" für Informationen zu Metriken für jeden Objekttyp.

Leistungsverlaufsdaten

Verlaufsdaten werden in Leistungsdaten als Liste von Zeitstempel- und Zählerkartenpaaren dargestellt.

Die Benennung der Verlaufszähler basiert auf dem Namen des Leistungsmetrikobjekts. Beispielsweise unterstützt das Leistungsobjekt der virtuellen Maschine „diskThroughput“, sodass die Verlaufskarte Schlüssel mit den Namen „diskThroughput.read“, „diskThroughput.write“ und „diskThroughput.total“ enthält.

Der Zeitstempel liegt im UNIX-Zeitformat vor.

Nachfolgend sehen Sie ein Beispiel für die Leistungsdaten einer Festplatte im JSON-Format:

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


Objekte mit Kapazitätsattributen

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

KapazitätArtikel

CapacityItem ist eine einzelne logische Kapazitätseinheit. Es verfügt über „Wert“ und „hoher Schwellenwert“ in Einheiten, die durch sein übergeordnetes Objekt definiert sind. Es unterstützt auch eine optionale Aufschlüsselungskarte, die erklärt, wie der Kapazitätswert aufgebaut ist. Beispielsweise wäre die Gesamtkapazität eines 100-TB-Speicherpools ein CapacityItem mit dem Wert 100. Die Aufschlüsselung kann ergeben, dass 60 TB für „Daten“ und 40 TB für „Schnappschüsse“ vorgesehen sind.

Hinweis: „highThreshold“ stellt systemdefinierte Schwellenwerte für die entsprechenden Metriken dar, die ein Client verwenden kann, um Warnungen oder visuelle Hinweise auf Werte zu generieren, die außerhalb der akzeptablen konfigurierten Bereiche liegen.

Im Folgenden wird die Kapazität für StoragePools mit mehreren Kapazitätszählern angezeigt:

Verwenden der Suche zum Nachschlagen von Objekten

Die Such-API ist ein einfacher Einstiegspunkt in das System. Der einzige Eingabeparameter für die API ist eine Zeichenfolge in freier Form und das resultierende JSON enthält eine kategorisierte Ergebnisliste. Typen sind verschiedene Asset-Typen aus dem Inventar, wie Speicher, Hosts, Datenspeicher usw. Jeder Typ würde eine Liste von Objekten des Typs enthalten, die den Suchkriterien entsprechen.

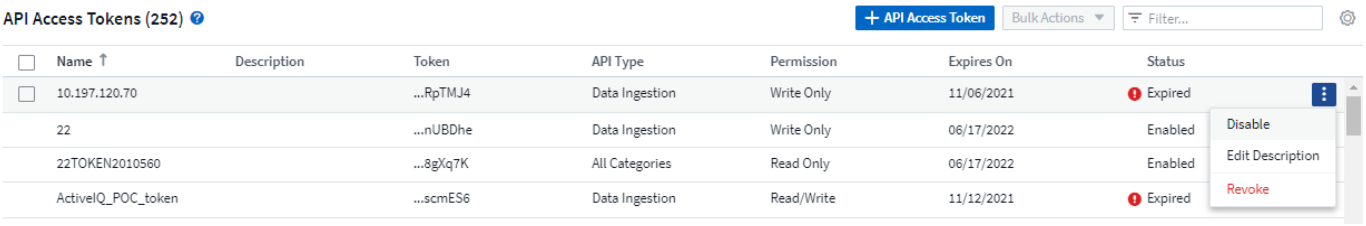
Data Infrastructure Insights ist eine erweiterbare (weit offene) Lösung, die Integrationen mit Orchestrierungs-, Geschäftsverwaltungs-, Änderungskontroll- und Ticketsystemen von Drittanbietern sowie benutzerdefinierte CMDB-Integrationen ermöglicht.

Die RESTful-API von Cloud Insight ist ein primärer Integrationspunkt, der eine einfache und effektive Datenübertragung ermöglicht und Benutzern einen nahtlosen Zugriff auf ihre Daten ermöglicht.

Deaktivieren oder Widerrufen eines API-Tokens

Um ein API-Token vorübergehend zu deaktivieren, klicken Sie auf der API-Token-Listenseite auf das Menü mit den drei Punkten für die API und wählen Sie *Deaktivieren*. Sie können das Token jederzeit wieder aktivieren, indem Sie im selben Menü „Aktivieren“ auswählen.

Um ein API-Token dauerhaft zu entfernen, wählen Sie im Menü „Widerrufen“ aus. Sie können ein widerrufenes Token nicht erneut aktivieren. Sie müssen ein neues Token erstellen.



Rotieren abgelaufener API-Zugriffstoken

API-Zugriffstoken haben ein Ablaufdatum. Wenn ein API-Zugriffstoken abläuft, müssen Benutzer ein neues Token (vom Typ *Data Ingestion* mit Lese-/Schreibberechtigungen) generieren und Telegraf neu konfigurieren, um das neu generierte Token anstelle des abgelaufenen Tokens zu verwenden. Die folgenden Schritte beschreiben die Vorgehensweise im Detail.

Kubernetes

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

Hinweis: Wenn Sie den neuesten NetApp Kubernetes Monitoring Operator installiert haben und ein erneuerbares API-Zugriffstoken verwenden, werden ablaufende Token automatisch durch neue/aktualisierte API-Zugriffstoken ersetzt. Es ist nicht erforderlich, die unten aufgeführten manuellen Schritte auszuführen.

- Erstellen Sie ein neues API-Token.
- Befolgen Sie die Schritte für"Manuelles Upgrade" und wählen Sie das neue API-Token aus.

Hinweis: Kunden, die ihren NetApp Kubernetes Monitoring Operator mit einem Konfigurationsverwaltungstool wie Kustomize verwalten, können dieselben Schritte ausführen, um einen aktualisierten Satz von YAMLs zu generieren und herunterzuladen, um ihn in ihr Repository zu übertragen.

RHEL/CentOS und Debian/Ubuntu

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

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

```
sudo systemctl restart telegraf
```

Windows

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

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

- Starten Sie Telegraf neu.

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

Überwachung Ihrer Umgebung

Wirtschaftsprüfung

Um sowohl erwartete (zur Nachverfolgung) als auch unerwartete (zur Fehlerbehebung) Änderungen zu identifizieren, können Sie einen Prüfpfad der Data Infrastructure Insights -Systemereignisse und Benutzeraktivitäten anzeigen.

Anzeigen überwachter Ereignisse

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

- **Zeit** – Datum und Uhrzeit des Ereignisses oder der Aktivität
- **Benutzer** – Der Benutzer, der die Aktivität initiiert hat
- **Rolle** – Die Rolle des Benutzers in Data Infrastructure Insights (Gast, Benutzer, Administrator)
- **IP** – Die mit dem Ereignis verknüpfte IP-Adresse
- **Aktion** – Art der Aktivität, z. B. Anmelden, Erstellen, Aktualisieren
- **Kategorie** - Die Kategorie der Aktivität
- **Details** - Details der Aktivität

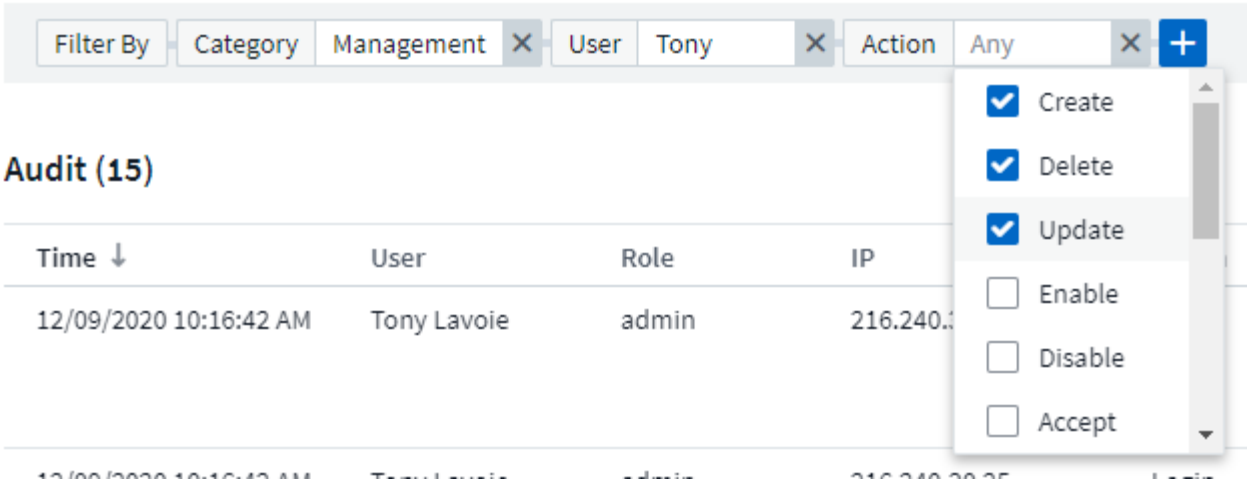
Anzeigen von Auditeinträgen

Es gibt verschiedene Möglichkeiten, Auditeinträge anzuzeigen:

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

  Standardmäßig zeigt die Tabelle die Einträge in absteigender zeitlicher Reihenfolge an.

- Mithilfe der Filterfelder können Sie sich in der Tabelle nur die gewünschten Einträge anzeigen lassen. Klicken Sie auf die Schaltfläche [+], um weitere Filter hinzuzufügen.



Mehr zum Filtern

Sie können Ihren Filter mit den folgenden Optionen verfeinern:

Filter	Was es bewirkt	Beispiel	Ergebnis
* (Sternchen)	ermöglicht Ihnen die Suche nach allem	vol*rhel	gibt alle Ressourcen zurück, die mit „vol“ beginnen und mit „rhel“ enden
? (Fragezeichen)	ermöglicht die Suche nach einer bestimmten Anzahl von Zeichen	BOS-PRD??-S12	gibt BOS-PRD***12***-S12, BOS-PRD***23***-S12 usw. zurück
ODER	ermöglicht Ihnen die Angabe mehrerer Entitäten	FAS2240 ODER CX600 ODER FAS3270	gibt einen der folgenden Werte zurück: FAS2440, CX600 oder FAS3270
NICHT	ermöglicht es Ihnen, Text aus den Suchergebnissen auszuschließen	NICHT EMV*	gibt alles zurück, was nicht mit "EMC" beginnt
Keiner	sucht nach Leerzeichen/NULL/Keine in jedem ausgewählten Feld	*Keiner*	gibt Ergebnisse zurück, bei denen das Zielfeld nicht leer ist
Nicht *	wie bei *Keine* oben, aber Sie können dieses Formular auch verwenden, um nach NULL-Werten in *Nur-Text* -Feldern zu suchen	Nicht *	gibt Ergebnisse zurück, bei denen das Zielfeld nicht leer ist.
""	sucht nach einer genauen Übereinstimmung	"NetApp*"	gibt Ergebnisse zurück, die die exakte Zeichenfolge *NetApp** enthalten

Wenn Sie eine Filterzeichenfolge in doppelte Anführungszeichen setzen, behandelt Insight alles zwischen dem

ersten und letzten Anführungszeichen als exakte Übereinstimmung. Alle Sonderzeichen oder Operatoren innerhalb der Anführungszeichen werden als Literale behandelt. Wenn Sie beispielsweise nach „*“ filtern, werden Ergebnisse zurückgegeben, die ein Sternchen sind. Das Sternchen wird in diesem Fall nicht als Platzhalter behandelt. Die Operatoren OR und NOT werden auch als Literalzeichenfolgen behandelt, wenn sie in doppelte Anführungszeichen eingeschlossen sind.

Überwachte Ereignisse und Aktionen

Die von Data Infrastructure Insights geprüften Ereignisse und Aktionen können in die folgenden allgemeinen Bereiche eingeteilt werden:

- **Benutzerkonto**: Anmelden, Abmelden, Rollenwechsel usw.
- **Erfassungseinheit**: erstellen, löschen usw.

  Beispiel: *Erfassungseinheit **AU-Boston-1** entfernt*.

- **Datensammler**: hinzufügen, entfernen, ändern, verschieben/fortsetzen, Erfassungseinheit ändern, starten/stoppen usw.

  Beispiel: *Datenquelle * FlexPod Lab* entfernt, Anbieter * NetApp*, Modell * ONTAP Data Management Software*, IP **192.168.106.5***.

- **Anwendung**: hinzufügen, Objekt zuweisen, entfernen usw.

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

- **Annotation**: Hinzufügen, Zuweisen, Entfernen, Aktionen für Annotationsregeln, Änderungen von Annotationswert usw.

  Beispiel: *Annotationswert **Boston** zum Annotationtyp **SalesOffice*** hinzugefügt.

- **Abfrage**: hinzufügen, entfernen usw.

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

- **Monitor**: hinzufügen, entfernen usw.

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

- **Benachrichtigung**: E-Mail ändern usw.

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

Exportieren von Audit-Ereignissen

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

Schritte

1. Legen Sie auf der Seite „Audit“ den gewünschten Zeitraum und alle gewünschten Filter fest. Data Infrastructure Insights exportiert nur die Audit-Einträge, die der von Ihnen festgelegten Filterung und Zeitspanne entsprechen.
2. Klicken Sie auf die Schaltfläche _Exportieren_ oben rechts in der Tabelle.

Die angezeigten Audit-Ereignisse werden in eine CSV-Datei mit maximal 10.000 Zeilen exportiert.

Aufbewahrung von Prüfdaten

Die Dauer der Aufbewahrung von Audit-Daten Data Infrastructure Insights hängt von Ihrem Abonnement ab:

- Testumgebungen: Auditdaten werden 30 Tage lang aufbewahrt
- Abonnierte Umgebungen: Auditdaten werden 1 Jahr plus 1 Tag aufbewahrt

Prüfeinträge, die älter als die Aufbewahrungsdauer sind, werden automatisch gelöscht. Es ist keine Benutzerinteraktion erforderlich.

Prüfeinträge, die älter als die Aufbewahrungsdauer sind, werden automatisch gelöscht. Es ist keine Benutzerinteraktion erforderlich.

Fehlerbehebung

Hier finden Sie Vorschläge zur Behebung von Problemen mit Audit.

Problem:	Versuchen Sie Folgendes:
Ich sehe Audit-Meldungen, die mir mitteilen, dass ein Monitor exportiert wurde.	Der Export einer benutzerdefinierten Monitorkonfiguration wird normalerweise von NetApp -Ingenieuren während der Entwicklung und Prüfung neuer Funktionen verwendet. Wenn Sie diese Meldung nicht erwartet haben, prüfen Sie bitte die Aktionen des in der geprüften Aktion genannten Benutzers oder wenden Sie sich an den Support.

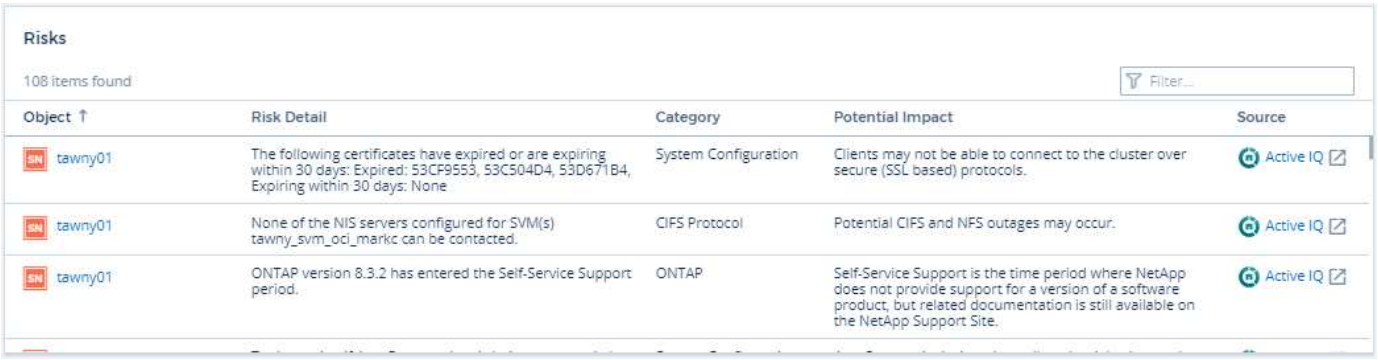
Active IQ Digital Advisor

NetApp"Active IQ Digital Advisor" (auch bekannt als Digital Advisor) bietet NetApp -Kunden eine Reihe von Visualisierungen, Analysen und anderen Support-bezogenen Diensten für ihre Hardware-/Softwaresysteme. Die von Digital Advisor gemeldeten Daten können die Fehlerbehebung bei Systemproblemen verbessern und außerdem Einblicke in die Optimierung und prädiktive Analyse Ihrer Geräte bieten.

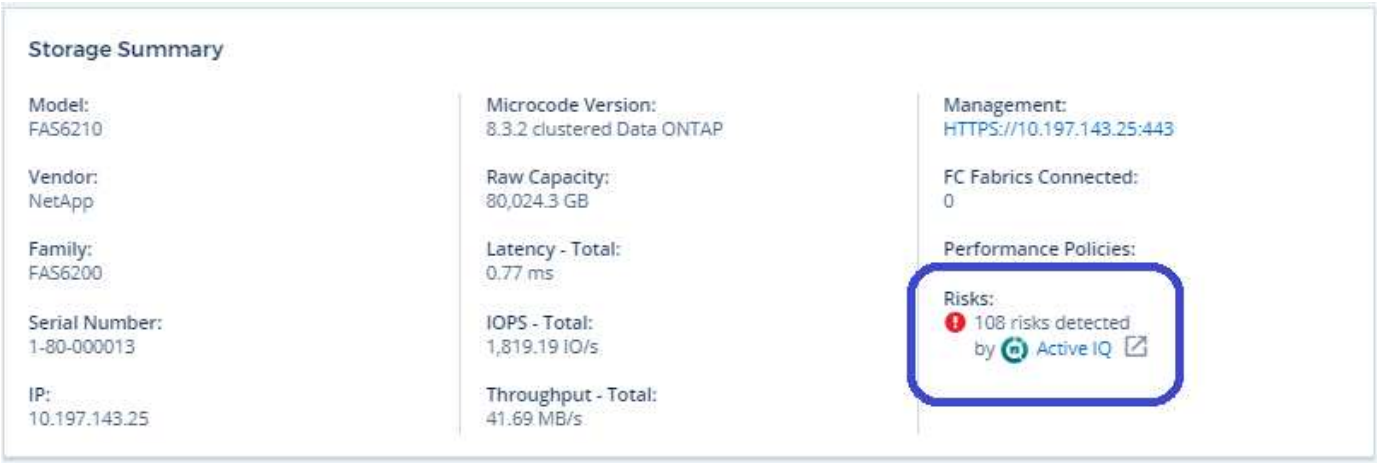
Data Infrastructure Insights sammelt die **Risiken** für jedes NetApp Clustered Data ONTAP -Speichersystem, das von Digital Advisor überwacht und gemeldet wird. Für die Speichersysteme gemeldete Risiken werden von Data Infrastructure Insights im Rahmen der Datenerfassung von diesen Geräten automatisch erfasst. Sie müssen den entsprechenden Datensammler zu Data Infrastructure Insights hinzufügen, um Risikoinformationen zu Digital Advisor zu sammeln.

Data Infrastructure Insights zeigt keine Risikodaten für ONTAP -Systeme an, die nicht von Digital Advisor überwacht und gemeldet werden.

Die gemeldeten Risiken werden in Data Infrastructure Insights auf den Zielseiten der Assets „Storage“ und „Storage Node“ in der Tabelle „Risiken“ angezeigt. Die Tabelle zeigt Risikodetails, Risikokategorie und potenzielle Auswirkungen des Risikos und bietet außerdem einen Link zur Digital Advisor -Seite, auf der alle Risiken für den Speicherknoten zusammengefasst sind (Anmeldung beim NetApp Support-Konto erforderlich).



Eine Anzahl der gemeldeten Risiken wird auch im Zusammenfassungs-Widget der Zielseite angezeigt, mit einem Link zur entsprechenden Digital Advisor -Seite. Auf einer *Speicher*-Landingpage ist die Anzahl die Summe der Risiken aller zugrunde liegenden Speicherknoten.



Öffnen der Digital Advisor Seite

Wenn Sie auf den Link zu einer Digital Advisor -Seite klicken und derzeit nicht bei Ihrem Digital Advisor -Konto angemeldet sind, müssen Sie die folgenden Schritte ausführen, um die Digital Advisor -Seite für den Speicherknoten anzuzeigen.

1. Klicken Sie im Widget „Zusammenfassung der Data Infrastructure Insights“ oder in der Risikotabelle auf den Link „Digital Advisor“.
2. Sign in bei Ihrem NetApp Support-Konto an. Sie werden direkt zur Speicherknotenseite in Digital Advisor weitergeleitet.

Abfragen nach Risiken

In Data Infrastructure Insights können Sie die Spalte **monitoring.count** zu einer Speicher- oder Speicherknotenabfrage hinzufügen. Wenn das zurückgegebene Ergebnis von Digital Advisor überwachte Speichersysteme umfasst, wird in der Spalte „monitoring.count“ die Anzahl der Risiken für das Speichersystem oder den Knoten angezeigt.

Dashboards

Sie können Widgets erstellen (z. B. Kreisdiagramm-, Tabellen-Widget, Balken-, Säulen-, Streudiagramm- und Einzelwert-Widgets), um Objektrisiken für Speicher und Speicherknoten für NetApp Clustered Data ONTAP Systeme zu visualisieren, die von Digital Advisor überwacht werden. „Objektrisiken“ können in diesen Widgets als Spalte oder Metrik ausgewählt werden, wobei Speicher oder Speicherknoten im Mittelpunkt stehen.

Object Risks by Array

12 items found

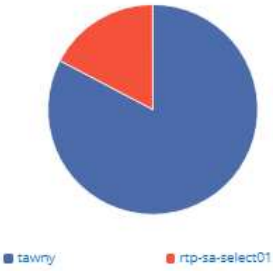
Name	Object Risks
tawny	110
rtp-sa-select01	23
rtp-sa-cl02	N/A
rtp-sa-cl07	N/A
oci-phonehome	N/A
durlabprdsfc01	N/A
oci-3070-01	N/A

Object Risks by Node

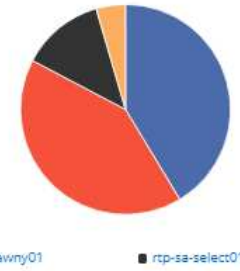
25 items found

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



Object Risks by Storage Node



Total Storage Risks

133.00

Object Risks

Workload-Sicherheit

Informationen zur Speicher-Workload-Sicherheit

Data Infrastructure Insights Storage Workload Security (früher Cloud Secure) hilft Ihnen, Ihre Daten mit verwertbaren Informationen zu Insider-Bedrohungen zu schützen. Es bietet eine zentrale Sichtbarkeit und Kontrolle aller Unternehmensdatenzugriffe in Hybrid-Cloud-Umgebungen, um sicherzustellen, dass Sicherheits- und Compliance-Ziele erreicht werden.

Sichtweite

Erhalten Sie zentrale Transparenz und Kontrolle über den Benutzerzugriff auf Ihre kritischen Unternehmensdaten, die vor Ort oder in der Cloud gespeichert sind.

Ersetzen Sie Tools und manuelle Prozesse, die keinen zeitnahen und genauen Einblick in den Datenzugriff und die Datenkontrolle bieten. Workload Security funktioniert auf einzigartige Weise sowohl auf Cloud- als auch auf lokalen Speichersystemen und warnt Sie in Echtzeit vor böswilligem Benutzerverhalten.

Schutz

Schützen Sie Unternehmensdaten durch fortschrittliches maschinelles Lernen und Anomalieerkennung vor Missbrauch durch böswillige oder kompromittierte Benutzer.

Warnt Sie bei abnormalen Datenzugriffen durch fortschrittliches maschinelles Lernen und Anomalieerkennung des Benutzerverhaltens.

Einhaltung

Stellen Sie die Unternehmenskonformität sicher, indem Sie den Benutzerdatenzugriff auf Ihre kritischen Unternehmensdaten prüfen, die vor Ort oder in der Cloud gespeichert sind.

Erste Schritte

Erste Schritte mit Workload-Sicherheit

Bevor Sie Workload Security zur Überwachung der Benutzeraktivität verwenden können, müssen einige Konfigurationsaufgaben abgeschlossen werden.

Das Workload Security-System verwendet einen Agenten, um Zugriffsdaten von Speichersystemen und Benutzerinformationen von Directory Services-Servern zu sammeln.

Bevor Sie mit der Datenerfassung beginnen können, müssen Sie Folgendes konfigurieren:

Aufgabe	Ähnliche Informationen

Konfigurieren eines Agenten	"Agentenanforderungen" "Agent hinzufügen" "**Video**: Agentenbereitstellung"
Konfigurieren eines Benutzerverzeichnis-Connectors	"Benutzerverzeichnis-Connector hinzufügen" "**Video**: Active Directory-Verbindung"
Konfigurieren von Datensammlern	Klicken Sie auf **Workload-Sicherheit > Collector**. Klicken Sie auf den Datensammler, den Sie konfigurieren möchten. Weitere Informationen finden Sie im Abschnitt „Data Collector Vendor Reference“ der Dokumentation."**Video**: ONTAP SVM-Verbindung"
Benutzerkonten erstellen	"Benutzerkonten verwalten"
Fehlerbehebung	"**Video**: Fehlerbehebung"

Workload Security kann auch in andere Tools integriert werden. Zum Beispiel,"siehe diese Anleitung" zur Integration mit Splunk.

Anforderungen für den Workload Security Agent

Sie müssen"Installieren Sie einen Workload Security Agent" um Informationen von Ihren Datensammlern zu erhalten. Stellen Sie vor der Installation des Agenten sicher, dass Ihre Umgebung die Anforderungen an Betriebssystem, CPU, Arbeitsspeicher und Festplattenspeicher erfüllt.

Komponente	Linux-Anforderungen
Betriebssystem	Ein Computer, auf dem eine lizenzierte Version eines der folgenden Betriebssysteme ausgeführt wird: * AlmaLinux 9.4 (64 Bit) bis 9.5 (64 Bit), 10 (64 Bit), einschließlich SELinux * CentOS Stream 9 (64 Bit) * Debian 11 (64 Bit), 12 (64 Bit), einschließlich SELinux * OpenSUSE Leap 15.3 (64 Bit) bis 15.6 (64 Bit) * Oracle Linux 8.10 (64 Bit), 9.1 (64 Bit) bis 9.6 (64 Bit), einschließlich SELinux * Red Hat Enterprise Linux 8.10 (64 Bit), 9.1 (64 Bit) bis 9.6 (64 Bit), 10 (64 Bit), einschließlich SELinux * Rocky 9.4 (64 Bit) bis 9.6 (64 Bit), einschließlich SELinux * SUSE Linux Enterprise Server 15 SP4 (64-Bit) bis 15 SP6 (64-Bit), einschließlich SELinux * Ubuntu 20.04 LTS (64-Bit), 22.04 LTS (64-Bit), 24.04 LTS (64-Bit) Auf diesem Computer sollte keine andere Software auf Anwendungsebene ausgeführt werden. Ein dedizierter Server wird empfohlen.
Befehle	Für die Installation ist „Entpacken“ erforderlich. Darüber hinaus ist der Befehl „sudo su –“ für die Installation, das Ausführen von Skripts und die Deinstallation erforderlich.
CPU	4 CPU-Kerne
Erinnerung	16 GB RAM

Komponente	Linux-Anforderungen
Verfügbarer Speicherplatz	Der Speicherplatz sollte folgendermaßen zugewiesen werden: /opt/netapp 36 GB (mindestens 35 GB freier Speicherplatz nach der Erstellung des Dateisystems). Hinweis: Es wird empfohlen, etwas zusätzlichen Speicherplatz zuzuweisen, um die Erstellung des Dateisystems zu ermöglichen. Stellen Sie sicher, dass im Dateisystem mindestens 35 GB freier Speicherplatz vorhanden sind. Wenn es sich bei /opt um einen bereitgestellten Ordner aus einem NAS-Speicher handelt, stellen Sie sicher, dass lokale Benutzer Zugriff auf diesen Ordner haben. Die Installation des Agenten oder Datensammlers schlägt möglicherweise fehl, wenn lokale Benutzer keine Berechtigung für diesen Ordner haben. Weitere Informationen finden Sie im"Fehlerbehebung" Weitere Einzelheiten finden Sie im Abschnitt „Informationen zur Sicherheit“.
Netzwerk	100 Mbit/s bis 1 Gbit/s Ethernet-Verbindung, statische IP-Adresse, IP-Konnektivität zu allen Geräten und ein erforderlicher Port zur Workload Security-Instanz (80 oder 443).

Bitte beachten: Der Workload Security-Agent kann auf derselben Maschine wie eine Data Infrastructure Insights Erfassungseinheit und/oder ein Agent installiert werden. Es empfiehlt sich jedoch, diese auf separaten Maschinen zu installieren. Falls diese auf derselben Maschine installiert sind, weisen Sie den Speicherplatz wie unten gezeigt zu:

Verfügbarer Speicherplatz	50–55 GB Für Linux sollte der Speicherplatz folgendermaßen zugewiesen werden: /opt/netapp 25–30 GB /var/log/netapp 25 GB

Zusätzliche Empfehlungen

- Es wird dringend empfohlen, die Zeit sowohl auf dem ONTAP -System als auch auf der Agent-Maschine mithilfe von **Network Time Protocol (NTP)** oder **Simple Network Time Protocol (SNTP)** zu synchronisieren.

Cloud-Netzwerkzugriffsregeln

Für **US-basierte** Workload Security-Umgebungen:

Protokoll	Hafen	Quelle	Ziel	Beschreibung
TCP	443	Workload-Sicherheitsagent	<Sitename>.cs01.cloudinsights.netapp.com <Sitename>.c01.cloudinsights.netapp.com <Sitename>.c02.cloudinsights.netapp.com	Zugriff auf Data Infrastructure Insights
TCP	443	Workload-Sicherheitsagent	agentlogin.cs01.cloudinsights.netapp.com	Zugriff auf Authentifizierungsdienste

Für **in Europa ansässige** Workload Security-Umgebungen:

Protokoll	Hafen	Quelle	Ziel	Beschreibung
TCP	443	Workload-Sicherheitsagent	<Sitename>.cs01-eu-1.cloudinsights.netapp.com <Sitename>.c01-eu-1.cloudinsights.netapp.com <Sitename>.c02-eu-1.cloudinsights.netapp.com	Zugriff auf Data Infrastructure Insights
TCP	443	Workload-Sicherheitsagent	agentlogin.cs01-eu-1.cloudinsights.netapp.com	Zugriff auf Authentifizierungsdienste

Für **APAC-basierte** Workload Security-Umgebungen:

Protokoll	Hafen	Quelle	Ziel	Beschreibung
TCP	443	Workload-Sicherheitsagent	<Sitename>.cs01-ap-1.cloudinsights.netapp.com <Sitename>.c01-ap-1.cloudinsights.netapp.com <Sitename>.c02-ap-1.cloudinsights.netapp.com	Zugriff auf Data Infrastructure Insights
TCP	443	Workload-Sicherheitsagent	agentlogin.cs01-ap-1.cloudinsights.netapp.com	Zugriff auf Authentifizierungsdienste

Netzwerkinterne Regeln

Protokoll	Hafen	Quelle	Ziel	Beschreibung
TCP	389 (LDAP) 636 (LDAPs / Start-TLS)	Workload-Sicherheitsagent	LDAP-Server-URL	Mit LDAP verbinden
TCP	443	Workload-Sicherheitsagent	Cluster- oder SVM-Verwaltungs-IP-Adresse (abhängig von der SVM-Collector-Konfiguration)	API-Kommunikation mit ONTAP

Protokoll	Hafen	Quelle	Ziel	Beschreibung
TCP	35000 - 55000	SVM-Daten-LIF-IP-Adressen	Workload-Sicherheitsagent	Kommunikation von ONTAP an den Workload Security Agent für Fpolicy-Ereignisse. Diese Ports müssen für den Workload Security Agent geöffnet werden, damit ONTAP Ereignisse an ihn senden kann, einschließlich einer Firewall auf dem Workload Security Agent selbst (sofern vorhanden). BEACHTEN Sie, dass Sie nicht **alle** dieser Ports reservieren müssen, aber die Ports, die Sie dafür reservieren, müssen innerhalb dieses Bereichs liegen. Es wird empfohlen, zunächst etwa 100 Ports zu reservieren und diese bei Bedarf zu erhöhen.

Protokoll	Hafen	Quelle	Ziel	Beschreibung
TCP	35000-55000	Cluster-Verwaltungs-IP	Workload-Sicherheitsagent	Kommunikation von der ONTAP Cluster Management IP zum Workload Security Agent für **EMS-Ereignisse**. Diese Ports müssen für den Workload Security Agent geöffnet werden, damit ONTAP **EMS-Ereignisse** an ihn senden kann, einschließlich einer Firewall auf dem Workload Security Agent selbst (sofern vorhanden). BEACHTEN Sie, dass Sie nicht **alle** dieser Ports reservieren müssen, aber die Ports, die Sie dafür reservieren, müssen innerhalb dieses Bereichs liegen. Es wird empfohlen, zunächst etwa 100 Ports zu reservieren und diese bei Bedarf zu erhöhen.
SSH	22	Workload-Sicherheitsagent	Clusterverwaltung	Wird für die CIFS/SMB-Benutzerblockierung benötigt.

Systemdimensionierung

Siehe die"Event-Raten-Checker" Informationen zur Größenbestimmung finden Sie in der Dokumentation.

Installation des Workload Security Agent

Workload Security (früher Cloud Secure) sammelt Benutzeraktivitätsdaten mithilfe eines oder mehrerer Agenten. Agenten stellen eine Verbindung zu Geräten auf Ihrem Mandanten her und erfassen Daten, die zur Analyse an die Workload Security SaaS-Schicht gesendet werden. Sehen"Agentenanforderungen" um eine Agent-VM zu konfigurieren.

Bevor Sie beginnen

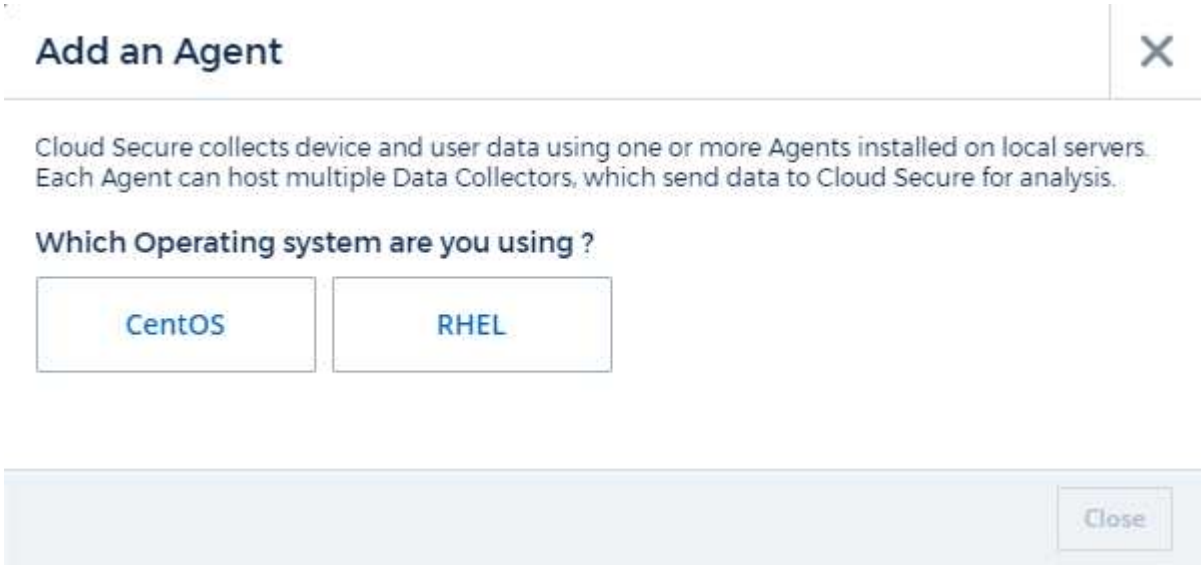
- Für die Installation, das Ausführen von Skripts und die Deinstallation ist das Sudo-Privileg erforderlich.
- Während der Installation des Agenten werden auf dem Computer ein lokaler Benutzer *cssys* und eine lokale Gruppe *cssys* erstellt. Wenn die Berechtigungseinstellungen die Erstellung eines lokalen Benutzers nicht zulassen und stattdessen Active Directory erfordern, muss auf dem Active Directory-Server ein Benutzer mit dem Benutzernamen *cssys* erstellt werden.
- Sie können mehr über die Sicherheit von Data Infrastructure Insights lesen"hier," .

Globale Änderungen können sich möglicherweise auf Ihre ONTAP Systeme auswirken. Es wird dringend empfohlen, Änderungen, die eine große Anzahl von Datensammlern betreffen, außerhalb der Spitzenzeiten vorzunehmen.

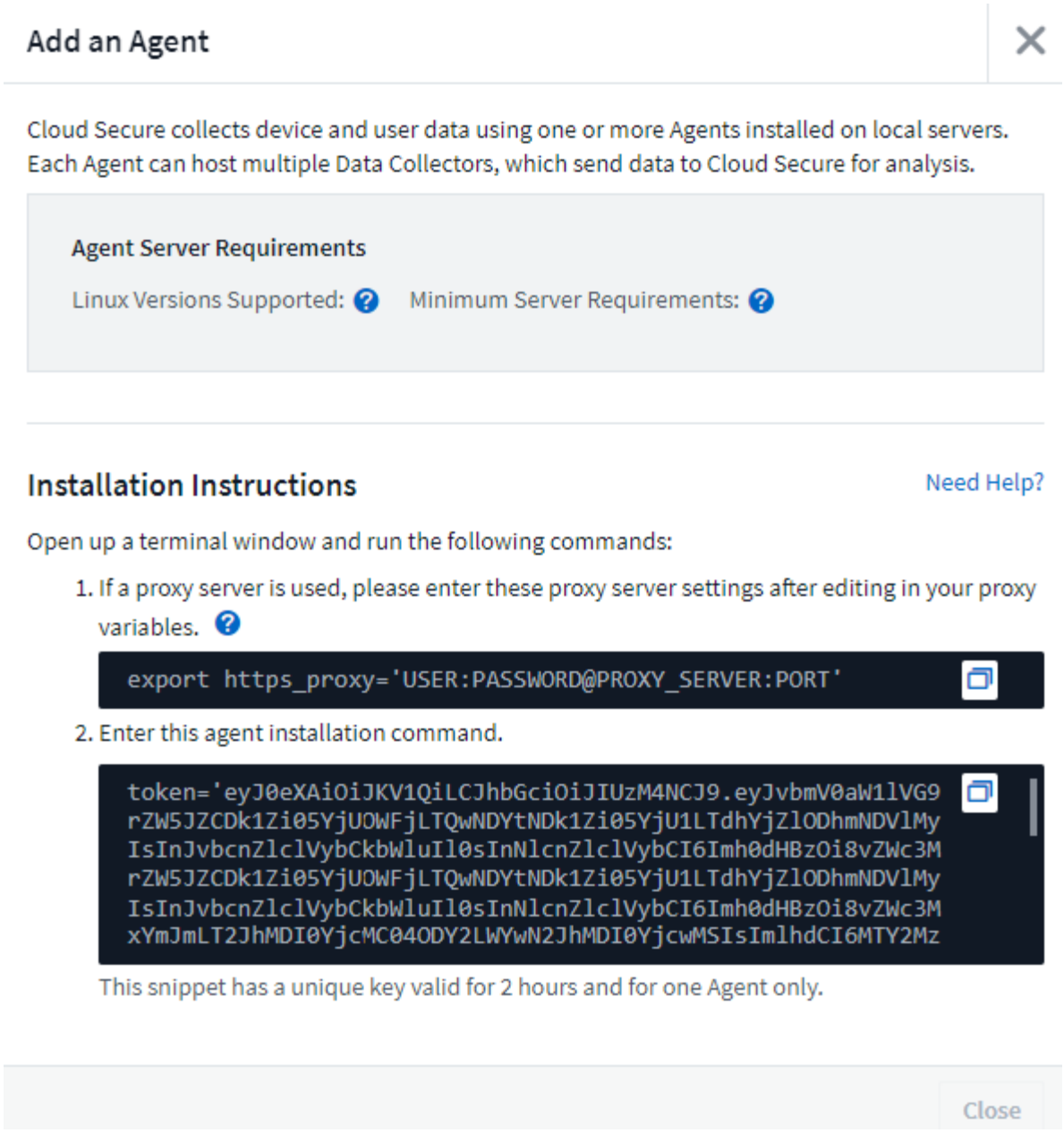
Schritte zum Installieren des Agenten

1. Melden Sie sich als Administrator oder Kontobesitzer bei Ihrer Workload Security-Umgebung an.
2. Wählen Sie **Sammler > Agenten > +Agent**

   Das System zeigt die Seite „Agent hinzufügen“ an:



3. Stellen Sie sicher, dass der Agent-Server die Mindestsystemanforderungen erfüllt.
4. Um zu überprüfen, ob auf dem Agent-Server eine unterstützte Linux-Version ausgeführt wird, klicken Sie auf *Unterstützte Versionen (i)*.
5. Wenn Ihr Netzwerk einen Proxyserver verwendet, legen Sie die Proxyserverdetails fest, indem Sie den Anweisungen im Abschnitt „Proxy“ folgen.



6. Klicken Sie auf das Symbol „In die Zwischenablage kopieren“, um den Installationsbefehl zu kopieren.
7. Führen Sie den Installationsbefehl in einem Terminalfenster aus.
8. Wenn die Installation erfolgreich abgeschlossen ist, zeigt das System die folgende Meldung an:

Nach Abschluss

1. Sie müssen eine"Benutzerverzeichnis-Sammler" .
2. Sie müssen einen oder mehrere Datensammler konfigurieren.

Netzwerkkonfiguration

Führen Sie die folgenden Befehle auf dem lokalen System aus, um Ports zu öffnen, die von Workload Security verwendet werden. Wenn Sicherheitsbedenken hinsichtlich des Portbereichs bestehen, können Sie einen kleineren Portbereich verwenden, beispielsweise *35000:35100*. Jede SVM verwendet zwei Ports.

Schritte

1. `sudo firewall-cmd --permanent --zone=public --add-port=35000-55000/tcp`
2. `sudo firewall-cmd --reload`

Befolgen Sie die nächsten Schritte entsprechend Ihrer Plattform:

CentOS 7.x / RHEL 7.x:

1. `sudo iptables-save | grep 35000`

Beispielausgabe:

```
 -A IN_public_allow -p tcp -m tcp --dport 35000:55000 -m conntrack
-ctstate NEW,UNTRACKED -j ACCEPT
*CentOS 8.x / RHEL 8.x*:
```

1. `sudo firewall-cmd --zone=public --list-ports | grep 35000`(für CentOS 8)

Beispielausgabe:

```
35000-55000/tcp
```

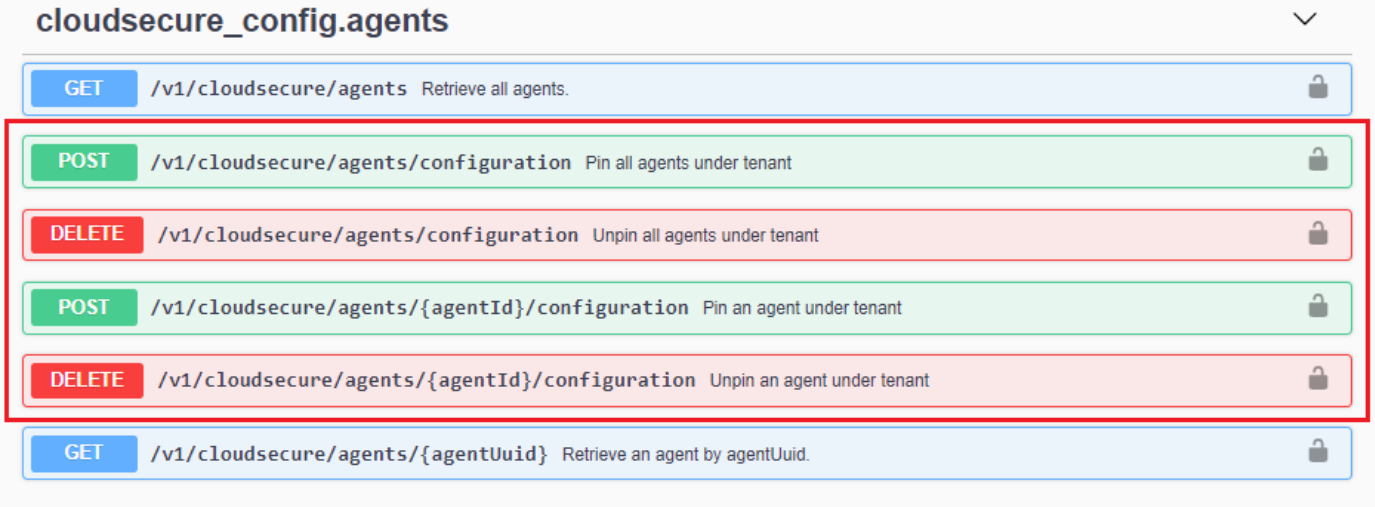
Einen Agenten auf der aktuellen Version „fixieren“

Standardmäßig aktualisiert Data Infrastructure Insights Workload Security Agents automatisch. Einige Kunden möchten die automatische Aktualisierung möglicherweise anhalten, wodurch ein Agent auf seiner aktuellen Version verbleibt, bis eines der folgenden Ereignisse eintritt:

- Der Kunde nimmt die automatischen Agent-Updates wieder auf.
- 30 Tage sind vergangen. Beachten Sie, dass die 30 Tage am Tag der letzten Agentenaktualisierung beginnen und nicht an dem Tag, an dem der Agent angehalten wird.

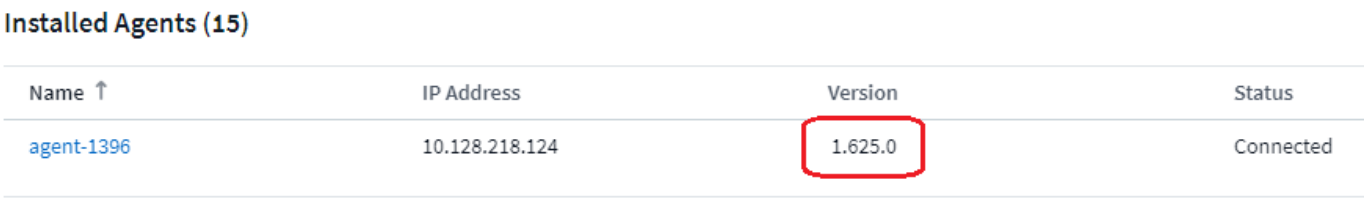
In jedem dieser Fälle wird der Agent bei der nächsten Aktualisierung der Workload-Sicherheit aktualisiert.

Um automatische Agent-Updates anzuhalten oder fortzusetzen, verwenden Sie die *cloudsecure_config.agents* -APIs:



Beachten Sie, dass es bis zu fünf Minuten dauern kann, bis die Pausen- oder Fortsetzungsaktion wirksam wird.

Sie können Ihre aktuellen Agent-Versionen auf der Seite **Workload Security > Collectors** auf der Registerkarte **Agents** anzeigen.



Fehlerbehebung bei Agentenfehlern

Bekannte Probleme und deren Lösungen werden in der folgenden Tabelle beschrieben.

Problem:	Auflösung:
Bei der Agent-Installation kann der Ordner /opt/netapp/cloudsecure/agent/logs/agent.log nicht erstellt werden und die Datei install.log enthält keine relevanten Informationen.	Dieser Fehler tritt beim Bootstrapping des Agenten auf. Der Fehler wird nicht in den Protokolldateien protokolliert, da er vor der Initialisierung des Loggers auftritt. Der Fehler wird zur Standardausgabe umgeleitet und ist im Serviceprotokoll mit dem `journalctl -u cloudsecure-agent.service` Befehl. Dieser Befehl kann zur weiteren Fehlerbehebung des Problems verwendet werden. est
Die Agenteninstallation schlägt mit der Meldung „Diese Linux-Distribution wird nicht unterstützt“ fehl. Beenden der Installation‘.	Dieser Fehler tritt auf, wenn Sie versuchen, den Agenten auf einem nicht unterstützten System zu installieren. Sehen "Agentenanforderungen" .

Problem:	Auflösung:
Die Agenteninstallation ist mit folgendem Fehler fehlgeschlagen: „-bash: unzip: Befehl nicht gefunden“	Installieren Sie „Unzip“ und führen Sie den Installationsbefehl erneut aus. Wenn Yum auf dem Computer installiert ist, versuchen Sie „yum install unzip“, um die Entpackungssoftware zu installieren. Kopieren Sie anschließend den Befehl erneut aus der Benutzeroberfläche der Agent-Installation und fügen Sie ihn in die CLI ein, um die Installation erneut auszuführen.

Der Agent wurde installiert und lief. Der Agent hat jedoch plötzlich aufgehört.	Stellen Sie eine SSH-Verbindung zum Agent-Computer her. Überprüfen Sie den Status des Agentendienstes über `sudo systemctl status cloudsecure-agent.service` . 1. Überprüfen Sie, ob in den Protokollen die Meldung „Workload Security-Daemon-Dienst konnte nicht gestartet werden“ angezeigt wird. 2. Überprüfen Sie, ob der CSSY-Benutzer auf dem Agent-Computer vorhanden ist oder nicht. Führen Sie die folgenden Befehle nacheinander mit Root-Berechtigung aus und prüfen Sie, ob der Benutzer und die Gruppe CSSYS vorhanden sind.
	`sudo id cssys`
	`sudo groups cssys` 3. Wenn keines vorhanden ist, wurde der CSSY-Benutzer möglicherweise durch eine zentralisierte Überwachungsrichtlinie gelöscht. 4. Erstellen Sie den CSSY-Benutzer und die CSSY-Gruppe manuell, indem Sie die folgenden Befehle ausführen.
	`sudo useradd cssys`
	`sudo groupadd cssys` 5. Starten Sie den Agentendienst anschließend neu, indem Sie den folgenden Befehl ausführen:
	`sudo systemctl restart cloudsecure-agent.service` 6. Wenn es immer noch nicht läuft, prüfen Sie bitte die anderen Optionen zur Fehlerbehebung.

Es können nicht mehr als 50 Datensammler zu einem Agenten hinzugefügt werden.	Einem Agenten können nur 50 Datensammler hinzugefügt werden. Dies kann eine Kombination aller Collector-Typen sein, beispielsweise Active Directory, SVM und andere Collector.
Die Benutzeroberfläche zeigt, dass sich der Agent im Status NOT_CONNECTED befindet.	Schritte zum Neustart des Agenten. 1. Stellen Sie eine SSH-Verbindung zum Agent-Computer her. 2. Starten Sie den Agentendienst anschließend neu, indem Sie den folgenden Befehl ausführen: `sudo systemctl restart cloudsecure-agent.service` 3. Überprüfen Sie den Status des Agentendienstes über `sudo systemctl status cloudsecure-agent.service` . 4. Der Agent sollte in den Status „VERBUNDEN“ wechseln.

Problem:	Auflösung:
Die Agent-VM befindet sich hinter dem Zscaler-Proxy und die Agent-Installation schlägt fehl. Aufgrund der SSL-Prüfung des Zscaler-Proxys werden die Workload-Sicherheitszertifikate so angezeigt, als wären sie von der Zscaler-Zertifizierungsstelle signiert, sodass der Agent der Kommunikation nicht vertraut.	Deaktivieren Sie die SSL-Prüfung im Zscaler-Proxy für die URL *.cloudinsights.netapp.com. Wenn Zscaler eine SSL-Prüfung durchführt und die Zertifikate ersetzt, funktioniert Workload Security nicht.
Während der Installation des Agenten bleibt die Installation nach dem Entpacken hängen.	Der Befehl „chmod 755 -Rf“ schlägt fehl. Der Befehl schlägt fehl, wenn der Agent-Installationsbefehl von einem Nicht-Root-Sudo-Benutzer ausgeführt wird, der Dateien im Arbeitsverzeichnis hat, die einem anderen Benutzer gehören, und die Berechtigungen dieser Dateien nicht geändert werden können. Aufgrund des fehlgeschlagenen chmod-Befehls wird der Rest der Installation nicht ausgeführt. 1. Erstellen Sie ein neues Verzeichnis mit dem Namen „cloudsecure“. 2. Gehen Sie zu diesem Verzeichnis. 3. Kopieren Sie den vollständigen Installationsbefehl „token=…… … ./cloudsecure-agent-install.sh“, fügen Sie ihn ein und drücken Sie die Eingabetaste. 4. Die Installation sollte fortgesetzt werden können.
Wenn der Agent immer noch keine Verbindung zu Saas herstellen kann, öffnen Sie bitte einen Fall beim NetApp Support. Geben Sie die Seriennummer von Data Infrastructure Insights an, um einen Fall zu öffnen, und hängen Sie die Protokolle wie angegeben an den Fall an.	So fügen Sie Protokolle an den Koffer an: 1. Führen Sie das folgende Skript mit Root-Berechtigung aus und geben Sie die Ausgabedatei (cloudsecure-agent-symptoms.zip) frei. a. /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent-symptom-collector.sh 2. Führen Sie die folgenden Befehle nacheinander mit Root-Berechtigung aus und teilen Sie die Ausgabe. a. id cssys b. groups cssys c. cat /etc/os-release
Das Skript cloudsecure-agent-symptom-collector.sh schlägt mit dem folgenden Fehler fehl. [root@machine tmp]# /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent-symptom-collector.sh Dienstprotokoll sammeln Anwendungsprotokolle sammeln Agentenkonfigurationen sammeln Servicestatus-Snapshot erstellen Snapshot der Agentenverzeichnisstruktur erstellen …… …… /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent-symptom-collector.sh: Zeile 52: zip: Befehl nicht gefunden. FEHLER: /tmp/cloudsecure-agent-symptoms.zip konnte nicht erstellt werden.	Das Zip-Tool ist nicht installiert. Installieren Sie das Zip-Tool, indem Sie den Befehl „yum install zip“ ausführen. Führen Sie dann cloudsecure-agent-symptom-collector.sh erneut aus.

Problem:	Auflösung:
Die Agenteninstallation schlägt mit useradd fehl: Verzeichnis /home/cssys kann nicht erstellt werden	Dieser Fehler kann auftreten, wenn das Anmeldeverzeichnis des Benutzers aufgrund fehlender Berechtigungen nicht unter /home erstellt werden kann. Die Problemumgehung besteht darin, einen CSSY-Benutzer zu erstellen und sein Anmeldeverzeichnis manuell mit dem folgenden Befehl hinzuzufügen: *sudo useradd user_name -m -d HOME_DIR* -m: Erstellen Sie das Home-Verzeichnis des Benutzers, falls es nicht vorhanden ist. -d: Der neue Benutzer wird mit HOME_DIR als Wert für das Anmeldeverzeichnis des Benutzers erstellt. Beispielsweise fügt *sudo useradd cssys -m -d /cssys* einen Benutzer *cssys* hinzu und erstellt sein Anmeldeverzeichnis unter root.
Der Agent wird nach der Installation nicht ausgeführt. *Systemctl status cloudsecure-agent.service* zeigt Folgendes: [root@demo ~]# systemctl status cloudsecure-agent.service agent.service – Workload Security Agent Daemon Service Loaded: geladen (/usr/lib/systemd/system/cloudsecure-agent.service; aktiviert; Vendor-Vorgabe: deaktiviert) Active: Aktivierung (automatischer Neustart) (Ergebnis: Exitcode) seit Dienstag, 03.08.2021, 21:12:26 PDT; Vor 2 Sekunden Prozess: 25889 ExecStart=/bin/bash /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent (Code=exited Status=126) Haupt-PID: 25889 (Code=exited, Status=126), 3. August 21:12:26 Demo systemd[1]: cloudsecure-agent.service: Hauptprozess beendet, Code=exited, Status=126/n/a 3. August 21:12:26 Demo systemd[1]: Einheit cloudsecure-agent.service ist in den Zustand „Fehler“ gewechselt. 03. Aug. 21:12:26 Demo systemd[1]: cloudsecure-agent.service fehlgeschlagen.	Dies kann fehlschlagen, weil der Benutzer *cssys* möglicherweise keine Berechtigung zur Installation hat. Wenn es sich bei /opt/netapp um einen NFS-Mount handelt und der Benutzer *cssys* keinen Zugriff auf diesen Ordner hat, schlägt die Installation fehl. *cssys* ist ein lokaler Benutzer, der vom Workload Security-Installationsprogramm erstellt wurde und möglicherweise keine Berechtigung zum Zugriff auf die bereitgestellte Freigabe hat. Sie können dies überprüfen, indem Sie versuchen, mit dem Benutzer *cssys* auf /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent zuzugreifen. Wenn die Meldung „Berechtigung verweigert“ angezeigt wird, liegt keine Installationsberechtigung vor. Installieren Sie die Software nicht in einem bereitgestellten Ordner, sondern in einem lokalen Verzeichnis auf dem Computer.
Der Agent wurde ursprünglich über einen Proxyserver verbunden und der Proxy wurde während der Agentinstallation festgelegt. Jetzt hat sich der Proxyserver geändert. Wie kann die Proxy-Konfiguration des Agenten geändert werden?	Sie können die agent.properties bearbeiten, um die Proxy-Details hinzuzufügen. Gehen Sie folgendermaßen vor: 1. Wechseln Sie in den Ordner, der die Eigenschaftendatei enthält: cd /opt/netapp/cloudsecure/conf 2. Öffnen Sie die Datei *agent.properties* zur Bearbeitung mit Ihrem bevorzugten Texteditor. 3. Fügen Sie die folgenden Zeilen hinzu oder ändern Sie sie: AGENT_PROXY_HOST=scspa1950329001.vm.netapp.com AGENT_PROXY_PORT=80 AGENT_PROXY_USER=pxuser AGENT_PROXY_PASSWORD=pass1234 4. Speichern Sie die Datei. 5. Starten Sie den Agenten neu: sudo systemctl restart cloudsecure-agent.service

Löschen eines Workload Security Agent

Wenn Sie einen Workload Security Agent löschen, müssen zuerst alle mit dem Agent verknüpften Datensammler gelöscht werden.

Löschen eines Agenten

> Durch das Löschen eines Agenten werden alle mit dem Agenten verknüpften Datensammler gelöscht. Wenn Sie die Datensammler mit einem anderen Agenten konfigurieren möchten, sollten Sie vor dem Löschen des Agenten eine Sicherungskopie der Datensammlerkonfigurationen erstellen.

Bevor Sie beginnen

1. Stellen Sie sicher, dass alle mit dem Agenten verknüpften Datensammler aus dem Workload Security-Portal gelöscht werden.

   Hinweis: Ignorieren Sie diesen Schritt, wenn sich alle zugehörigen Collector im Status STOPPED befinden.

Schritte zum Löschen eines Agenten:

1. Melden Sie sich per SSH bei der Agent-VM an und führen Sie den folgenden Befehl aus. Geben Sie bei der entsprechenden Aufforderung „y“ ein, um fortzufahren.

   ```
   sudo /opt/netapp/cloudsecure/agent/install/cloudsecure-agent-
   uninstall.sh
   Uninstall CloudSecure Agent? [y|N]:
   ```

2. Klicken Sie auf **Workload-Sicherheit > Collectors > Agents**

   Das System zeigt die Liste der konfigurierten Agenten an.

3. Klicken Sie auf das Optionsmenü für den Agenten, den Sie löschen.
4. Klicken Sie auf **Löschen**.

   Das System zeigt die Seite **Agent löschen** an.

5. Klicken Sie auf **Löschen**, um den Löschvorgang zu bestätigen.

Konfigurieren eines Active Directory (AD)-Benutzerverzeichnis-Collectors

Workload Security kann so konfiguriert werden, dass Benutzerattribute von Active Directory-Servern erfasst werden.

Bevor Sie beginnen

- Sie müssen ein Data Infrastructure Insights Administrator oder Kontoinhaber sein, um diese Aufgabe auszuführen.
- Sie müssen über die IP-Adresse des Servers verfügen, auf dem der Active Directory-Server gehostet wird.
- Bevor Sie einen Benutzerverzeichnis-Connector konfigurieren, muss ein Agent konfiguriert werden.

Schritte zum Konfigurieren eines Benutzerverzeichnis-Collectors

1. Klicken Sie im Menü „Workload Security“ auf: **Collectors > User Directory Collectors > + User Directory Collector** und wählen Sie **Active Directory**

   Das System zeigt den Bildschirm „Benutzerverzeichnis hinzufügen“ an.

Konfigurieren Sie den User Directory Collector, indem Sie die erforderlichen Daten in die folgenden Tabellen eingeben:

Name	Beschreibung
Name	Eindeutiger Name für das Benutzerverzeichnis. Zum Beispiel *GlobalADCollector*
Agent	Wählen Sie einen konfigurierten Agenten aus der Liste aus
Server-IP/Domänenname	IP-Adresse oder vollqualifizierter Domänenname (FQDN) des Servers, auf dem das Active Directory gehostet wird
Waldname	Gesamtstrukturebene der Verzeichnisstruktur. Der Gesamtstrukturname lässt die beiden folgenden Formate zu: *x.y.z* ⇒ direkter Domänenname, wie er auf Ihrem SVM vorhanden ist. [Beispiel: hq.firmenname.com] *DC=x,DC=y,DC=z* ⇒ Relative Distinguished Names [Beispiel: DC=hq,DC= Firmenname,DC=com] Oder Sie können Folgendes angeben: *OU=Engineering,DC=hq,DC= Firmenname,DC=com* [um nach einer bestimmten OU Engineering zu filtern] *CN=Benutzername,OU=Engineering,DC=Firmennam e, DC=NetApp, DC=com* [um nur bestimmte Benutzer mit <Benutzername> aus der OU <Engineering> abzurufen] *CN=Acrobat-Benutzer,CN=Benutzer,DC=hq,DC=Firmenname,DC= com,O= Firmenname,L=Boston,S=MA,C=US* [um alle Acrobat-Benutzer innerhalb der Benutzer in dieser Organisation abzurufen] Vertrauenswürdige Active Directory-Domänen werden ebenfalls unterstützt.
Bind-DN	Der Benutzer darf das Verzeichnis durchsuchen. Beispiel: *Benutzername@Firmenname.com* oder *Benutzername@Domänenname.com*. Außerdem ist die Berechtigung „Nur Lesen“ für die Domäne erforderlich. Der Benutzer muss Mitglied der Sicherheitsgruppe „Schreibgeschützte Domänencontroller“ sein.
BIND-Passwort	Kennwort für den Verzeichnisserver (d. h. Kennwort für den im Bind-DN verwendeten Benutzernamen)
Protokoll	ldap, ldaps, ldap-start-tls
Häfen	Port auswählen

Geben Sie die folgenden für Directory Server erforderlichen Attribute ein, wenn die Standardattributnamen in Active Directory geändert wurden. Meistens werden diese Attributnamen in Active Directory *nicht* geändert. In

diesem Fall können Sie einfach mit dem Standardattributnamen fortfahren.

Eigenschaften	Attributname im Verzeichnisserver
Anzeigename	Name
SID	Objekt-ID
Benutzername	sAMAccountName

Klicken Sie auf „Optionale Attribute einschließen“, um die folgenden Attribute hinzuzufügen:

Eigenschaften	Attributname im Verzeichnisserver
E-Mail-Adresse	mail
Telefonnummer	Telefonnummer
Rolle	Titel
Land	co
Status	Zustand
Abteilung	Abteilung
Foto	Miniaturfoto
ManagerDN	Manager
Gruppen	Mitglied von

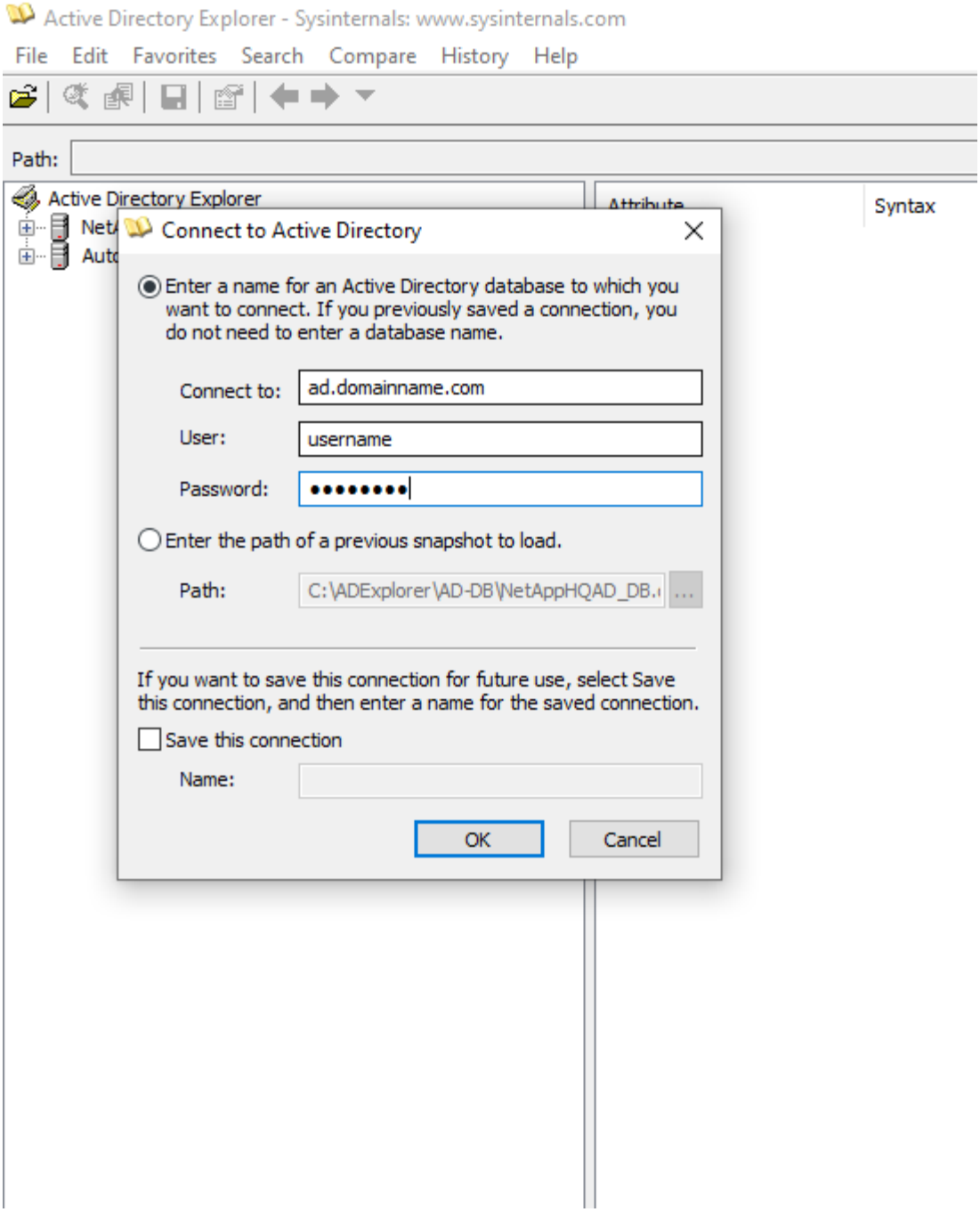
Testen der Konfiguration Ihres Benutzerverzeichnis-Collectors

Sie können LDAP-Benutzerberechtigungen und Attributdefinitionen mithilfe der folgenden Verfahren validieren:

- Verwenden Sie den folgenden Befehl, um die LDAP-Benutzerberechtigung für Workload Security zu validieren:

  ```
  ldapsearch -o ldif-wrap=no -LLL -x -b "dc=netapp,dc=com" -h 10.235.40.29 -p
  389 -D Administrator@netapp.com -W
  ```

- Verwenden Sie AD Explorer, um in einer AD-Datenbank zu navigieren, Objekteigenschaften und -attribute anzuzeigen, Berechtigungen anzuzeigen, das Schema eines Objekts anzuzeigen und komplexe Suchvorgänge auszuführen, die Sie speichern und erneut ausführen können.
  - Installieren"AD Explorer" auf jedem Windows-Computer, der eine Verbindung zum AD-Server herstellen kann.
  - Stellen Sie mit dem Benutzernamen/Passwort des AD-Verzeichnisservers eine Verbindung zum AD-Server her.



Fehlerbehebung bei Konfigurationsfehlern des User Directory Collector

In der folgenden Tabelle werden bekannte Probleme und Lösungen beschrieben, die während der Collector-Konfiguration auftreten können:

Problem:	Auflösung:
Das Hinzufügen eines Benutzerverzeichnis-Konnektors führt zum Status „Fehler“. Der Fehler lautet: „Ungültige Anmeldeinformationen für LDAP-Server angegeben.“	Falscher Benutzername oder falsches Passwort angegeben. Bearbeiten Sie den richtigen Benutzernamen und das richtige Passwort und geben Sie es ein.

Problem:	Auflösung:
Das Hinzufügen eines Benutzerverzeichnis-Konnektors führt zum Status „Fehler“. Der Fehler lautet: „Das Objekt, das DN=DC=hq,DC=domainname,DC=com entspricht und als Gesamtstrukturname angegeben wurde, konnte nicht abgerufen werden.“	Falscher Gesamtstrukturname angegeben. Bearbeiten Sie den Vorgang und geben Sie den richtigen Gesamtstrukturnamen ein.
Die optionalen Attribute des Domänenbenutzers werden auf der Workload Security-Benutzerprofilseite nicht angezeigt.	Dies liegt wahrscheinlich an einer Nichtübereinstimmung zwischen den Namen der in CloudSecure hinzugefügten optionalen Attribute und den tatsächlichen Attributnamen in Active Directory. Bearbeiten Sie die Datei und geben Sie die korrekten optionalen Attributnamen an.
Datensammler im Fehlerzustand mit „Fehler beim Abrufen der LDAP-Benutzer.“ Grund für den Fehler: „Verbindung zum Server nicht möglich, die Verbindung ist null“	Starten Sie den Collector neu, indem Sie auf die Schaltfläche *Neustart* klicken.
Das Hinzufügen eines Benutzerverzeichnis-Konnektors führt zum Status „Fehler“.	Stellen Sie sicher, dass Sie für die erforderlichen Felder (Server, Gesamtstrukturname, Bind-DN, Bind-Passwort) gültige Werte angegeben haben. Stellen Sie sicher, dass die Bind-DN-Eingabe immer als „Administrator@<Domänengesamtstrukturname>“ oder als Benutzerkonto mit Domänenadministratorrechten erfolgt.
Das Hinzufügen eines Benutzerverzeichnis-Konnektors führt zum Status „WIEDERHOLT“. Zeigt den Fehler „Der Status des Collectors konnte nicht definiert werden, Grund: Der TCP-Befehl [Connect(localhost:35012,None,List(),Some(,seconds),true)] ist aufgrund von java.net.ConnectionException:Connection refused fehlgeschlagen.“	Für den AD-Server wurde eine falsche IP-Adresse oder ein falscher FQDN angegeben. Bearbeiten und geben Sie die richtige IP-Adresse oder den richtigen FQDN ein.
Das Hinzufügen eines Benutzerverzeichnis-Konnektors führt zum Status „Fehler“. Der Fehler lautet: „LDAP-Verbindung konnte nicht hergestellt werden.“	Für den AD-Server wurde eine falsche IP-Adresse oder ein falscher FQDN angegeben. Bearbeiten und geben Sie die richtige IP-Adresse oder den richtigen FQDN ein.
Das Hinzufügen eines Benutzerverzeichnis-Konnektors führt zum Status „Fehler“. Der Fehler lautet: „Die Einstellungen konnten nicht geladen werden.“ Grund: Die Datenquellenkonfiguration weist einen Fehler auf. Spezifischer Grund: /connector/conf/application.conf: 70: ldap.ldap-port hat den Typ STRING statt NUMBER“	Falscher Wert für Port angegeben. Versuchen Sie, die Standard-Portwerte oder die richtige Portnummer für den AD-Server zu verwenden.
Ich habe mit den obligatorischen Attributen begonnen und es hat funktioniert. Nach dem Hinzufügen der optionalen Attribute werden die Daten der optionalen Attribute nicht aus AD abgerufen.	Dies liegt wahrscheinlich an einer Nichtübereinstimmung zwischen den in CloudSecure hinzugefügten optionalen Attributen und den tatsächlichen Attributnamen in Active Directory. Bearbeiten Sie den korrekten obligatorischen oder optionalen Attributnamen und geben Sie ihn an.

Problem:	Auflösung:
Wann erfolgt die AD-Synchronisierung nach dem Neustart des Collectors?	Die AD-Synchronisierung erfolgt unmittelbar nach dem Neustart des Collectors. Das Abrufen der Benutzerdaten von etwa 300.000 Benutzern dauert etwa 15 Minuten und wird alle 12 Stunden automatisch aktualisiert.
Benutzerdaten werden von AD mit CloudSecure synchronisiert. Wann werden die Daten gelöscht?	Benutzerdaten werden 13 Monate lang gespeichert, wenn keine Aktualisierung erfolgt. Bei Löschung des Mandanten werden auch die Daten gelöscht.
Der Benutzerverzeichnis-Connector führt zum Status „Fehler“. „Der Connector befindet sich im Fehlerzustand. Dienstname: usersLdap. Grund für den Fehler: LDAP-Benutzer konnten nicht abgerufen werden. Grund für den Fehler: 80090308: LdapErr: DSID-0C090453, Kommentar: AcceptSecurityContext-Fehler, Daten 52e, v3839"	Falscher Gesamtstrukturname angegeben. Informationen zum Angeben des richtigen Gesamtstrukturnamens finden Sie oben.
Die Telefonnummer wird auf der Benutzerprofilseite nicht eingetragen.	Dies liegt höchstwahrscheinlich an einem Attributzuordnungsproblem mit Active Directory. 1. Bearbeiten Sie den jeweiligen Active Directory-Collector, der die Benutzerinformationen aus Active Directory abruft. 2. Beachten Sie, dass unter den optionalen Attributen ein Feldname „Telefonnummer“ vorhanden ist, der dem Active Directory-Attribut „Telefonnummer“ zugeordnet ist. 4. Verwenden Sie nun das Tool „Active Directory Explorer“ wie oben beschrieben, um das Active Directory zu durchsuchen und den richtigen Attributnamen anzuzeigen. 3. Stellen Sie sicher, dass es im Active Directory ein Attribut mit dem Namen „Telefonnummer“ gibt, das tatsächlich die Telefonnummer des Benutzers enthält. 5. Nehmen wir an, es wurde im Active Directory in „Telefonnummer“ geändert. 6. Bearbeiten Sie dann den CloudSecure-Benutzerverzeichnis-Collector. Ersetzen Sie im Abschnitt „Optionale Attribute“ „Telefonnummer“ durch „Telefonnummer“. 7. Speichern Sie den Active Directory-Collector. Der Collector wird neu gestartet, ruft die Telefonnummer des Benutzers ab und zeigt diese auf der Benutzerprofilseite an.
Wenn das Verschlüsselungszertifikat (SSL) auf dem Active Directory (AD)-Server aktiviert ist, kann der Workload Security User Directory Collector keine Verbindung zum AD-Server herstellen.	Deaktivieren Sie die AD-Server-Verschlüsselung, bevor Sie einen User Directory Collector konfigurieren. Sobald die Benutzerdetails abgerufen wurden, bleiben sie 13 Monate lang dort. Wenn die Verbindung zum AD-Server nach dem Abrufen der Benutzerdetails getrennt wird, werden die neu hinzugefügten Benutzer in AD nicht abgerufen. Zum erneuten Abrufen muss der Benutzerverzeichnis-Collector mit AD verbunden sein.

Problem:	Auflösung:
Daten aus Active Directory sind in CloudInsights Security vorhanden. Möchten Sie alle Benutzerinformationen aus CloudInsights löschen.	Es ist nicht möglich, NUR Active Directory-Benutzerinformationen aus CloudInsights Security zu löschen. Um den Benutzer zu löschen, muss der gesamte Mandant gelöscht werden.

Konfigurieren eines LDAP-Verzeichnisserver-Collectors

Sie konfigurieren Workload Security, um Benutzerattribute von LDAP-Verzeichnisservern zu erfassen.

Bevor Sie beginnen

- Sie müssen ein Data Infrastructure Insights Administrator oder Kontoinhaber sein, um diese Aufgabe auszuführen.
- Sie müssen über die IP-Adresse des Servers verfügen, auf dem der LDAP-Verzeichnisserver gehostet wird.
- Bevor Sie einen LDAP-Verzeichnis-Connector konfigurieren, muss ein Agent konfiguriert werden.

Schritte zum Konfigurieren eines Benutzerverzeichnis-Collectors

1. Klicken Sie im Menü „Workload Security“ auf: **Collectors > User Directory Collectors > + User Directory Collector** und wählen Sie **LDAP Directory Server** aus.

   Das System zeigt den Bildschirm „Benutzerverzeichnis hinzufügen“ an.

Konfigurieren Sie den User Directory Collector, indem Sie die erforderlichen Daten in die folgenden Tabellen eingeben:

Name	Beschreibung
Name	Eindeutiger Name für das Benutzerverzeichnis. Zum Beispiel *GlobalLDAPCollector*
Agent	Wählen Sie einen konfigurierten Agenten aus der Liste aus
Server-IP/Domänenname	IP-Adresse oder vollqualifizierter Domänenname (FQDN) des Servers, auf dem der LDAP-Verzeichnisserver gehostet wird

Suchbasis	Suchbasis des LDAP-Servers. Suchbasis erlaubt die beiden folgenden Formate: *x.y.z* ⇒ direkter Domänenname, wie Sie ihn auf Ihrem SVM haben. [Beispiel: hq.firmenname.com] *DC=x,DC=y,DC=z* ⇒ Relative Distinguished Names [Beispiel: DC=hq,DC=Firmenname,DC=com] Oder Sie können Folgendes angeben: *OU=Engineering,DC=hq,DC=Firmenname,DC=com* [um nach einer bestimmten OU Engineering zu filtern] *CN=Benutzername,OU=Engineering,DC=Firmenname, DC=NetApp, DC=com* [um nur bestimmte Benutzer mit <Benutzername> aus der OU <Engineering> abzurufen] *CN=Acrobat-Benutzer,CN=Benutzer,DC=hq,DC=Firmenname,DC=com,O= Firmenname,L=Boston,S=MA,C=US* [um alle Acrobat-Benutzer innerhalb der Benutzer in dieser Organisation abzurufen]
Bind-DN	Der Benutzer darf das Verzeichnis durchsuchen. Beispiel: uid=ldapuser,cn=users,cn=accounts,dc=domain,dc=companyname,dc=com uid=john,cn=users,cn=accounts,dc=dorp,dc=company,dc=com für einen Benutzer john@dorp.company.com. dorp.company.com
--accounts	--users
--John	--anna
BIND-Passwort	Kennwort für den Verzeichnisserver (d. h. Kennwort für den im Bind-DN verwendeten Benutzernamen)
Protokoll	ldap, ldaps, ldap-start-tls
Häfen	Port auswählen

Geben Sie die folgenden für den Verzeichnisserver erforderlichen Attribute ein, wenn die Standardattributnamen im LDAP-Verzeichnisserver geändert wurden. Meistens werden diese Attributnamen im LDAP-Verzeichnisserver *nicht* geändert. In diesem Fall können Sie einfach mit dem Standardattributnamen fortfahren.

Eigenschaften	Attributname im Verzeichnisserver
Anzeigename	Name
UNIXID	UID-Nummer
Benutzername	UID

Klicken Sie auf „Optionale Attribute einschließen“, um die folgenden Attribute hinzuzufügen:

Eigenschaften	Attributname im Verzeichnisserver
E-Mail-Adresse	mail
Telefonnummer	Telefonnummer

Rolle	Titel
Land	co
Status	Zustand
Abteilung	Abteilungsnummer
Foto	Foto
ManagerDN	Manager
Gruppen	Mitglied von

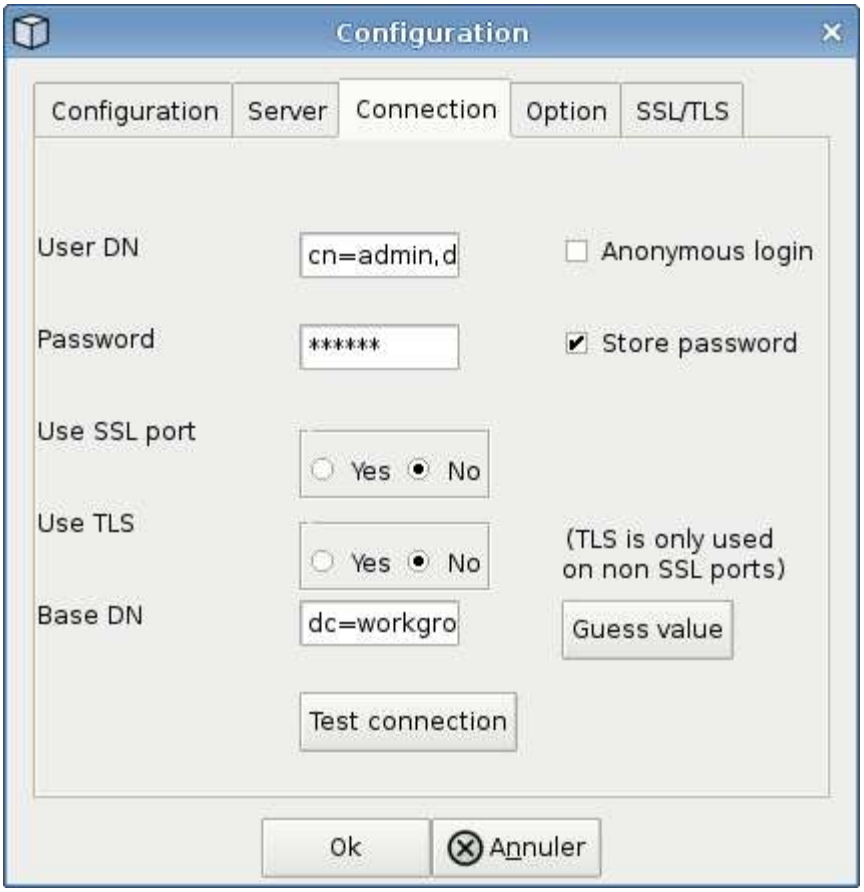
Testen der Konfiguration Ihres Benutzerverzeichnis-Collectors

Sie können LDAP-Benutzerberechtigungen und Attributdefinitionen mithilfe der folgenden Verfahren validieren:

- Verwenden Sie den folgenden Befehl, um die LDAP-Benutzerberechtigung für Workload Security zu validieren:

```
 ldapsearch -D "uid=john
,cn=users,cn=accounts,dc=dorp,dc=company,dc=com" -W -x -LLL -o ldif-
wrap=no -b "cn=accounts,dc=dorp,dc=company,dc=com" -H
ldap://vmwipaapp08.dorp.company.com
* Verwenden Sie den LDAP Explorer, um in einer LDAP-Datenbank zu
navigieren, Objekteigenschaften und -attribute anzuzeigen,
Berechtigungen anzuzeigen, das Schema eines Objekts anzuzeigen und
komplexe Suchvorgänge auszuführen, die Sie speichern und erneut
ausführen können.
```

  - Installieren Sie den LDAP Explorer(http://ldaptool.sourceforge.net/) oder Java LDAP Explorer(http://jxplorer.org/) auf jedem Windows-Computer, der eine Verbindung zum LDAP-Server herstellen kann.
  - Stellen Sie mit dem Benutzernamen/Passwort des LDAP-Verzeichnisservers eine Verbindung zum LDAP-Server her.



Fehlerbehebung bei Konfigurationsfehlern des LDAP-Verzeichnissammlers

In der folgenden Tabelle werden bekannte Probleme und Lösungen beschrieben, die während der Collector-Konfiguration auftreten können:

Problem:	Auflösung:
Das Hinzufügen eines LDAP-Verzeichniskonnektors führt zum Status „Fehler“. Der Fehler lautet: „Ungültige Anmeldeinformationen für LDAP-Server angegeben.“	Falscher Bind-DN oder falsches Bind-Passwort oder falsche Suchbasis angegeben. Bearbeiten und geben Sie die richtigen Informationen ein.
Das Hinzufügen eines LDAP-Verzeichniskonnektors führt zum Status „Fehler“. Der Fehler lautet: „Das Objekt, das DN=DC=hq,DC=domainname,DC=com entspricht und als Gesamtstrukturname angegeben wurde, konnte nicht abgerufen werden.“	Falsche Suchbasis angegeben. Bearbeiten Sie den Vorgang und geben Sie den richtigen Gesamtstrukturnamen ein.
Die optionalen Attribute des Domänenbenutzers werden auf der Workload Security-Benutzerprofilseite nicht angezeigt.	Dies liegt wahrscheinlich an einer Nichtübereinstimmung zwischen den Namen der in CloudSecure hinzugefügten optionalen Attribute und den tatsächlichen Attributnamen in Active Directory. Bei den Feldern wird zwischen Groß- und Kleinschreibung unterschieden. Bearbeiten Sie die Datei und geben Sie die korrekten optionalen Attributnamen an.

Problem:	Auflösung:
Datensammler im Fehlerzustand mit „Fehler beim Abrufen der LDAP-Benutzer.“ Grund für den Fehler: „Verbindung zum Server nicht möglich, die Verbindung ist null“	Starten Sie den Collector neu, indem Sie auf die Schaltfläche *Neustart* klicken.
Das Hinzufügen eines LDAP-Verzeichniskonnektors führt zum Status „Fehler“.	Stellen Sie sicher, dass Sie für die erforderlichen Felder (Server, Gesamtstrukturname, Bind-DN, Bind-Passwort) gültige Werte angegeben haben. Stellen Sie sicher, dass die Bind-DN-Eingabe immer als uid=ldapuser,cn=users,cn=accounts,dc=domain,dc=companyname,dc=com bereitgestellt wird.
Das Hinzufügen eines LDAP-Verzeichniskonnektors führt zum Status „WIEDERHOLT“. Zeigt den Fehler „Fehler beim Ermitteln des Zustands des Collectors, daher erneuter Versuch“ an.	Stellen Sie sicher, dass die richtige Server-IP und Suchbasis angegeben ist ////
Beim Hinzufügen des LDAP-Verzeichnisses wird der folgende Fehler angezeigt: „Der Zustand des Collectors konnte innerhalb von 2 Versuchen nicht ermittelt werden. Versuchen Sie, den Collector erneut neu zu starten (Fehlercode: AGENT008)“	Stellen Sie sicher, dass die richtige Server-IP und Suchbasis angegeben ist
Das Hinzufügen eines LDAP-Verzeichniskonnektors führt zum Status „WIEDERHOLT“. Zeigt den Fehler „Der Status des Collectors konnte nicht definiert werden, Grund: Der TCP-Befehl [Connect(localhost:35012,None,List(),Some(,seconds),true)] ist aufgrund von java.net.ConnectionException:Connection refused fehlgeschlagen.“	Für den AD-Server wurde eine falsche IP-Adresse oder ein falscher FQDN angegeben. Bearbeiten und geben Sie die richtige IP-Adresse oder den richtigen FQDN ein. ////
Das Hinzufügen eines LDAP-Verzeichniskonnektors führt zum Status „Fehler“. Der Fehler lautet: „LDAP-Verbindung konnte nicht hergestellt werden.“	Für den LDAP-Server wurde eine falsche IP-Adresse oder ein falscher FQDN angegeben. Bearbeiten und geben Sie die richtige IP-Adresse oder den richtigen FQDN ein. Oder falscher Wert für den angegebenen Port. Versuchen Sie, die Standard-Portwerte oder die richtige Portnummer für den LDAP-Server zu verwenden.
Das Hinzufügen eines LDAP-Verzeichniskonnektors führt zum Status „Fehler“. Der Fehler lautet: „Die Einstellungen konnten nicht geladen werden.“ Grund: Die Datenquellenkonfiguration weist einen Fehler auf. Spezifischer Grund: /connector/conf/application.conf: 70: ldap.ldap-port hat den Typ STRING statt NUMBER“	Falscher Wert für Port angegeben. Versuchen Sie, die Standard-Portwerte oder die richtige Portnummer für den AD-Server zu verwenden.
Ich habe mit den obligatorischen Attributen begonnen und es hat funktioniert. Nach dem Hinzufügen der optionalen Attribute werden die Daten der optionalen Attribute nicht aus AD abgerufen.	Dies liegt wahrscheinlich an einer Nichtübereinstimmung zwischen den in CloudSecure hinzugefügten optionalen Attributen und den tatsächlichen Attributnamen in Active Directory. Bearbeiten Sie den korrekten obligatorischen oder optionalen Attributnamen und geben Sie ihn an.

Problem:	Auflösung:
Wann erfolgt die LDAP-Synchronisierung nach dem Neustart des Collectors?	Die LDAP-Synchronisierung erfolgt unmittelbar nach dem Neustart des Collectors. Das Abrufen der Benutzerdaten von etwa 300.000 Benutzern dauert etwa 15 Minuten und wird alle 12 Stunden automatisch aktualisiert.
Benutzerdaten werden von LDAP mit CloudSecure synchronisiert. Wann werden die Daten gelöscht?	Benutzerdaten werden 13 Monate lang gespeichert, wenn keine Aktualisierung erfolgt. Bei Löschung des Mandanten werden auch die Daten gelöscht.
Der LDAP-Verzeichnis-Connector führt zum Status „Fehler“. „Der Connector befindet sich im Fehlerzustand. Dienstname: usersLdap. Grund für den Fehler: LDAP-Benutzer konnten nicht abgerufen werden. Grund für den Fehler: 80090308: LdapErr: DSID-0C090453, Kommentar: AcceptSecurityContext-Fehler, Daten 52e, v3839"	Falscher Gesamtstrukturname angegeben. Informationen zum Angeben des richtigen Gesamtstrukturnamens finden Sie oben.
Die Telefonnummer wird auf der Benutzerprofilseite nicht eingetragen.	Dies liegt höchstwahrscheinlich an einem Attributzuordnungsproblem mit Active Directory. 1. Bearbeiten Sie den jeweiligen Active Directory-Collector, der die Benutzerinformationen aus Active Directory abruft. 2. Beachten Sie, dass unter den optionalen Attributen ein Feldname „Telefonnummer“ vorhanden ist, der dem Active Directory-Attribut „Telefonnummer“ zugeordnet ist. 4. Verwenden Sie nun das Tool „Active Directory Explorer“ wie oben beschrieben, um den LDAP-Verzeichnisserver zu durchsuchen und den richtigen Attributnamen anzuzeigen. 3. Stellen Sie sicher, dass im LDAP-Verzeichnis ein Attribut mit dem Namen „Telefonnummer“ vorhanden ist, das tatsächlich die Telefonnummer des Benutzers enthält. 5. Nehmen wir an, im LDAP-Verzeichnis wurde es in „Telefonnummer“ geändert. 6. Bearbeiten Sie dann den CloudSecure-Benutzerverzeichnis-Collector. Ersetzen Sie im Abschnitt „Optionale Attribute“ „Telefonnummer“ durch „Telefonnummer“. 7. Speichern Sie den Active Directory-Collector. Der Collector wird neu gestartet, ruft die Telefonnummer des Benutzers ab und zeigt diese auf der Benutzerprofilseite an.
Wenn das Verschlüsselungszertifikat (SSL) auf dem Active Directory (AD)-Server aktiviert ist, kann der Workload Security User Directory Collector keine Verbindung zum AD-Server herstellen.	Deaktivieren Sie die AD-Server-Verschlüsselung, bevor Sie einen User Directory Collector konfigurieren. Sobald die Benutzerdetails abgerufen wurden, bleiben sie 13 Monate lang dort. Wenn die Verbindung zum AD-Server nach dem Abrufen der Benutzerdetails getrennt wird, werden die neu hinzugefügten Benutzer in AD nicht abgerufen. Zum erneuten Abrufen muss der Benutzerverzeichnis-Collector mit AD verbunden sein.

Konfigurieren des ONTAP SVM-Datenkollektors

Der ONTAP SVM Data Collector ermöglicht Workload Security die Überwachung von Datei- und Benutzerzugriffsaktivitäten auf NetApp ONTAP Storage Virtual Machines (SVMs). Dieses Handbuch führt Sie durch die Konfiguration und Verwaltung des SVM-Datensammlers, um eine umfassende Sicherheitsüberwachung Ihrer ONTAP Umgebung zu gewährleisten.

Globale Änderungen können sich möglicherweise auf Ihre ONTAP Systeme auswirken. Es wird dringend empfohlen, Änderungen, die eine große Anzahl von Datensammlern betreffen, außerhalb der Spitzenzeiten vorzunehmen.

Bevor Sie beginnen

- Dieser Datensammler wird mit Folgendem unterstützt:
  - Data ONTAP 9.2 und spätere Versionen. Verwenden Sie für optimale Leistung eine Data ONTAP Version höher als 9.13.1.
  - SMB-Protokollversion 3.1 und früher.
  - NFS-Versionen bis einschließlich NFS 4.1 (Beachten Sie, dass NFS 4.1 mit ONTAP 9.15 oder höher unterstützt wird).
  - Flexgroup wird ab ONTAP 9.4 und späteren Versionen unterstützt
  - FlexCache wird für NFS mit ONTAP 9.7 und späteren Versionen unterstützt.
  - FlexCache wird für SMB mit ONTAP 9.14.1 und späteren Versionen unterstützt.
  - ONTAP Select wird unterstützt
- Es werden nur Datentyp-SVMs unterstützt. SVMs mit unbegrenzten Volumes werden nicht unterstützt.
- SVM hat mehrere Untertypen. Davon werden nur *default*, *sync_source* und *sync_destination* unterstützt.
- Ein Agent"muss konfiguriert werden" bevor Sie Datensammler konfigurieren können.
- Stellen Sie sicher, dass Sie über einen ordnungsgemäß konfigurierten Benutzerverzeichnis-Connector verfügen. Andernfalls werden auf der Seite „Aktivitätsforensik“ verschlüsselte Benutzernamen und nicht der tatsächliche Name des Benutzers (wie in Active Directory gespeichert) angezeigt.
- • ONTAP Persistent Store wird ab 9.14.1 unterstützt.
- Für eine optimale Leistung sollten Sie den FPolicy-Server so konfigurieren, dass er sich im selben Subnetz wie das Speichersystem befindet.
- Sie müssen eine SVM mit einer der folgenden beiden Methoden hinzufügen:
  - Durch Verwendung der Cluster-IP, des SVM-Namens sowie des Benutzernamens und Kennworts für die Clusterverwaltung. ***Dies ist die empfohlene Methode.***
    - Der SVM-Name muss genau so lauten, wie er in ONTAP angezeigt wird, und die Groß-/Kleinschreibung muss beachtet werden.
  - Durch Verwendung von SVM Vserver Management IP, Benutzername und Passwort
  - Wenn Sie den vollständigen Benutzernamen und das Kennwort für die Cluster-/SVM-Verwaltung des Administrators nicht verwenden können oder möchten, können Sie einen benutzerdefinierten Benutzer mit geringeren Berechtigungen erstellen, wie im Abschnitt„Ein Hinweis zu Berechtigungen“ Abschnitt unten. Dieser benutzerdefinierte Benutzer kann entweder für den SVM- oder Cluster-Zugriff erstellt werden.

- o Sie können auch einen AD-Benutzer mit einer Rolle verwenden, die mindestens über die Berechtigungen von csrole verfügt, wie im Abschnitt „Hinweis zu Berechtigungen“ weiter unten erwähnt. Siehe auch die"ONTAP-Dokumentation" .

- Stellen Sie sicher, dass die richtigen Anwendungen für die SVM eingestellt sind, indem Sie den folgenden Befehl ausführen:

```
clustershell:> security login show -vserver <vservername> -user-or-group
-name <username>
```

Beispielausgabe:

```
Vserver: svmname
                                                                  Second
User/Group                  Authentication                 Acct   Authentication
Name           Application  Method        Role Name        Locked Method
-------------- -----------  ------------- ---------------- ------ --------------
vsadmin        http         password      vsadmin          no     none
vsadmin        ontapi       password      vsadmin          no     none
vsadmin        ssh          password      vsadmin          no     none
3 entries were displayed.
```

- Stellen Sie sicher, dass für die SVM ein CIFS-Server konfiguriert ist: clustershell:> `vserver cifs show`

  Das System gibt den VServer-Namen, den CIFS-Servernamen und zusätzliche Felder zurück.

- Legen Sie ein Kennwort für den SVM-Benutzer vsadmin fest. Wenn Sie einen benutzerdefinierten Benutzer oder einen Cluster-Administratorbenutzer verwenden, überspringen Sie diesen Schritt. clustershell:> `security login password -username vsadmin -vserver svmname`
- Entsperren Sie den SVM-Benutzer vsadmin für den externen Zugriff. Wenn Sie einen benutzerdefinierten Benutzer oder einen Cluster-Administratorbenutzer verwenden, überspringen Sie diesen Schritt. clustershell:> `security login unlock -username vsadmin -vserver svmname`
- Stellen Sie sicher, dass die Firewall-Richtlinie des Daten-LIF auf „mgmt“ (nicht „data“) eingestellt ist. Überspringen Sie diesen Schritt, wenn Sie zum Hinzufügen der SVM ein dediziertes Management-LIF verwenden. clustershell:> `network interface modify -lif <SVM_data_LIF_name> -firewall -policy mgmt`
- Wenn eine Firewall aktiviert ist, müssen Sie eine Ausnahme definiert haben, um TCP-Verkehr für den Port zuzulassen, der den Data ONTAP Data Collector verwendet.

  Sehen"Agentenanforderungen" für Konfigurationsinformationen. Dies gilt für lokale Agenten und in der Cloud installierte Agenten.

- Wenn ein Agent in einer AWS EC2-Instanz installiert wird, um eine Cloud ONTAP SVM zu überwachen, müssen sich Agent und Speicher im selben VPC befinden. Wenn sie sich in separaten VPCs befinden, muss eine gültige Route zwischen den VPCs vorhanden sein.

Testen der Konnektivität für Datensammler

Die Funktion zum Testen der Konnektivität (eingeführt im März 2025) soll Endbenutzern dabei helfen, die spezifischen Ursachen von Fehlern beim Einrichten von Datensammlern in Data Infrastructure Insights (DII) Workload Security zu identifizieren. Dadurch können die Benutzer Probleme im Zusammenhang mit der Netzwerkkommunikation oder fehlenden Rollen selbst beheben.

Mithilfe dieser Funktion können Benutzer vor dem Einrichten eines Datensammlers feststellen, ob alle netzwerkbezogenen Prüfungen durchgeführt wurden. Darüber hinaus werden Benutzer über die Funktionen informiert, auf die sie basierend auf der ONTAP Version, den Rollen und den ihnen in ONTAP zugewiesenen Berechtigungen zugreifen können.

Testkonnektivität wird für Benutzerverzeichnis-Collectors nicht unterstützt.

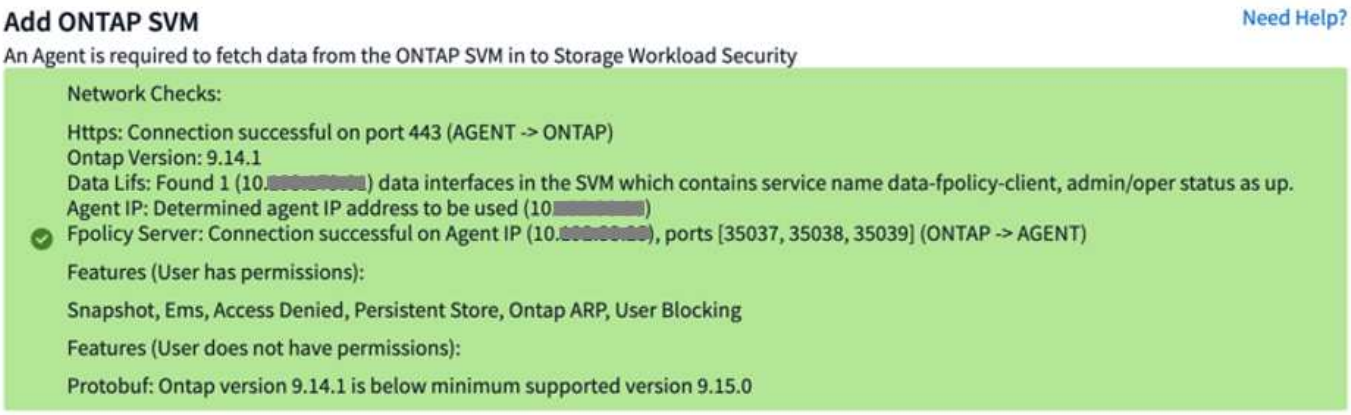
Voraussetzungen für den Verbindungstest

- Damit diese Funktion vollständig funktioniert, sind Anmeldeinformationen auf Clusterebene erforderlich.
- Die Überprüfung des Funktionszugriffs wird im SVM-Modus nicht unterstützt.
- Wenn Sie Anmeldeinformationen für die Clusterverwaltung verwenden, sind keine neuen Berechtigungen erforderlich.
- Wenn Sie einen benutzerdefinierten Benutzer verwenden (z. B. *csuser*), geben Sie die erforderlichen Berechtigungen und funktionsspezifischen Berechtigungen für die Funktionen an, die Sie verwenden möchten.

Lesen Sie unbedingt dieBerechtigungen Abschnitt weiter unten.

Testen der Verbindung

Der Benutzer kann zur Seite „Collector hinzufügen/bearbeiten“ gehen, die Details auf Clusterebene (im Clustermodus) oder auf SVM-Ebene (im SVM-Modus) eingeben und auf die Schaltfläche **Verbindung testen** klicken. Workload Security verarbeitet dann die Anfrage und zeigt eine entsprechende Erfolgs- oder Fehlermeldung an.



Voraussetzungen für die Benutzerzugriffssperre

Beachten Sie Folgendes für"Sperrung des Benutzerzugriffs" :

Damit diese Funktion funktioniert, sind Anmeldeinformationen auf Clusterebene erforderlich.

Wenn Sie Anmeldeinformationen für die Clusterverwaltung verwenden, sind keine neuen Berechtigungen erforderlich.

Wenn Sie einen benutzerdefinierten Benutzer (z. B. *csuser*) mit dem Benutzer erteilten Berechtigungen verwenden, befolgen Sie die Schritte in"Sperrung des Benutzerzugriffs" um Workload Security die Berechtigung zum Blockieren von Benutzern zu erteilen.

Ein Hinweis zu Berechtigungen

Berechtigungen beim Hinzufügen über Cluster Management IP:

Wenn Sie den Clusterverwaltungsadministratorbenutzer nicht verwenden können, um Workload Security Zugriff auf den ONTAP SVM-Datensammler zu gewähren, können Sie einen neuen Benutzer namens „csuser“ mit den in den folgenden Befehlen gezeigten Rollen erstellen. Verwenden Sie den Benutzernamen „csuser“ und das Kennwort für „csuser“, wenn Sie den Workload Security-Datenkollektor für die Verwendung der Cluster Management-IP konfigurieren.

Hinweis: Sie können eine einzelne Rolle erstellen, die für alle Funktionsberechtigungen eines benutzerdefinierten Benutzers verwendet wird. Wenn ein Benutzer vorhanden ist, löschen Sie zuerst den vorhandenen Benutzer und die Rolle mit diesen Befehlen:

```
security login delete -user-or-group-name csuser -application *
security login role delete -role csrole -cmddirname *
security login rest-role delete -role csrestrole -api *
security login rest-role delete -role arwrole -api *
```

Um den neuen Benutzer zu erstellen, melden Sie sich bei ONTAP mit dem Benutzernamen/Passwort des Clusterverwaltungsadministrators an und führen Sie die folgenden Befehle auf dem ONTAP -Server aus:

```
security login role create -role csrole -cmddirname DEFAULT -access
readonly
```

```
security login role create -role csrole -cmddirname "vserver fpolicy"
-access all
security login role create -role csrole -cmddirname "volume snapshot"
-access all -query "-snapshot cloudsecure_*"
security login role create -role csrole -cmddirname "event catalog"
-access all
security login role create -role csrole -cmddirname "event filter" -access
all
security login role create -role csrole -cmddirname "event notification
destination" -access all
security login role create -role csrole -cmddirname "event notification"
-access all
security login role create -role csrole -cmddirname "security certificate"
-access all
security login role create -role csrole -cmddirname "cluster application-
record" -access all
security login create -user-or-group-name csuser -application ontapi
-authmethod password -role csrole
security login create -user-or-group-name csuser -application ssh
-authmethod password -role csrole
security login create -user-or-group-name csuser -application http
-authmethod password -role csrole
```

Berechtigungen beim Hinzufügen über Vserver Management IP:

Wenn Sie den Clusterverwaltungsadministratorbenutzer nicht verwenden können, um Workload Security Zugriff auf den ONTAP SVM-Datensammler zu gewähren, können Sie einen neuen Benutzer namens „csuser“ mit den in den folgenden Befehlen gezeigten Rollen erstellen. Verwenden Sie den Benutzernamen „csuser“ und das Kennwort für „csuser“, wenn Sie den Workload Security-Datensammler für die Verwendung der Vserver Management IP konfigurieren.

Hinweis: Sie können eine einzelne Rolle erstellen, die für alle Funktionsberechtigungen eines benutzerdefinierten Benutzers verwendet wird. Wenn ein Benutzer vorhanden ist, löschen Sie zuerst den vorhandenen Benutzer und die Rolle mit diesen Befehlen:

```
security login delete -user-or-group-name csuser -application * -vserver
<vservername>
security login role delete -role csrole -cmddirname * -vserver
<vservername>
security login rest-role delete -role csrestrole -api * -vserver
<vservername>
```

Um den neuen Benutzer zu erstellen, melden Sie sich mit dem Benutzernamen/Passwort des Clusterverwaltungsadministrators bei ONTAP an und führen Sie die folgenden Befehle auf dem ONTAP Server aus. Kopieren Sie diese Befehle der Einfachheit halber in einen Texteditor und ersetzen Sie <vservername> durch Ihren Vserver-Namen, bevor Sie diese Befehle auf ONTAP ausführen:

```
security login role create -vserver <vservername> -role csrole -cmddirname
DEFAULT -access none
```

```
security login role create -vserver <vservername> -role csrole -cmddirname
"network interface" -access readonly
security login role create -vserver <vservername> -role csrole -cmddirname
version -access readonly
security login role create -vserver <vservername> -role csrole -cmddirname
volume -access readonly
security login role create -vserver <vservername> -role csrole -cmddirname
vserver -access readonly
```

```
security login role create -vserver <vservername> -role csrole -cmddirname
"vserver fpolicy" -access all
security login role create -vserver <vservername> -role csrole -cmddirname
"volume snapshot" -access all
```

```
security login create -user-or-group-name csuser -application ontapi
-authmethod password -role csrole -vserver <vservername>
security login create -user-or-group-name csuser -application http
-authmethod password -role csrole -vserver <vservername>
```

Protobuf-Modus

Workload Security konfiguriert die FPolicy-Engine im Protobuf-Modus, wenn diese Option in den *Erweiterten Konfigurationseinstellungen* des Collectors aktiviert ist. Der Protobuf-Modus wird in ONTAP Version 9.15 und höher unterstützt.

Weitere Einzelheiten zu dieser Funktion finden Sie im"ONTAP-Dokumentation" .

Für protobuf sind bestimmte Berechtigungen erforderlich (einige oder alle davon sind möglicherweise bereits vorhanden):

Cluster-Modus:

```
 security login role create -role csrole -cmddirname "vserver fpolicy"
-access all
VServer-Modus:
```

```
security login role create -vserver <vservername> -role csrole -cmddirname
"vserver fpolicy" -access all
```

Berechtigungen für ONTAP Autonomous Ransomware Protection und ONTAP Access Denied

Wenn Sie Anmeldeinformationen für die Clusterverwaltung verwenden, sind keine neuen Berechtigungen erforderlich.

Wenn Sie einen benutzerdefinierten Benutzer (z. B. *csuser*) mit dem Benutzer erteilten Berechtigungen verwenden, führen Sie die folgenden Schritte aus, um Workload Security die Berechtigung zum Sammeln von ARP-bezogenen Informationen von ONTAP zu erteilen.

Weitere Informationen finden Sie unter"Integration mit ONTAP Access Denied"

Und"Integration mit ONTAP Autonomous Ransomware Protection"

Konfigurieren des Datensammlers

Schritte zur Konfiguration

1. Melden Sie sich als Administrator oder Kontoinhaber bei Ihrer Data Infrastructure Insights Umgebung an.
2. Klicken Sie auf **Workload-Sicherheit > Collectors > +Datensammler**

   Das System zeigt die verfügbaren Datensammler an.

3. Bewegen Sie den Mauszeiger über die Kachel * NetApp SVM und klicken Sie auf **+Überwachen**.

   Das System zeigt die ONTAP SVM-Konfigurationsseite an. Geben Sie für jedes Feld die erforderlichen Daten ein.

Feld	Beschreibung
Name	Eindeutiger Name für den Datensammler
Agent	Wählen Sie einen konfigurierten Agenten aus der Liste aus.
Verbindung über Management-IP für:	Wählen Sie entweder Cluster-IP oder SVM-Verwaltungs-IP
Cluster-/SVM-Verwaltungs-IP-Adresse	Die IP-Adresse für den Cluster oder die SVM, abhängig von Ihrer obigen Auswahl.
Name SVM	Der Name der SVM (dieses Feld ist erforderlich, wenn eine Verbindung über die Cluster-IP hergestellt wird)
Benutzername	Benutzername für den Zugriff auf SVM/Cluster. Beim Hinzufügen über die Cluster-IP sind die Optionen: 1. Cluster-Administrator 2. 'csuser' 3. AD-Benutzer mit ähnlicher Rolle wie csuser. Beim Hinzufügen über die SVM-IP sind die Optionen: 4. vsadmin 5. 'csuser' 6. AD-Benutzername mit ähnlicher Rolle wie csuser.
Passwort	Passwort für den oben genannten Benutzernamen
Filtern von Anteilen/Volumes	Wählen Sie, ob Freigaben/Volumes in die Ereigniserfassung einbezogen oder ausgeschlossen werden sollen

Geben Sie die vollständigen Freigabenamen ein, die ausgeschlossen/eingeschlossen werden sollen	Durch Kommas getrennte Liste von Freigaben, die (je nach Bedarf) aus der Ereignissammlung ausgeschlossen oder eingeschlossen werden sollen
Geben Sie vollständige Volumenamen ein, die ausgeschlossen/eingeschlossen werden sollen	Durch Kommas getrennte Liste der Datenträger, die (je nach Bedarf) von der Ereigniserfassung ausgeschlossen oder eingeschlossen werden sollen
Ordnerzugriff überwachen	Wenn diese Option aktiviert ist, werden Ereignisse für die Ordnerzugriffsüberwachung aktiviert. Beachten Sie, dass das Erstellen/Umbenennen und Löschen von Ordnern auch ohne Auswahl dieser Option überwacht wird. Durch die Aktivierung wird die Anzahl der überwachten Ereignisse erhöht.
ONTAP Sendepuffergröße festlegen	Legt die Größe des ONTAP Fpolicy-Sendepuffers fest. Wenn eine ONTAP Version vor 9.8p7 verwendet wird und Leistungsprobleme auftreten, kann die Größe des ONTAP Sendepuffers geändert werden, um die ONTAP Leistung zu verbessern. Wenden Sie sich an den NetApp -Support, wenn Sie diese Option nicht sehen und sie ausprobieren möchten.

Nach Abschluss

- Verwenden Sie auf der Seite „Installierte Datensammler“ das Optionsmenü rechts neben jedem Sammler, um den Datensammler zu bearbeiten. Sie können den Datensammler neu starten oder die Konfigurationsattribute des Datensammlers bearbeiten.

Empfohlene Konfiguration für MetroCluster

Folgendes wird für MetroCluster empfohlen:

1. Verbinden Sie zwei Datensammler, einen mit dem Quell-SVM und einen mit dem Ziel-SVM.
2. Die Datensammler sollten über *Cluster-IP* verbunden sein.
3. Der Datensammler des aktuell „laufenden“ SVM wird jederzeit als „*Läuft*“ angezeigt. Der aktuell „gestoppte“ Datensammler des SVM wird als *Gestoppt* angezeigt.
4. Bei jeder Umschaltung ändert sich der Status des Datensammlers von *Läuft* zu *Gestoppt* und umgekehrt.
5. Es dauert bis zu zwei Minuten, bis der Datensammler vom Status „Gestoppt“ in den Status „Läuft“ wechselt.

Servicerichtlinie

Wenn Sie die Servicerichtlinie mit ONTAP **Version 9.9.1 oder neuer** verwenden, ist zum Herstellen einer Verbindung mit dem Data Source Collector der Dienst *data-fpolicy-client* zusammen mit dem Datendienst *data-nfs* und/oder *data-cifs* erforderlich.

Beispiel:

```
Testcluster-1:*> net int service-policy create -policy only_data_fpolicy
-allowed-addresses 0.0.0.0/0 -vserver aniket_svm
-services data-cifs,data-nfs,data,-core,data-fpolicy-client
(network interface service-policy create)
```

In ONTAP -Versionen vor 9.9.1 muss *data-fpolicy-client* nicht festgelegt werden.

Play-Pause-Datensammler

Wenn sich der Datensammler im Status „Wird ausgeführt“ befindet, können Sie die Sammlung anhalten. Öffnen Sie das „Drei-Punkte“-Menü für den Collector und wählen Sie PAUSE. Während der Collector angehalten ist, werden keine Daten von ONTAP gesammelt und keine Daten vom Collector an ONTAP gesendet. Dies bedeutet, dass keine Fpolicy-Ereignisse von ONTAP zum Datensammler und von dort zu Data Infrastructure Insights fließen.

Beachten Sie, dass Workload Security die Daten nicht sammelt, wenn auf ONTAP neue Volumes usw. erstellt werden, während der Collector angehalten ist, und dass diese Volumes usw. nicht in Dashboards oder Tabellen angezeigt werden.

Ein Collector kann nicht angehalten werden, wenn er über eingeschränkte Benutzer verfügt. Stellen Sie den Benutzerzugriff wieder her, bevor Sie den Collector anhalten.

Beachten Sie Folgendes:

- Gemäß den für einen angehaltenen Collector konfigurierten Einstellungen wird keine Snapshot-Bereinigung durchgeführt.
- EMS-Ereignisse (wie ONTAP ARP) werden auf einem angehaltenen Collector nicht verarbeitet. Das bedeutet, dass Data Infrastructure Insights Workload Security dieses Ereignis nicht erfassen kann, wenn ONTAP einen Ransomware-Angriff erkennt.
- Für einen pausierten Collector werden KEINE E-Mails mit Gesundheitsbenachrichtigungen gesendet.
- Manuelle oder automatische Aktionen (wie Snapshot oder Benutzerblockierung) werden bei einem angehaltenen Collector nicht unterstützt.
- Bei Agent- oder Collector-Upgrades, Neustarts/Neustarts der Agent-VM oder Neustarts des Agent-Dienstes bleibt ein angehaltener Collector im Status *Angehalten*.
- Wenn sich der Datensammler im Status *Fehler* befindet, kann der Sammler nicht in den Status *Pausiert* geändert werden. Die Schaltfläche „Pause“ wird nur aktiviert, wenn der Status des Collectors „Wird ausgeführt“ ist.
- Wenn die Verbindung zum Agenten getrennt wird, kann der Collector nicht in den Status *Pausiert* versetzt werden. Der Collector wechselt in den Status „Gestoppt“ und die Schaltfläche „Pause“ wird deaktiviert.

Persistenter Speicher

Persistenter Speicher wird mit ONTAP 9.14.1 und höher unterstützt. Beachten Sie, dass die Anweisungen für Volumenamen von ONTAP 9.14 bis 9.15 variieren.

Der persistente Speicher kann durch Aktivieren des Kontrollkästchens auf der Seite „Bearbeiten/Hinzufügen“ des Collectors aktiviert werden. Nach dem Aktivieren des Kontrollkästchens wird ein Textfeld zur Annahme des Datenträgernamens angezeigt. Der Volumename ist ein Pflichtfeld zum Aktivieren des persistenten Speichers.

- Für ONTAP 9.14.1 müssen Sie das Volume vor der Aktivierung der Funktion erstellen und im Feld *Volume Name* denselben Namen angeben. Die empfohlene Volumegröße beträgt 16 GB.
- Für ONTAP 9.15.1 wird das Volume vom Collector automatisch mit einer Größe von 16 GB erstellt, wobei der im Feld *Volume Name* angegebene Name verwendet wird.

Für den persistenten Speicher sind bestimmte Berechtigungen erforderlich (einige oder alle davon sind möglicherweise bereits vorhanden):

Cluster-Modus:

```
security login role create -role csrole -cmddirname "vserver fpolicy"
-access all
security login role create -role csrole -cmddirname "job show" -access
readonly
```

VServer-Modus:

```
security login role create -vserver <vservername> -role csrole -cmddirname
"vserver fpolicy" -access all
security login role create -vserver <vservername> -role csrole -cmddirname
"job show" -access readonly
```

Migrieren von Collectoren

Sie können einen Workload Security-Collector problemlos von einem Agenten auf einen anderen migrieren und so einen effizienten Lastenausgleich der Collector-Instanzen zwischen den Agenten ermöglichen.

Voraussetzungen

- Der Quellagent muss sich im Status *verbunden* befinden.
- Der zu migrierende Collector muss sich im Status „Laufend“ befinden.

Hinweis:

- Migrate wird sowohl für Daten- als auch für Benutzerverzeichnis-Sammler unterstützt.
- Die Migration eines Collectors wird für manuell verwaltete Mandanten nicht unterstützt.

Migrieren des Collectors

Um einen Collector zu migrieren, führen Sie die folgenden Schritte aus:

1. Gehen Sie zur Seite „Collector bearbeiten“.
2. Wählen Sie einen Zielagenten aus der Agenten-Dropdownliste aus.
3. Klicken Sie auf die Schaltfläche „Collector speichern“.

Workload Security verarbeitet die Anfrage. Nach erfolgreicher Migration wird der Benutzer zur Seite mit der Sammlerliste weitergeleitet. Im Fehlerfall wird auf der Bearbeitungsseite eine entsprechende Meldung angezeigt.

Hinweis: Alle zuvor auf der Seite „Collector bearbeiten“ vorgenommenen Konfigurationsänderungen bleiben auch nach der erfolgreichen Migration des Collectors zum Zielagenten wirksam.

Fehlerbehebung

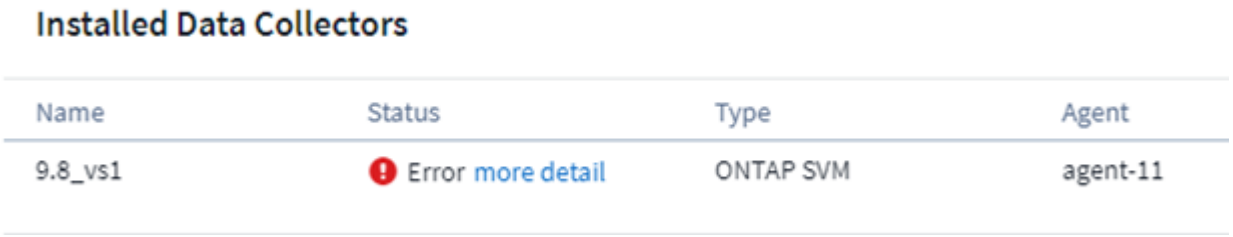
Siehe die"Fehlerbehebung beim SVM Collector" Seite für Tipps zur Fehlerbehebung.

Fehlerbehebung beim ONTAP SVM Data Collector

Workload Security verwendet Datensammler, um Datei- und Benutzerzugriffsdaten von Geräten zu erfassen. Hier finden Sie Tipps zur Behebung von Problemen mit diesem Collector.

Siehe die"Konfigurieren des SVM-Collectors" Seite für Anweisungen zum Konfigurieren dieses Collectors.

Im Falle eines Fehlers können Sie auf der Seite „Installierte Datensammler“ in der Spalte „Status“ auf „Weitere Details“ klicken, um Einzelheiten zum Fehler anzuzeigen.



Bekannte Probleme und deren Lösungen werden unten beschrieben.

Problem: Der Datensammler läuft eine Zeit lang und stoppt nach einer zufälligen Zeit mit der Fehlermeldung: „Fehlermeldung: Connector befindet sich im Fehlerzustand.“ Dienstname: Audit. Grund für den Fehler: Externer fpolicy-Server überlastet."

Versuchen Sie Folgendes: Die Ereignisrate von ONTAP war viel höher als das, was die Agent-Box verarbeiten kann. Daher wurde die Verbindung beendet.

Überprüfen Sie den Spitzenverkehr in CloudSecure, als die Verbindung getrennt wurde. Dies können Sie auf der Seite **CloudSecure > Aktivitätsforensik > Alle Aktivitäten** überprüfen.

Wenn der aggregierte Spitzenverkehr höher ist als das, was die Agent Box verarbeiten kann, lesen Sie auf der Seite „Event Rate Checker“ nach, wie Sie die Größe für die Collector-Bereitstellung in einer Agent Box festlegen.

Wenn der Agent vor dem 4. März 2021 in der Agent-Box installiert wurde, führen Sie die folgenden Befehle in der Agent-Box aus:

```
echo 'net.core.rmem_max=8388608' >> /etc/sysctl.conf
echo 'net.ipv4.tcp_rmem = 4096 2097152 8388608' >> /etc/sysctl.conf
sysctl -p
```

Starten Sie den Collector nach der Größenänderung über die Benutzeroberfläche neu.

Problem: Der Collector meldet die Fehlermeldung: „Auf dem Connector wurde keine lokale IP-Adresse gefunden, die die Datenschnittstellen der SVM erreichen kann.“ **Versuchen Sie Folgendes:** Dies liegt höchstwahrscheinlich an einem Netzwerkproblem auf der ONTAP Seite. Bitte befolgen Sie diese Schritte:

1. Stellen Sie sicher, dass auf der SVM-Daten- oder Verwaltungsebene keine Firewalls vorhanden sind, die die Verbindung von der SVM blockieren.
2. Wenn Sie eine SVM über eine Cluster-Management-IP hinzufügen, stellen Sie sicher, dass die Datenlebensdauer und die Managementlebensdauer der SVM von der Agent-VM aus pingbar sind. Überprüfen Sie bei Problemen das Gateway, die Netzmaske und die Routen für das Leben.

   Sie können auch versuchen, sich über SSH mit der Cluster-Verwaltungs-IP beim Cluster anzumelden und die Agent-IP anzupingen. Stellen Sie sicher, dass die Agent-IP pingbar ist:

   ```
   network ping -vserver <vserver name> -destination <Agent IP> -lif
   <Lif Name> -show-detail
   ```

   Wenn kein Ping möglich ist, stellen Sie sicher, dass die Netzwerkeinstellungen in ONTAP korrekt sind, sodass der Agent-Computer pingbar ist.
3. Wenn Sie versucht haben, eine Verbindung über die Cluster-IP herzustellen, und dies nicht funktioniert hat, versuchen Sie, eine direkte Verbindung über die SVM-IP herzustellen. Die Schritte zum Herstellen einer Verbindung über die SVM-IP finden Sie oben.
4. Überprüfen Sie beim Hinzufügen des Collectors über die SVM-IP und die VSadmin-Anmeldeinformationen, ob für SVM Lif die Rolle „Data plus Mgmt“ aktiviert ist. In diesem Fall funktioniert ein Ping zum SVM Lif, ein SSH zum SVM Lif funktioniert jedoch nicht. Wenn ja, erstellen Sie ein SVM Mgmt Only Lif und versuchen Sie, über dieses SVM Management Only Lif eine Verbindung herzustellen.
5. Wenn es immer noch nicht funktioniert, erstellen Sie ein neues SVM-Lif und versuchen Sie, über dieses Lif eine Verbindung herzustellen. Stellen Sie sicher, dass die Subnetzmaske richtig eingestellt ist.
6. Erweitertes Debuggen:
   a. Starten Sie eine Paketverfolgung in ONTAP.
   b. Versuchen Sie, einen Datensammler über die CloudSecure-Benutzeroberfläche mit dem SVM zu verbinden.
   c. Warten Sie, bis der Fehler auftritt. Stoppen Sie die Paketverfolgung in ONTAP.
   d. Öffnen Sie die Paketverfolgung von ONTAP. Es ist an diesem Standort verfügbar

```
 https://<cluster_mgmt_ip>/spi/<clustername>/etc/log/packet_traces/
.. Stellen Sie sicher, dass ein SYN von ONTAP zur Agent-Box vorhanden ist.
.. Wenn kein SYN von ONTAP vorhanden ist, liegt ein Problem mit der Firewall in ONTAP vor.
.. Öffnen Sie die Firewall in ONTAP, damit ONTAP eine Verbindung zur Agent-Box herstellen kann.
```

7. Wenn es immer noch nicht funktioniert, wenden Sie sich bitte an das Netzwerkteam, um sicherzustellen, dass keine externe Firewall die Verbindung von ONTAP zur Agent-Box blockiert.
8. Wenn keine der oben genannten Maßnahmen das Problem löst, eröffnen Sie einen Fall bei"Netapp-Support" für weitere Unterstützung.

Problem: Meldung: „ ONTAP -Typ für [Hostname: <IP-Adresse>] konnte nicht ermittelt werden. Grund: Verbindungsfehler zum Speichersystem <IP-Adresse>: Host ist nicht erreichbar (Host nicht erreichbar)"
Versuchen Sie Folgendes:

1. Überprüfen Sie, ob die richtige SVM-IP-Verwaltungsadresse oder Cluster-Verwaltungs-IP angegeben wurde.
2. Stellen Sie per SSH eine Verbindung zum SVM oder Cluster her, zu dem Sie eine Verbindung herstellen möchten. Sobald Sie verbunden sind, stellen Sie sicher, dass der SVM- oder Clustername korrekt ist.

Problem: Fehlermeldung: „Connector befindet sich im Fehlerzustand. Dienstname: Audit. Grund für den Fehler: Externer fpolicy-Server beendet." **Versuchen Sie Folgendes:**

1. Höchstwahrscheinlich blockiert eine Firewall die erforderlichen Ports auf dem Agent-Computer. Überprüfen Sie, ob der Portbereich 35000–55000/TCP für die Agent-Maschine geöffnet ist, damit sie eine Verbindung vom SVM herstellen kann. Stellen Sie außerdem sicher, dass auf der ONTAP -Seite keine Firewalls aktiviert sind, die die Kommunikation mit dem Agent-Computer blockieren.
2. Geben Sie den folgenden Befehl in das Agent-Feld ein und stellen Sie sicher, dass der Portbereich geöffnet ist.

   ```
   sudo iptables-save | grep 3500*
   ```

   Die Beispielausgabe sollte folgendermaßen aussehen:

   ```
    -A IN_public_allow -p tcp -m tcp --dport 35000 -m conntrack
   -ctstate NEW -j ACCEPT
   . Melden Sie sich bei SVM an, geben Sie die folgenden Befehle ein
   und überprüfen Sie, dass keine Firewall eingerichtet ist, die die
   Kommunikation mit ONTAP blockiert.
   ```

   ```
   system services firewall show
   system services firewall policy show
   ```

   "Firewall-Befehle prüfen"auf der ONTAP -Seite.

3. Stellen Sie per SSH eine Verbindung zum SVM/Cluster her, den Sie überwachen möchten. Pingen Sie die Agent-Box vom SVM-Datenlebenszyklus aus (mit Unterstützung für CIFS- und NFS-Protokolle) und stellen Sie sicher, dass der Ping funktioniert:

   ```
   network ping -vserver <vserver name> -destination <Agent IP> -lif
   <Lif Name> -show-detail
   ```

   Wenn kein Ping möglich ist, stellen Sie sicher, dass die Netzwerkeinstellungen in ONTAP korrekt sind, sodass der Agent-Computer pingbar ist.

4. Wenn ein einzelner SVM über zwei Datensammler zweimal zu einem Mandanten hinzugefügt wird, wird dieser Fehler angezeigt. Löschen Sie einen der Datensammler über die Benutzeroberfläche. Starten Sie dann den anderen Datensammler über die Benutzeroberfläche neu. Anschließend zeigt der Datensammler den Status „RUNNING“ an und beginnt mit dem Empfang von Ereignissen vom SVM.

   Grundsätzlich sollte in einem Mandanten 1 SVM nur einmal über 1 Datensammler hinzugefügt werden. 1 SVM sollte nicht zweimal über 2 Datensammler hinzugefügt werden.

5. In Fällen, in denen dieselbe SVM in zwei verschiedenen Workload Security-Umgebungen

(Mandanten) hinzugefügt wurde, ist die letzte immer erfolgreich. Der zweite Collector konfiguriert fpolicy mit seiner eigenen IP-Adresse und wirft den ersten raus. Der Collector im ersten empfängt also keine Ereignisse mehr und sein „Audit“-Dienst wechselt in einen Fehlerzustand. Um dies zu verhindern, konfigurieren Sie jede SVM in einer einzelnen Umgebung.

6. Dieser Fehler kann auch auftreten, wenn die Servicerichtlinien nicht richtig konfiguriert sind. Um bei ONTAP 9.8 oder höher eine Verbindung zum Data Source Collector herzustellen, ist der Dienst data-fpolicy-client zusammen mit dem Datendienst data-nfs und/oder data-cifs erforderlich. Darüber hinaus muss der Dienst „data-fpolicy-client“ mit den Datenlebensdauern für die überwachte SVM verknüpft werden.

Problem: Auf der Aktivitätsseite wurden keine Ereignisse angezeigt. **Versuchen Sie Folgendes:**

1. Überprüfen Sie, ob sich der ONTAP Collector im Status „RUNNING“ befindet. Wenn ja, stellen Sie sicher, dass einige CIFS-Ereignisse auf den CIFS-Client-VMs generiert werden, indem Sie einige Dateien öffnen.
2. Wenn keine Aktivitäten angezeigt werden, melden Sie sich bitte beim SVM an und geben Sie den folgenden Befehl ein.

   ```
   <SVM>event log show -source fpolicy
   ```

   Bitte stellen Sie sicher, dass keine Fehler im Zusammenhang mit fpolicy vorliegen.

3. Wenn keine Aktivitäten angezeigt werden, melden Sie sich bitte beim SVM an. Geben Sie den folgenden Befehl ein:

   ```
   <SVM>fpolicy show
   ```

   Überprüfen Sie, ob die fpolicy-Richtlinie mit dem Präfix „cloudsecure_“ festgelegt wurde und der Status „Ein“ ist. Wenn nicht festgelegt, kann der Agent die Befehle im SVM höchstwahrscheinlich nicht ausführen. Bitte stellen Sie sicher, dass alle Voraussetzungen, wie am Anfang der Seite beschrieben, erfüllt sind.

Problem: Der SVM-Datensammler befindet sich im Fehlerzustand und die Fehlermeldung lautet „Der Agent konnte keine Verbindung zum Sammler herstellen.“ **Versuchen Sie Folgendes:**

1. Höchstwahrscheinlich ist der Agent überlastet und kann keine Verbindung zu den Datenquellen-Sammlern herstellen.
2. Überprüfen Sie, wie viele Datenquellensammler mit dem Agenten verbunden sind.
3. Überprüfen Sie auch die Datenflussrate auf der Seite „Alle Aktivitäten“ in der Benutzeroberfläche.
4. Wenn die Anzahl der Aktivitäten pro Sekunde sehr hoch ist, installieren Sie einen anderen Agenten und verschieben Sie einige der Datenquellensammler auf den neuen Agenten.

Problem: SVM Data Collector zeigt die Fehlermeldung „fpolicy.server.connectError: Knoten konnte keine Verbindung mit dem FPolicy-Server „12.195.15.146“ herstellen (Grund: „Select Timed out“)“ an. **Versuchen Sie Folgendes:** Die Firewall ist in SVM/Cluster aktiviert. Daher kann die fpolicy-Engine keine Verbindung zum fpolicy-Server herstellen. CLIs in ONTAP , die zum Abrufen weiterer Informationen verwendet werden können, sind:

```
event log show -source fpolicy which shows the error
event log show -source fpolicy -fields event,action,description which
shows more details.
```

"Firewall-Befehle prüfen"auf der ONTAP -Seite.

Problem: Fehlermeldung: „Der Connector befindet sich im Fehlerzustand. Dienstname: Audit. Grund für den Fehler: Auf der SVM wurde keine gültige Datenschnittstelle (Rolle: Daten, Datenprotokolle: NFS oder CIFS oder beide, Status: aktiv) gefunden.“ **Versuchen Sie Folgendes:** Stellen Sie sicher, dass eine funktionsfähige Schnittstelle vorhanden ist (mit der Rolle „Daten“ und dem Datenprotokoll „CIFS/NFS“).

Problem: Der Datensammler wechselt in den Fehlerzustand und nach einiger Zeit in den RUNNING-Zustand und dann wieder zurück in den Fehlerzustand. Dieser Zyklus wiederholt sich. **Versuchen Sie Folgendes:** Dies geschieht normalerweise im folgenden Szenario:

1. Es wurden mehrere Datensammler hinzugefügt.
2. Den Datensammlern, die dieses Verhalten zeigen, wird 1 SVM hinzugefügt. Das bedeutet, dass zwei oder mehr Datensammler mit einem SVM verbunden sind.
3. Stellen Sie sicher, dass 1 Datensammler nur mit 1 SVM verbunden ist.
4. Löschen Sie die anderen Datensammler, die mit derselben SVM verbunden sind.

Problem: Der Connector befindet sich im Fehlerzustand. Dienstname: Audit. Grund für den Fehler: Fehler beim Konfigurieren (Richtlinie auf SVM svmname). Grund: Ungültiger Wert für das Element „shares-to-include“ in „fpolicy.policy.scope-modify: „Federal“ angegeben. **Versuchen Sie Folgendes:** *Die Freigabenamen müssen ohne Anführungszeichen angegeben werden. Bearbeiten Sie die ONTAP SVM DSC-Konfiguration, um die Freigabenamen zu korrigieren.

Freigaben einschließen und ausschließen ist nicht für eine lange Liste von Freigabenamen vorgesehen. Verwenden Sie stattdessen die Filterung nach Volumen, wenn Sie eine große Anzahl von Aktien ein- oder ausschließen möchten.

Problem: Es gibt im Cluster vorhandene fpolicies, die nicht verwendet werden. Was sollte vor der Installation von Workload Security damit geschehen? **Versuchen Sie Folgendes:** Es wird empfohlen, alle vorhandenen, nicht verwendeten fpolicy-Einstellungen zu löschen, auch wenn sie getrennt sind. Workload Security erstellt fpolicy mit dem Präfix „cloudsecure_“. Alle anderen nicht verwendeten fpolicy-Konfigurationen können gelöscht werden.

CLI-Befehl zum Anzeigen der fpolicy-Liste:

```
 fpolicy show
Schritte zum Löschen von fpolicy-Konfigurationen:
```

```
fpolicy disable -vserver <svmname> -policy-name <policy_name>
fpolicy policy scope delete -vserver <svmname> -policy-name
<policy_name>
fpolicy policy delete -vserver <svmname> -policy-name <policy_name>
fpolicy policy event delete -vserver <svmname> -event-name
<event_list>
fpolicy policy external-engine delete -vserver <svmname> -engine-name
<engine_name>
```

|Nach der Aktivierung der Workload-Sicherheit wird die ONTAP Leistung beeinträchtigt: Die Latenz wird sporadisch hoch, die IOPs werden sporadisch niedrig. |Bei der Verwendung von ONTAP mit Workload Security können manchmal Latenzprobleme in ONTAP auftreten. Hierfür gibt es eine Reihe möglicher Gründe, die im Folgenden aufgeführt sind:"1372994" , "1415152" , "1438207" , "1479704" , "1354659" . Alle diese Probleme wurden in ONTAP 9.13.1 und höher behoben. Es wird dringend empfohlen, eine dieser neueren Versionen zu verwenden.

Problem: Beim Datensammler liegt ein Fehler vor, diese Fehlermeldung wird angezeigt. „Fehler: Connector befindet sich im Fehlerzustand. Dienstname: Audit. Grund für den Fehler: Die Richtlinie konnte auf SVM svm_test nicht konfiguriert werden. Grund: Fehlender Wert für Zapi-Feld: Ereignisse. „ **Versuchen Sie Folgendes:**

1. Beginnen Sie mit einer neuen SVM, auf der nur der NFS-Dienst konfiguriert ist.
2. Fügen Sie in Workload Security einen ONTAP SVM-Datensammler hinzu. CIFS wird als zulässiges Protokoll für die SVM konfiguriert, während der ONTAP SVM Data Collector in Workload Security hinzugefügt wird.
3. Warten Sie, bis der Datensammler in Workload Security einen Fehler anzeigt.
4. Da der CIFS-Server NICHT auf der SVM konfiguriert ist, wird dieser links angezeigte Fehler von Workload Security angezeigt.
5. Bearbeiten Sie den ONTAP SVM-Datensammler und deaktivieren Sie CIFs als zulässiges Protokoll. Speichern Sie den Datensammler. Es wird nur mit aktiviertem NFS-Protokoll ausgeführt.

Problem: Der Datensammler zeigt die Fehlermeldung an: „Fehler: Der Zustand des Sammlers konnte innerhalb von 2 Versuchen nicht ermittelt werden. Versuchen Sie, den Sammler erneut neu zu starten (Fehlercode: AGENT008)“. **Versuchen Sie Folgendes:**

1. Scrollen Sie auf der Seite „Datensammler“ nach rechts neben den Datensammler, der den Fehler ausgibt, und klicken Sie auf das Menü mit den drei Punkten. Wählen Sie *Bearbeiten*. Geben Sie das Passwort des Datensammlers erneut ein. Speichern Sie den Datensammler, indem Sie auf die Schaltfläche *Speichern* klicken. Data Collector wird neu gestartet und der Fehler sollte behoben sein.
2. Die Agent-Maschine verfügt möglicherweise nicht über genügend CPU- oder RAM-Reserve, weshalb die DSCs ausfallen. Bitte überprüfen Sie die Anzahl der Datensammler, die dem Agenten auf der Maschine hinzugefügt wurden. Wenn es mehr als 20 sind, erhöhen Sie bitte die CPU- und RAM-Kapazität der Agent-Maschine. Sobald die CPU und der RAM erhöht werden, wechseln die DSCs automatisch in den Initialisierungs- und dann in den Ausführungszustand. Schauen Sie in die Größentabelle auf"diese Seite" .

Problem: Der Datensammler gibt einen Fehler aus, wenn der SVM-Modus ausgewählt ist. **Versuchen Sie Folgendes:** Wenn beim Verbinden im SVM-Modus die Cluster-Management-IP anstelle der SVM-Management-IP zum Verbinden verwendet wird, tritt ein Verbindungsfehler auf. Stellen Sie sicher, dass die richtige SVM-IP verwendet wird.

Problem: Der Datensammler zeigt eine Fehlermeldung an, wenn die Funktion „Zugriff verweigert“ aktiviert ist: „Connector befindet sich im Fehlerzustand. Dienstname: Audit. Grund für den Fehler: Fehler beim Konfigurieren von fpolicy auf SVM test_svm. Grund: Der Benutzer ist nicht autorisiert." **Versuchen Sie Folgendes:** Dem Benutzer fehlen möglicherweise die REST-Berechtigungen, die für die Funktion „Zugriff verweigert“ erforderlich sind. Bitte folgen Sie den Anweisungen auf"diese Seite" um die Berechtigungen festzulegen.

Starten Sie den Collector neu, sobald die Berechtigungen festgelegt sind.

Wenn weiterhin Probleme auftreten, verwenden Sie die Support-Links auf der Seite **Hilfe > Support**.

Konfigurieren des Cloud Volumes ONTAP und Amazon FSx for NetApp ONTAP

Workload Security verwendet Datensammler, um Datei- und Benutzerzugriffsdaten von Geräten zu erfassen.

Cloud Volumes ONTAP Speicherkonfiguration

Informationen zum Konfigurieren einer AWS-Instanz mit einem einzelnen Knoten/HA zum Hosten des Workload Security Agent finden Sie in der OnCommand Cloud Volumes ONTAP Dokumentation:https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/index.html[]

Nachdem die Konfiguration abgeschlossen ist, befolgen Sie die Schritte zum Einrichten Ihres SVM:https://docs.netapp.com/us-en/cloudinsights/task_add_collector_svm.html[]

Unterstützte Plattformen

- Cloud Volumes ONTAP, wird von allen verfügbaren Cloud-Service-Anbietern unterstützt, sofern verfügbar. Zum Beispiel: Amazon, Azure, Google Cloud.
- ONTAP Amazon FSx

Agent-Computerkonfiguration

Die Agent-Maschine muss in den jeweiligen Subnetzen der Cloud-Dienstanbieter konfiguriert werden. Weitere Informationen zum Netzwerkzugriff finden Sie in den [Agentenanforderungen].

Nachfolgend finden Sie die Schritte zur Agenteninstallation in AWS. Für die Installation können in Azure oder Google Cloud die entsprechenden Schritte ausgeführt werden, sofern diese für den Cloud-Dienstanbieter gelten.

Führen Sie in AWS die folgenden Schritte aus, um die Maschine für die Verwendung als Workload Security Agent zu konfigurieren:

Führen Sie die folgenden Schritte aus, um die Maschine für die Verwendung als Workload Security Agent zu konfigurieren:

Schritte

1. Melden Sie sich bei der AWS-Konsole an, navigieren Sie zur Seite „EC2-Instances“ und wählen Sie „Instanz starten“ aus.
2. Wählen Sie ein RHEL- oder CentOS-AMI mit der entsprechenden Version aus, wie auf dieser Seite erwähnt:https://docs.netapp.com/us-en/cloudinsights/concept_cs_agent_requirements.html[]
3. Wählen Sie die VPC und das Subnetz aus, in denen sich die Cloud ONTAP -Instanz befindet.
4. Wählen Sie *t2.xlarge* (4 vcpus und 16 GB RAM) als zugewiesene Ressourcen.
    a. Erstellen Sie die EC2-Instanz.
5. Installieren Sie die erforderlichen Linux-Pakete mit dem YUM-Paketmanager:
    a. Installieren Sie *wget* und *unzip* native Linux-Pakete.

Installieren des Workload Security Agent

1. Melden Sie sich als Administrator oder Kontoinhaber bei Ihrer Data Infrastructure Insights Umgebung an.
2. Navigieren Sie zu Workload Security **Collectors** und klicken Sie auf die Registerkarte **Agents**.
3. Klicken Sie auf **+Agent** und geben Sie RHEL als Zielplattform an.
4. Kopieren Sie den Befehl zur Agenteninstallation.
5. Fügen Sie den Agent-Installationsbefehl in die RHEL EC2-Instanz ein, bei der Sie angemeldet sind. Dadurch wird der Workload Security-Agent installiert, der alle"Agentenvoraussetzungen" erfüllt sind.

Detaillierte Schritte finden Sie unter diesem Link: https://docs.netapp.com/us-en/cloudinsights/task_cs_add_agent.html#steps-to-install-agent

Fehlerbehebung

Bekannte Probleme und deren Lösungen werden in der folgenden Tabelle beschrieben.

Problem	Auflösung

Der Datensammler zeigt den Fehler „Workload-Sicherheit: ONTAP -Typ für Amazon FxSN-Datensammler konnte nicht ermittelt werden“ an. Der Kunde kann keinen neuen Amazon FSxN-Datensammler zu Workload Security hinzufügen. Bei der Verbindung vom Agenten zum FSxN-Cluster auf Port 443 kommt es zu einer Zeitüberschreitung. Für Firewall- und AWS-Sicherheitsgruppen sind die erforderlichen Regeln aktiviert, um die Kommunikation zu ermöglichen. Ein Agent ist bereits bereitgestellt und befindet sich auch im selben AWS-Konto. Derselbe Agent wird zum Verbinden und Überwachen der verbleibenden NetApp -Geräte verwendet (und alle funktionieren).	Lösen Sie dieses Problem, indem Sie der Sicherheitsregel des Agenten das LIF-Netzwerksegment fsxadmin hinzufügen. Alle Ports zulassen, wenn Sie sich bei den Ports nicht sicher sind.

Benutzerverwaltung

Workload Security-Benutzerkonten werden über Data Infrastructure Insights verwaltet.

Data Infrastructure Insights bietet vier Benutzerkontoebenen: Kontoinhaber, Administrator, Benutzer und Gast. Jedem Konto sind bestimmte Berechtigungsstufen zugewiesen. Ein Benutzerkonto mit Administratorrechten kann Benutzer erstellen oder ändern und jedem Benutzer eine der folgenden Workload-Sicherheitsrollen zuweisen:

Rolle	Workload-Sicherheitszugriff
Administrator	Kann alle Workload-Sicherheitsfunktionen ausführen, einschließlich der Funktionen für Warnungen, Forensik, Datensammler, Richtlinien für automatisierte Reaktionen und APIs für Workload-Sicherheit. Ein Administrator kann auch andere Benutzer einladen, aber nur Workload-Sicherheitsrollen zuweisen.
Benutzer	Kann Warnungen anzeigen und verwalten sowie forensische Daten anzeigen. Die Benutzerrolle kann den Alarmstatus ändern, eine Notiz hinzufügen, manuell Schnappschüsse machen und den Benutzerzugriff einschränken.
Gast	Kann Warnungen und Forensik anzeigen. Mit der Gastrolle können Sie den Alarmstatus nicht ändern, keine Notiz hinzufügen, manuell Schnappschüsse erstellen oder den Benutzerzugriff einschränken.

Schritte

1. Melden Sie sich bei Workload Security an
2. Klicken Sie im Menü auf **Admin > Benutzerverwaltung**

   Sie werden zur Benutzerverwaltungsseite von Data Infrastructure Insights weitergeleitet.

3. Wählen Sie für jeden Benutzer die gewünschte Rolle aus.

Wählen Sie beim Hinzufügen eines neuen Benutzers einfach die gewünschte Rolle aus (normalerweise Benutzer oder Gast).

Weitere Informationen zu Benutzerkonten und Rollen finden Sie in den Data Infrastructure Insights"Benutzerrolle" Dokumentation.

SVM-Ereignisratenprüfer (Leitfaden zur Agentendimensionierung)

Mit dem Event Rate Checker wird die kombinierte NFS/SMB-Ereignisrate im SVM überprüft, bevor ein ONTAP SVM-Datensammler installiert wird, um zu sehen, wie viele SVMs eine Agentenmaschine überwachen kann. Verwenden Sie den Event Rate Checker als Größenleitfaden zur Planung Ihrer Sicherheitsumgebung.

Ein Agent kann bis zu maximal 50 Datensammler unterstützen.

Anforderungen:

- Cluster-IP
- Benutzername und Kennwort des Clusteradministrators

Beim Ausführen dieses Skripts sollte kein ONTAP SVM Data Collector für die SVM ausgeführt werden, für die die Ereignisrate bestimmt wird.

Schritte:

1. Installieren Sie den Agenten, indem Sie den Anweisungen in CloudSecure folgen.
2. Sobald der Agent installiert ist, führen Sie das Skript *server_data_rate_checker.sh* als Sudo-Benutzer aus:

```
 /opt/netapp/cloudsecure/agent/install/svm_event_rate_checker.sh
. Für dieses Skript muss _sshpass_ auf der Linux-Maschine installiert
sein.  Es gibt zwei Möglichkeiten, es zu installieren:
```

   a. Führen Sie den folgenden Befehl aus:

```
 linux_prompt> yum install sshpass
.. Wenn das nicht funktioniert, laden Sie _sshpass_ aus dem Internet
auf die Linux-Maschine herunter und führen Sie den folgenden Befehl
aus:
```

```
linux_prompt> rpm -i sshpass
```

3. Geben Sie die richtigen Werte ein, wenn Sie dazu aufgefordert werden. Ein Beispiel finden Sie unten.
4. Die Ausführung des Skripts dauert ungefähr 5 Minuten.
5. Nach Abschluss des Laufs druckt das Skript die Ereignisrate vom SVM. Sie können die Ereignisrate pro SVM in der Konsolenausgabe überprüfen:

```
“Svm svm_rate is generating 100 events/sec”.
```

Jeder Ontap SVM-Datensammler kann mit einem einzelnen SVM verknüpft werden, was bedeutet, dass jeder Datensammler die Anzahl der Ereignisse empfangen kann, die ein einzelnes SVM generiert.

Beachten Sie Folgendes:

A) Verwenden Sie diese Tabelle als allgemeine Größenrichtlinie. Sie können die Anzahl der Kerne und/oder den Speicher erhöhen, um die Anzahl der unterstützten Datensammler auf bis zu 50 Datensammler zu erhöhen:

Agent-Computerkonfiguration	Anzahl der SVM-Datensammler	Maximale Ereignisrate, die der Agent-Computer verarbeiten kann
4 Kerne, 16 GB	10 Datensammler	20.000 Ereignisse/Sek.
4 Kerne, 32 GB	20 Datensammler	20.000 Ereignisse/Sek.

B) Um Ihre Gesamtereignisse zu berechnen, addieren Sie die für alle SVMs für diesen Agenten generierten Ereignisse.

C) Wenn das Skript nicht während der Spitzenzeiten ausgeführt wird oder wenn der Spitzenverkehr schwer vorherzusagen ist, halten Sie einen Ereignisratenpuffer von 30 % ein.

B + C sollte kleiner als A sein, sonst schlägt die Überwachung durch die Agent-Maschine fehl.

Mit anderen Worten: Die Anzahl der Datensammler, die einer einzelnen Agentenmaschine hinzugefügt werden können, sollte der folgenden Formel entsprechen:

```
 Sum of all Event rate of all Data Source Collectors + Buffer Event rate
of 30% < 20000 events/second
Siehe dielink:concept_cs_agent_requirements.html["Agentenanforderungen"]
Seite für zusätzliche Voraussetzungen und Anforderungen.
```

Beispiel

Nehmen wir an, wir haben drei SVMS, die Ereignisraten von 100, 200 bzw. 300 Ereignissen pro Sekunde generieren.

Wir wenden die Formel an:

```
 (100+200+300) + [(100+200+300)*30%] = 600+180 = 780events/sec
780 events/second is < 20000 events/second, so the 3 SVMs can be monitored
via one agent box.
```

Die Konsolenausgabe ist auf der Agent-Maschine unter dem Dateinamen *fpolicy_stat_<SVM-Name>.log* im aktuellen Arbeitsverzeichnis verfügbar.

Das Skript kann in den folgenden Fällen fehlerhafte Ergebnisse liefern:

- Es wurden falsche Anmeldeinformationen, IP-Adressen oder SVM-Namen angegeben.
- Eine bereits vorhandene fpolicy mit demselben Namen, derselben Sequenznummer usw. führt zu einem Fehler.
- Das Skript wird während der Ausführung abrupt gestoppt.

Ein Beispiel für die Ausführung eines Skripts wird unten angezeigt:

```
[root@ci-cs-data agent]#
/opt/netapp/cloudsecure/agent/install/svm_event_rate_checker.sh
```

```
Enter the cluster ip: 10.192.139.166
Enter the username to SSH: admin
Enter the password:
Getting event rate for NFS and SMB events.
Available SVMs in the Cluster
------------------------------
QA_SVM
Stage_SVM
Qa-fas8020
Qa-fas8020-01
Qa-fas8020-02
audit_svm
svm_rate
vs_new
vs_new2
```

```
-----------------------------
Enter [1/5] SVM name to check (press enter to skip): svm_rate
Enter [2/5] SVM name to check (press enter to skip): audit_svm
Enter [3/5] SVM name to check (press enter to skip):
Enter [4/5] SVM name to check (press enter to skip):
Enter [5/5] SVM name to check (press enter to skip):
Running check for svm svm_rate...
Running check for svm audit_svm...
Waiting 5 minutes for stat collection
Stopping sample svm_rate_sample
Stopping sample audit_svm_sample
fpolicy stats of svm svm_rate is saved in fpolicy_stat_svm_rate.log
Svm svm_rate is generating 100 SMB events/sec and 100 NFS events/sec
Overall svm svm_rate is generating 200 events/sec
fpolicy stats of svm audit_svm is saved in fpolicy_stat_audit_svm.log
Svm audit_svm is generating 200 SMB events/sec and 100 NFS events/sec
Overall svm audit_svm is generating 300 events/sec
```

```
[root@ci-cs-data agent]#
```

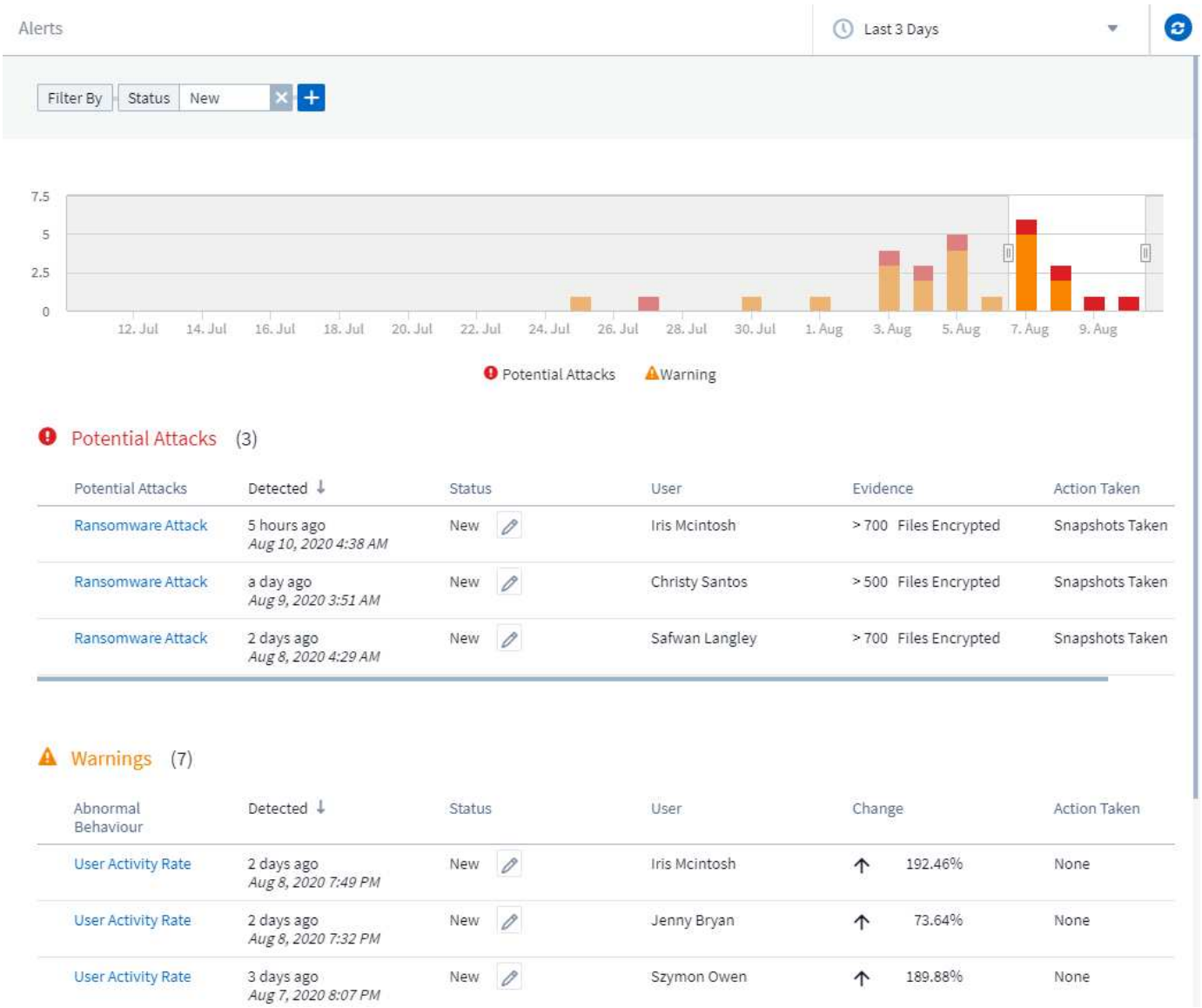
Fehlerbehebung

Frage	Antwort
Wenn ich dieses Skript auf einer SVM ausführe, die bereits für Workload Security konfiguriert ist, verwendet es dann einfach die vorhandene fpolicy-Konfiguration auf der SVM oder richtet es eine temporäre ein und führt den Prozess aus?	Der Event Rate Checker kann auch für eine SVM, die bereits für Workload Security konfiguriert ist, einwandfrei ausgeführt werden. Es sollte keine Auswirkungen geben.
Kann ich die Anzahl der SVMs erhöhen, auf denen das Skript ausgeführt werden kann?	Ja. Bearbeiten Sie einfach das Skript und ändern Sie die maximale Anzahl von SVMs von 5 auf eine beliebige Zahl.
Wenn ich die Anzahl der SVMs erhöhe, verlängert sich dann die Ausführungszeit des Skripts?	Nein. Das Skript wird maximal 5 Minuten lang ausgeführt, auch wenn die Anzahl der SVMs erhöht wird.
Kann ich die Anzahl der SVMs erhöhen, auf denen das Skript ausgeführt werden kann?	Ja. Sie müssen das Skript bearbeiten und die maximale Anzahl von SVMs von 5 auf eine beliebige Zahl ändern.
Wenn ich die Anzahl der SVMs erhöhe, verlängert sich dann die Ausführungszeit des Skripts?	Nein. Das Skript wird maximal 5 Minuten lang ausgeführt, auch wenn die Anzahl der SVMs erhöht wird.

Was passiert, wenn ich den Event Rate Checker mit einem vorhandenen Agenten ausführe?	Das Ausführen des Event Rate Checker für einen bereits vorhandenen Agenten kann zu einer Erhöhung der Latenz auf der SVM führen. Diese Erhöhung ist vorübergehender Natur, während der Event Rate Checker ausgeführt wird.

Warnungen

Auf der Seite „Workload-Sicherheitswarnungen“ wird eine Zeitleiste der jüngsten Angriffe und/oder Warnungen angezeigt und Sie können Details zu jedem Problem anzeigen.



Alarm

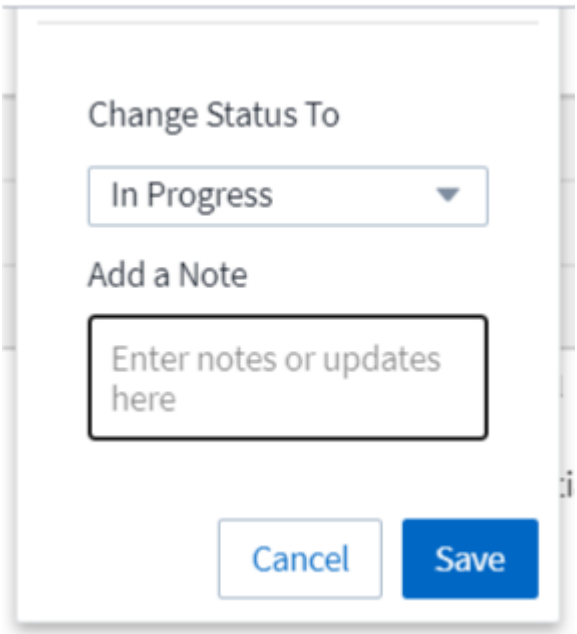
Die Warnliste zeigt ein Diagramm mit der Gesamtzahl der potenziellen Angriffe und/oder Warnungen an, die im ausgewählten Zeitraum ausgelöst wurden, gefolgt von einer Liste der Angriffe und/oder Warnungen, die in diesem Zeitraum aufgetreten sind. Sie können den Zeitbereich ändern, indem Sie die Schieberegler für Start- und Endzeit im Diagramm anpassen.

Für jeden Alarm wird Folgendes angezeigt:

Potenzielle Angriffe:

- Der *Potenzielle Angriffstyp* (z. B. Ransomware oder Sabotage)
- Datum und Uhrzeit der *Erkennung* des potenziellen Angriffs
- Der *Status* der Warnung:
  - **Neu**: Dies ist die Standardeinstellung für neue Warnungen.
  - **In Bearbeitung**: Die Warnung wird von einem oder mehreren Teammitgliedern untersucht.
  - **Gelöst**: Der Alarm wurde von einem Teammitglied als gelöst markiert.
  - **Abgelehnt**: Die Warnung wurde als falsch positiv oder als erwartetes Verhalten abgewiesen.

    Ein Administrator kann den Status der Warnung ändern und eine Notiz hinzufügen, um die Untersuchung zu unterstützen.



- Der *Benutzer*, dessen Verhalten den Alarm ausgelöst hat
- *Beweise* für den Angriff (z. B. wurde eine große Anzahl von Dateien verschlüsselt)
- Die *durchgeführte Aktion* (z. B. wurde ein Schnappschuss gemacht)

Warnungen:

- Das *Abnormale Verhalten*, das die Warnung ausgelöst hat
- Datum und Uhrzeit der *Erkennung* des Verhaltens
- Der *Status* der Warnung (Neu, In Bearbeitung usw.)
- Der *Benutzer*, dessen Verhalten den Alarm ausgelöst hat
- Eine Beschreibung der *Änderung* (z. B. ein ungewöhnlicher Anstieg der Dateizugriffe)
- Die *durchgeführte Aktion*

Filteroptionen

Sie können Warnungen nach Folgendem filtern:

- Der *Status* der Warnung
- Spezifischer Text in der *Anmerkung*
- Die Art der *Angriffe/Warnungen*
- Der *Benutzer*, dessen Aktionen den Alarm/die Warnung ausgelöst haben

Die Seite „Warnungsdetails“

Sie können auf der Seite mit der Warnmeldungsliste auf einen Warnmeldungslink klicken, um eine Detailseite für die Warnmeldung zu öffnen. Die Alarmdetails können je nach Art des Angriffs oder Alarms variieren. Beispielsweise kann eine Detailseite zu einem Ransomware-Angriff die folgenden Informationen anzeigen:

Abschnitt „Zusammenfassung“:

- Angriffstyp (Ransomware, Sabotage) und Warnmeldungs-ID (zugewiesen von Workload Security)
- Datum und Uhrzeit der Erkennung des Angriffs
- Durchgeführte Aktion (z. B. wurde ein automatischer Schnappschuss erstellt). Die Uhrzeit des Schnappschusses wird direkt unter dem Abschnitt „Zusammenfassung“ angezeigt.))
- Status (Neu, In Bearbeitung usw.)

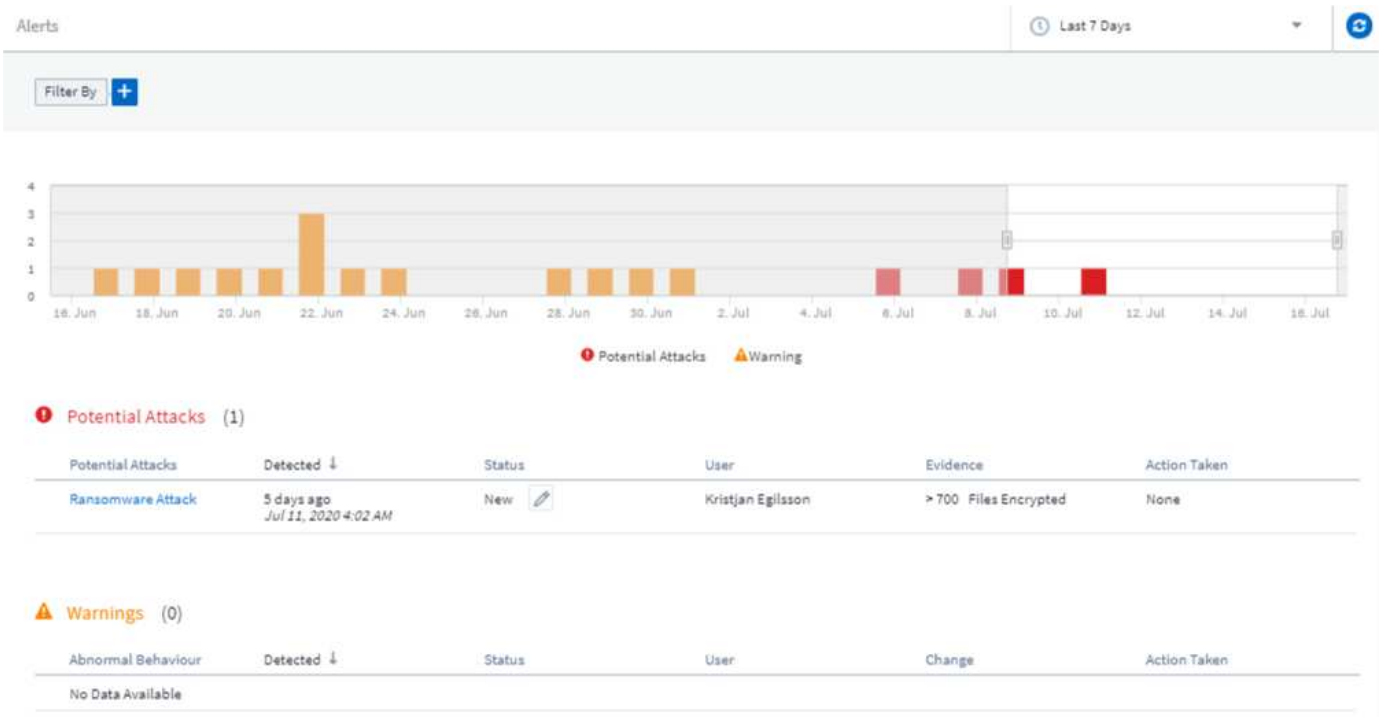
Abschnitt „Angriffsergebnisse“:

- Anzahl der betroffenen Volumes und Dateien
- Eine begleitende Zusammenfassung der Entdeckung
- Ein Diagramm, das die Dateiaktivität während des Angriffs zeigt

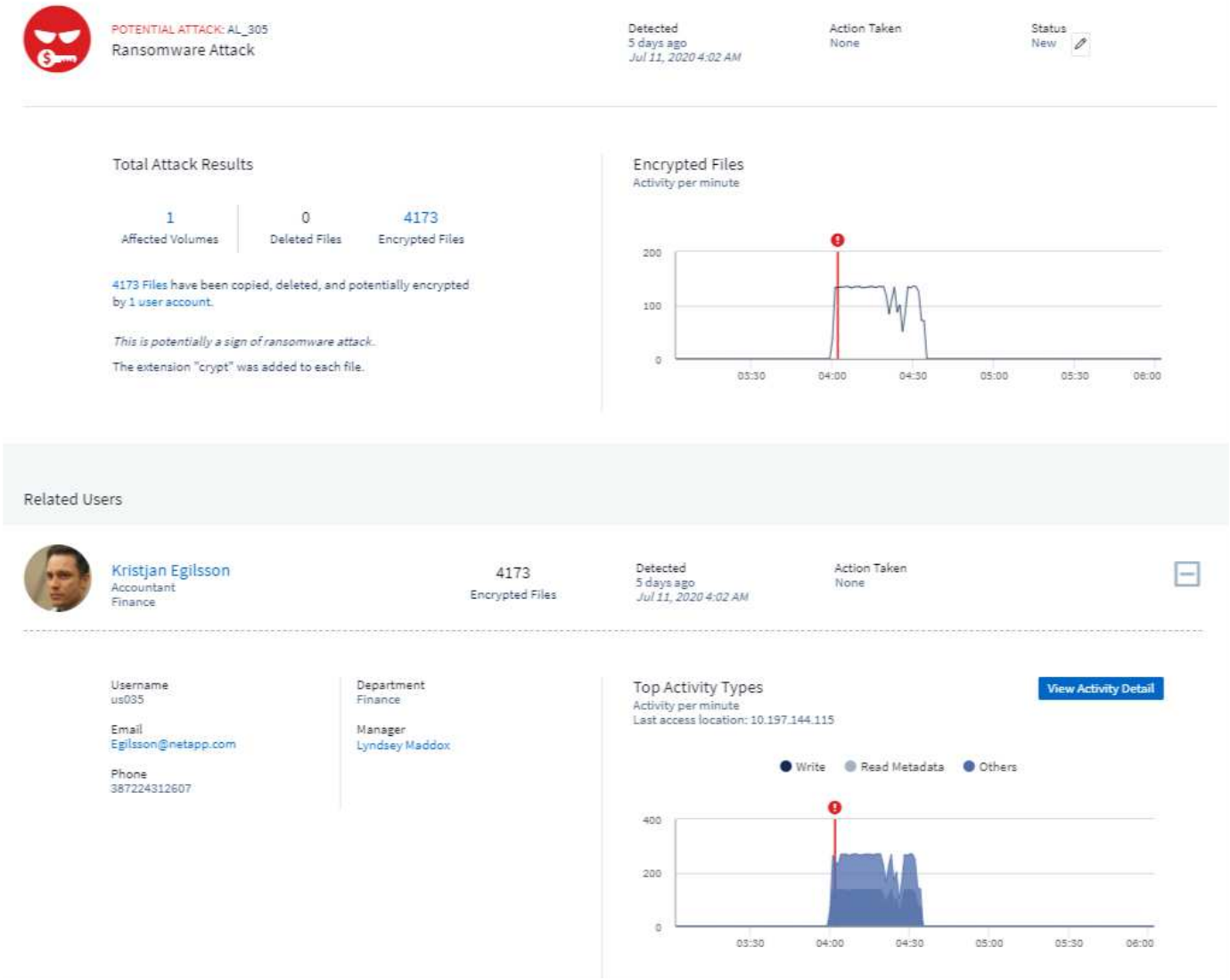
Abschnitt „Verwandte Benutzer“:

Dieser Abschnitt zeigt Details zum Benutzer, der an dem potenziellen Angriff beteiligt war, einschließlich eines Diagramms der Top-Aktivitäten des Benutzers.

Warnseite (dieses Beispiel zeigt einen potenziellen Ransomware-
Angriff):



Detailseite (dieses Beispiel zeigt einen potenziellen Ransomware-Angriff):

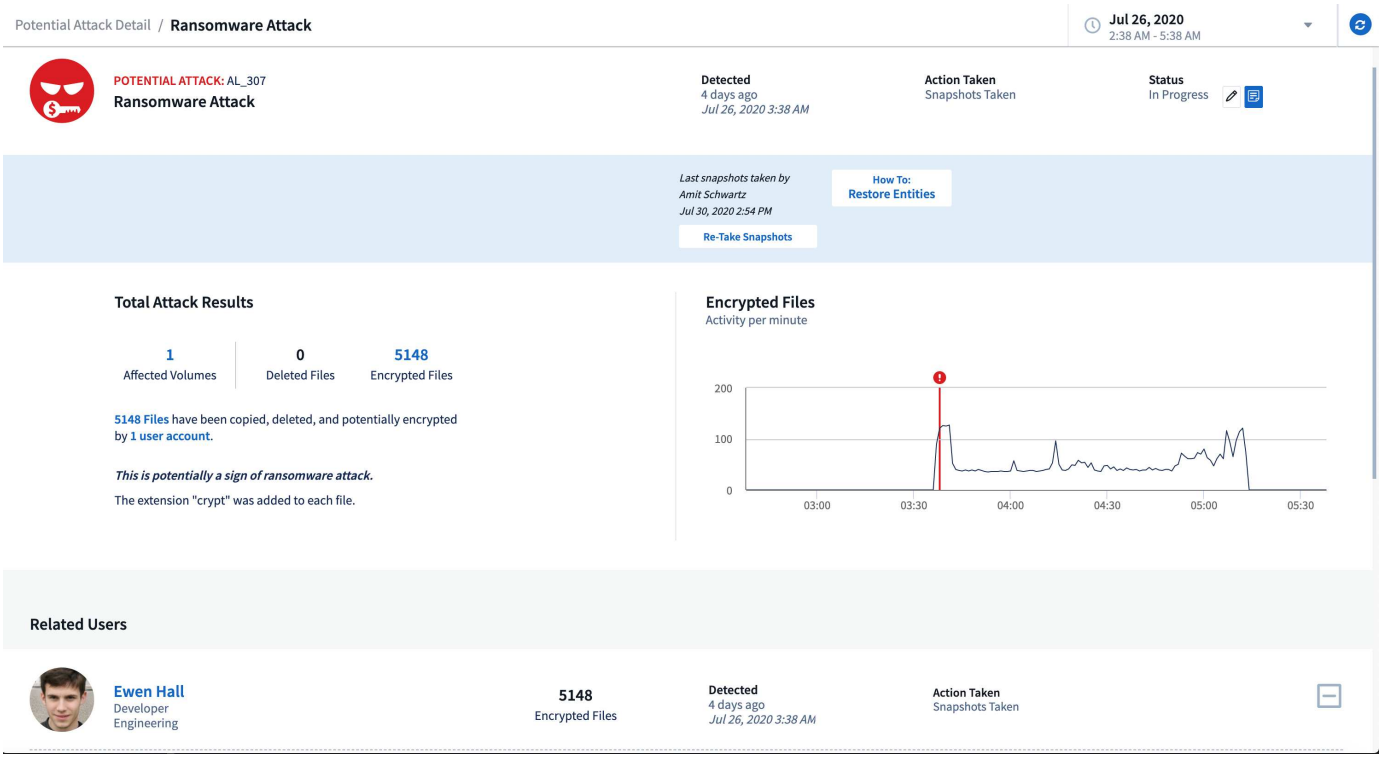


Aktion „Schnappschuss machen“

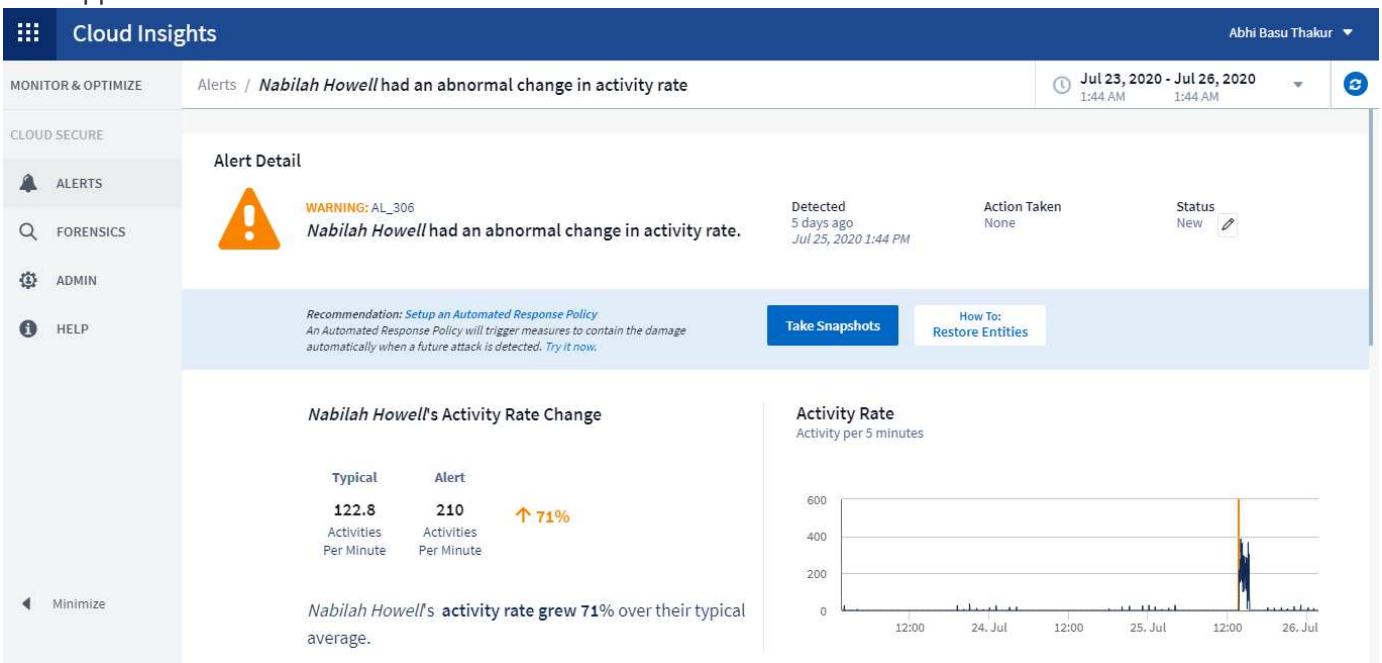
Workload Security schützt Ihre Daten, indem es automatisch einen Snapshot erstellt, wenn böswillige Aktivitäten erkannt werden, und so gewährleistet, dass Ihre Daten sicher gesichert werden.

Sie können definieren"Richtlinien für automatisierte Antworten" die einen Schnappschuss erstellen, wenn ein Ransomware-Angriff oder andere ungewöhnliche Benutzeraktivitäten erkannt werden. Sie können auch manuell einen Schnappschuss von der Warnseite aus erstellen.

Automatischer Schnappschuss
erstellt:



Manueller Schnappschuss:



Warnmeldungen

Für jede Aktion im Zusammenhang mit der Warnung werden E-Mail-Benachrichtigungen zu Warnungen an eine Warnungsempfängerliste gesendet. Um die Empfänger der Benachrichtigungen zu konfigurieren, klicken Sie auf **Admin > Benachrichtigungen** und geben Sie für jeden Empfänger eine E-Mail-Adresse ein.

Aufbewahrungsrichtlinie

Alarme und Warnungen werden 13 Monate lang gespeichert. Alarme und Warnungen, die älter als 13 Monate

sind, werden gelöscht. Wenn die Workload Security-Umgebung gelöscht wird, werden auch alle mit der Umgebung verknüpften Daten gelöscht.

Fehlerbehebung

Problem:	Versuchen Sie Folgendes:
Es gibt eine Situation, in der ONTAP stündlich Snapshots pro Tag erstellt. Werden Workload Security (WS)-Snapshots dies beeinflussen? Wird der WS-Snapshot den Platz des stündlichen Snapshots einnehmen? Wird der standardmäßige stündliche Snapshot gestoppt?	Snapshots der Workload-Sicherheit haben keinen Einfluss auf die stündlichen Snapshots. WS-Snapshots belegen nicht den stündlichen Snapshot-Speicherplatz und das sollte auch so bleiben wie bisher. Der standardmäßige stündliche Snapshot wird nicht gestoppt.
Was passiert, wenn die maximale Snapshot-Anzahl in ONTAP erreicht wird?	Wenn die maximale Snapshot-Anzahl erreicht ist, schlägt die nachfolgende Snapshot-Erstellung fehl und Workload Security zeigt eine Fehlermeldung mit dem Hinweis an, dass der Snapshot voll ist. Der Benutzer muss Snapshot-Richtlinien definieren, um die ältesten Snapshots zu löschen, andernfalls werden keine Snapshots erstellt. In ONTAP 9.3 und früheren Versionen kann ein Volume bis zu 255 Snapshot-Kopien enthalten. In ONTAP 9.4 und höher kann ein Volume bis zu 1023 Snapshot-Kopien enthalten. Informationen zu"Festlegen der Richtlinie zum Löschen von Snapshots" .
Workload Security kann überhaupt keine Snapshots erstellen.	Stellen Sie sicher, dass die zum Erstellen von Snapshots verwendete Rolle über den Link: korrekte Rechte zugewiesen verfügt. Stellen Sie sicher, dass *csrole* mit den richtigen Zugriffsrechten zum Erstellen von Snapshots erstellt wird: security login role create -vserver <vservername> -role csrole -cmddirname "volume snapshot" -access all
Snapshots schlagen für ältere Warnungen auf SVMs fehl, die aus Workload Security entfernt und anschließend wieder hinzugefügt wurden. Für neue Warnungen, die nach dem erneuten Hinzufügen von SVM auftreten, werden Snapshots erstellt.	Dies ist ein seltenes Szenario. Falls dies bei Ihnen der Fall ist, melden Sie sich bei ONTAP an und erstellen Sie die Snapshots für die älteren Warnungen manuell.
Auf der Seite „Alarmdetails“ wird unter der Schaltfläche „Snapshot erstellen“ die Fehlermeldung „Letzter Versuch fehlgeschlagen“ angezeigt. Wenn Sie mit der Maus über den Fehler fahren, wird „Zeitüberschreitung beim Aufrufen des API-Befehls für den Datensammler mit der ID“ angezeigt.	Dies kann passieren, wenn ein Datensammler über die SVM-Verwaltungs-IP zur Workload-Sicherheit hinzugefügt wird, wenn sich das LIF der SVM in ONTAP im Status *deaktiviert* befindet. Aktivieren Sie das jeweilige LIF in ONTAP und lösen Sie „Manuell Snapshot erstellen“ von Workload Security aus. Die Snapshot-Aktion wird dann erfolgreich sein.

Forensik

Forensik – Alle Aktivitäten

Auf der Seite „Alle Aktivitäten“ können Sie die Aktionen nachvollziehen, die an Entitäten

in der Workload Security-Umgebung ausgeführt werden.

Untersuchen aller Aktivitätsdaten

Klicken Sie auf **Forensik > Aktivitätsforensik** und dann auf die Registerkarte **Alle Aktivitäten**, um auf die Seite „Alle Aktivitäten“ zuzugreifen. Diese Seite bietet einen Überblick über die Aktivitäten Ihres Mandanten und hebt die folgenden Informationen hervor:

- Ein Diagramm, das den *Aktivitätsverlauf* zeigt (basierend auf einem ausgewählten globalen Zeitbereich)

  Sie können das Diagramm vergrößern, indem Sie ein Rechteck im Diagramm aufziehen. Die gesamte Seite wird geladen, um den gezoomten Zeitbereich anzuzeigen. Beim Vergrößern wird eine Schaltfläche angezeigt, mit der der Benutzer herauszoomen kann.

- Eine Liste aller Aktivitätsdaten.
- Ein Dropdown-Menü „Gruppieren nach“ bietet die Möglichkeit, die Aktivität nach Benutzern, Ordnern, Entitätstyp usw. zu gruppieren.
- Über der Tabelle ist eine Schaltfläche für den allgemeinen Pfad verfügbar, über die wir durch Anklicken ein ausziehbares Bedienfeld mit Details zum Entitätspfad erhalten.

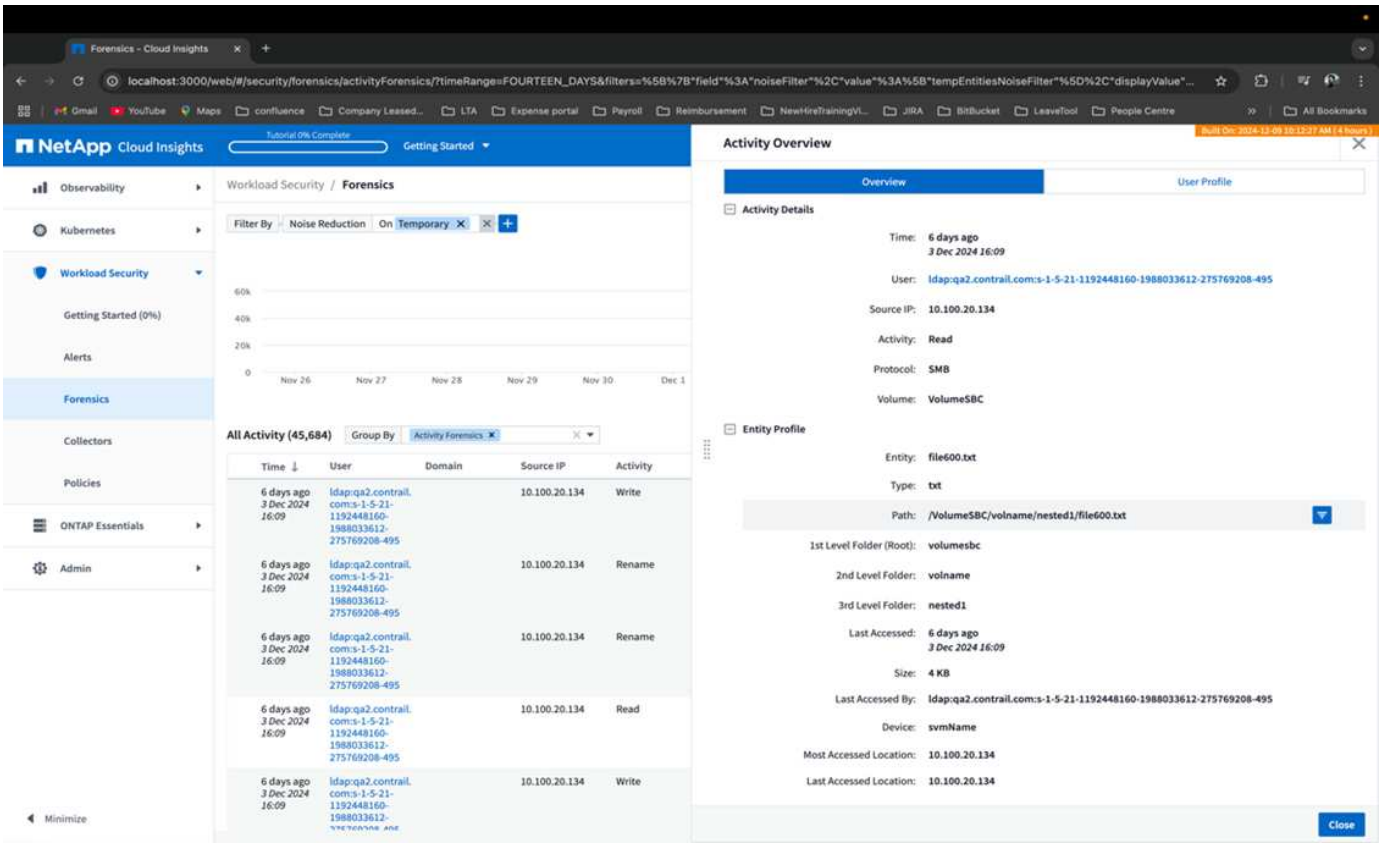
Die Tabelle **Alle Aktivitäten** zeigt die folgenden Informationen. Beachten Sie, dass nicht alle dieser Spalten standardmäßig angezeigt werden. Sie können die anzuzeigenden Spalten auswählen, indem Sie auf das Zahnradsymbol klicken.

- Die **Zeit**, zu der auf eine Entität zugegriffen wurde, einschließlich Jahr, Monat, Tag und Uhrzeit des letzten Zugriffs.
- Der **Benutzer**, der auf die Entität mit einem Link zugegriffen hat"Benutzerinformationen" als ausziehbare Platte.
- Die **Aktivität**, die der Benutzer ausgeführt hat. Unterstützte Typen sind:
  - **Gruppeneigentum ändern** – Der Gruppeneigentum einer Datei oder eines Ordners wird geändert. Weitere Einzelheiten zum Gruppeneigentum finden Sie unter"dieser Link."
  - **Eigentümer ändern** – Der Besitz einer Datei oder eines Ordners wird auf einen anderen Benutzer geändert.
  - **Berechtigung ändern** – Die Datei- oder Ordnerberechtigung wurde geändert.
  - **Erstellen** – Datei oder Ordner erstellen.
  - **Löschen** – Datei oder Ordner löschen. Wenn ein Ordner gelöscht wird, werden *delete*-Ereignisse für alle Dateien in diesem Ordner und den Unterordnern abgerufen.
  - **Lesen** – Datei wird gelesen.
  - **Metadaten lesen** – Nur beim Aktivieren der Ordnerüberwachungsoption. Wird beim Öffnen eines Ordners unter Windows oder beim Ausführen von „ls“ in einem Ordner unter Linux generiert.
  - **Umbenennen** – Datei oder Ordner umbenennen.
  - **Schreiben** – Daten werden in eine Datei geschrieben.
  - **Metadaten schreiben** – Dateimetadaten werden geschrieben, z. B. geänderte Berechtigungen.
  - **Andere Änderung** – Alle anderen Ereignisse, die oben nicht beschrieben sind. Alle nicht zugeordneten Ereignisse werden dem Aktivitätstyp „Andere Änderung“ zugeordnet. Gilt für Dateien und Ordner.
- Der **Pfad** ist der *Entitätspfad. Dies sollte entweder der genaue Entitätspfad (z. B.*

„/home/userX/nested1/nested2/abc.txt_“) ODER der Verzeichnisteil des Pfads für die rekursive Suche (z. B. „*/home/userX/nested1/nested2/*“) sein. HINWEIS: Regex-Pfadmuster (z. B. *verschachtelt*) sind hier NICHT zulässig. Alternativ können für die Pfadfilterung auch einzelne Filter auf Pfadordnerebene wie unten erwähnt angegeben werden.

- Der **Ordner der 1. Ebene (Stammverzeichnis)** ist das Stammverzeichnis des Entitätspfads in Kleinbuchstaben.
- Der **Ordner der zweiten Ebene** ist das Verzeichnis der zweiten Ebene des Entitätspfads in Kleinbuchstaben.
- Der **Ordner der 3. Ebene** ist das Verzeichnis der dritten Ebene des Entitätspfads in Kleinbuchstaben.
- Der **Ordner der 4. Ebene** ist das Verzeichnis der vierten Ebene des Entitätspfads in Kleinbuchstaben.
- Der **Entitätstyp**, einschließlich der Entitätserweiterung (d. h. Dateierweiterung) (.doc, .docx, .tmp usw.).
- Das **Gerät**, auf dem sich die Entitäten befinden.
- Das zum Abrufen von Ereignissen verwendete **Protokoll**.
- Der **Ursprüngliche Pfad**, der für Umbenennungsereignisse verwendet wurde, als die Originaldatei umbenannt wurde. Diese Spalte ist in der Tabelle standardmäßig nicht sichtbar. Verwenden Sie den Spaltenselektor, um diese Spalte zur Tabelle hinzuzufügen.
- Das **Volume**, in dem sich die Entitäten befinden. Diese Spalte ist in der Tabelle standardmäßig nicht sichtbar. Verwenden Sie den Spaltenselektor, um diese Spalte zur Tabelle hinzuzufügen.
- Der **Entitätsname** ist die letzte Komponente des Entitätspfads; beim Entitätstyp als Datei ist es der Dateiname.

Durch Auswählen einer Tabellenzeile wird ein ausziehbares Fenster mit dem Benutzerprofil auf einer Registerkarte und der Aktivitäts- und Entitätsübersicht auf einer anderen Registerkarte geöffnet.



Die Standardmethode „Gruppieren nach“ ist „Aktivitätsforensik“. Wenn Sie eine andere *Gruppieren nach*

-Methode auswählen, beispielsweise Entitätstyp, wird die Entitäts-*Gruppieren nach*-Tabelle angezeigt. Wenn keine Auswahl getroffen wird, wird *Gruppieren nach* **alle** angezeigt.

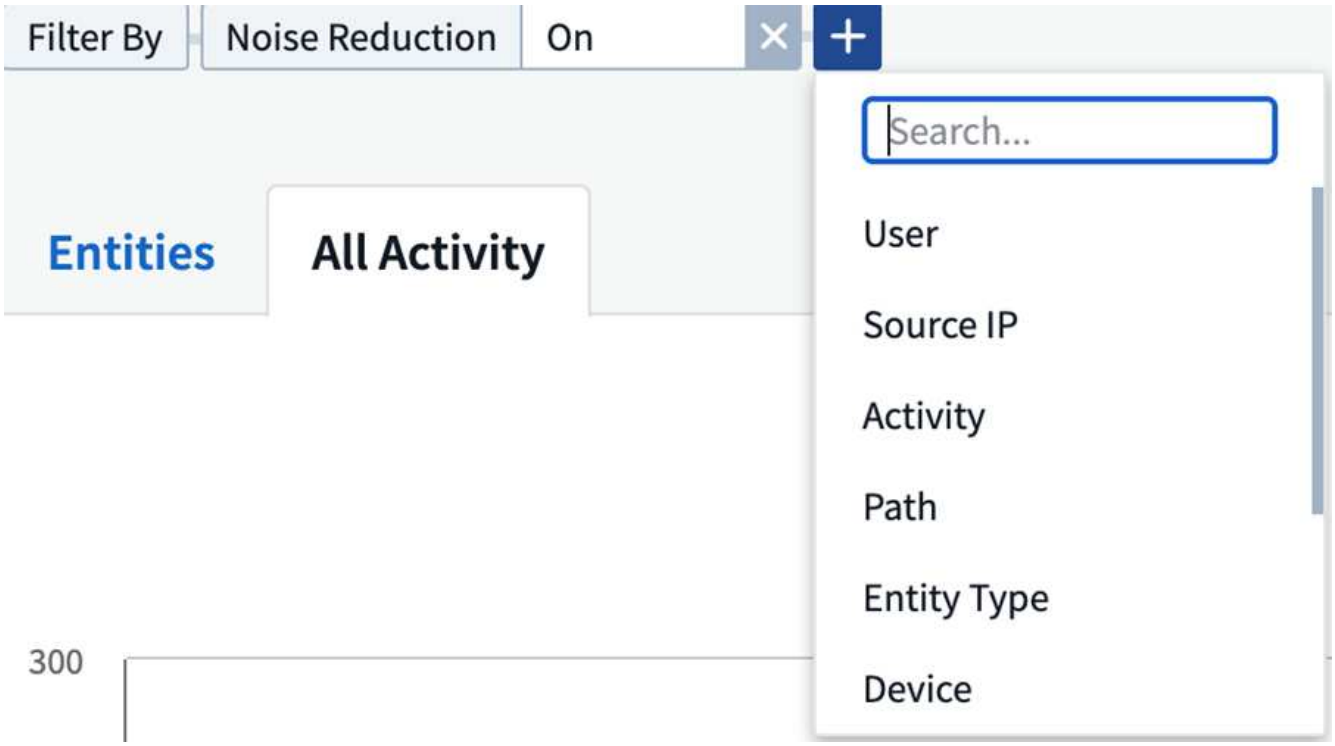
- Die Aktivitätsanzahl wird als Hyperlink angezeigt. Wenn Sie diesen auswählen, wird die ausgewählte Gruppierung als Filter hinzugefügt. Die Aktivitätstabelle wird basierend auf diesem Filter aktualisiert.
- Beachten Sie, dass Sie, wenn Sie den Filter ändern, den Zeitbereich ändern oder den Bildschirm aktualisieren, nicht zu den gefilterten Ergebnissen zurückkehren können, ohne den Filter erneut einzustellen.
- Bitte beachten Sie, dass das Dropdown-Menü „Gruppieren nach“ deaktiviert wird, wenn „Entitätsname“ als Filter ausgewählt ist. Wenn sich der Benutzer bereits auf dem Bildschirm „Gruppieren nach“ befindet, wird der Entitätsname als Filter deaktiviert.

Filtern von Daten zum forensischen Aktivitätsverlauf

Zum Filtern von Daten können Sie zwei Methoden verwenden.

- Der Filter kann über das ausziehbare Bedienfeld hinzugefügt werden. Der Wert wird den entsprechenden Filtern in der oberen Liste „Filtern nach“ hinzugefügt.
- Filtern Sie Daten, indem Sie in das Feld *Filtern nach* Folgendes eingeben:

  Wählen Sie den entsprechenden Filter aus dem oberen Widget „Filtern nach“ aus, indem Sie auf die Schaltfläche **[+]** klicken:



  Geben Sie den Suchtext ein

  Drücken Sie die Eingabetaste oder klicken Sie außerhalb des Filterfelds, um den Filter anzuwenden.

Sie können Daten zur forensischen Aktivität nach den folgenden Feldern filtern:

- Der *Aktivitäts*typ.

- **Protokoll** zum Abrufen protokollspezifischer Aktivitäten.
- **Benutzername** des Benutzers, der die Aktivität ausführt. Sie müssen den genauen Benutzernamen zum Filtern angeben. Die Suche mit einem teilweisen Benutzernamen oder einem teilweisen Benutzernamen mit dem Präfix oder Suffix „*“ funktioniert nicht.
- **Rauschunterdrückung** zum Filtern von Dateien, die in den letzten 2 Stunden vom Benutzer erstellt wurden. Es wird auch zum Filtern temporärer Dateien (z. B. .tmp-Dateien) verwendet, auf die der Benutzer zugreift.
- **Domäne** des Benutzers, der die Aktivität ausführt. Sie müssen die **genaue Domäne** zum Filtern angeben. Die Suche nach Teildomänen oder Teildomänen mit einem Platzhalter ('*') als Präfix oder Suffix funktioniert nicht. *None* kann angegeben werden, um nach fehlenden Domänen zu suchen.

Für die folgenden Felder gelten besondere Filterregeln:

- **Entitätstyp**, unter Verwendung der Entitäts-(Datei-)Erweiterung – es ist vorzuziehen, den genauen Entitätstyp in Anführungszeichen anzugeben. Zum Beispiel *"txt"*.
- **Pfad** der Entität – Dies sollte entweder der genaue Entitätspfad (z. B. *„/home/userX/nested1/nested2/abc.txt“*) ODER der Verzeichnisteil des Pfads für die rekursive Suche (z. B. *„/home/userX/nested1/nested2/“*) sein. HINWEIS: Regex-Pfadmuster (z. B. *verschachtelt*) sind hier NICHT zulässig. Für schnellere Ergebnisse werden Verzeichnispfadfilter (Pfadzeichenfolge endet mit /) mit einer Tiefe von bis zu 4 Verzeichnissen empfohlen. Beispiel: *„/home/userX/nested1/nested2/“*. Weitere Einzelheiten finden Sie in der folgenden Tabelle.
- Ordner der 1. Ebene (Stammverzeichnis) – Stammverzeichnis des Entitätspfads als Filter. Wenn der Entitätspfad beispielsweise /home/userX/nested1/nested2/ ist, kann home ODER „home“ verwendet werden.
- Ordner der 2. Ebene – Verzeichnis der 2. Ebene der Entitätspfadfilter. Wenn der Entitätspfad beispielsweise /home/userX/nested1/nested2/ ist, kann userX ODER „userX“ verwendet werden.
- Ordner der 3. Ebene – Verzeichnis der 3. Ebene der Entitätspfadfilter.
- Wenn der Entitätspfad beispielsweise /home/userX/nested1/nested2/ ist, kann nested1 ODER „nested1“ verwendet werden.
- Ordner der 4. Ebene – Verzeichnis Verzeichnis der 4. Ebene der Entitätspfadfilter. Wenn der Entitätspfad beispielsweise /home/userX/nested1/nested2/ ist, kann nested2 ODER „nested2“ verwendet werden.
- **Benutzer**, der die Aktivität ausführt – es ist vorzuziehen, den genauen Benutzer in Anführungszeichen anzugeben. Beispiel: *"Administrator"*.
- **Gerät** (SVM), auf dem sich Entitäten befinden
- **Volume**, in dem sich Entitäten befinden
- Der **Ursprüngliche Pfad**, der für Umbenennungsereignisse verwendet wurde, als die Originaldatei umbenannt wurde.
- **Quell-IP**, von der aus auf die Entität zugegriffen wurde.
  - Sie können die Platzhalter * und ? verwenden. Zum Beispiel: 10.0.0.**, 10.0?.0.10, 10.10**
  - Wenn eine exakte Übereinstimmung erforderlich ist, müssen Sie eine gültige Quell-IP-Adresse in Anführungszeichen angeben, beispielsweise „10.1.1.1.“. Unvollständige IPs mit Anführungszeichen wie „10.1.1.“, „10.1..*“ usw. funktionieren nicht.
- Der **Entitätsname** – der Dateiname des Entitätspfads als Filter. Wenn der Entitätspfad beispielsweise /home/userX/nested1/testfile.txt lautet, ist der Entitätsname testfile.txt. Bitte beachten Sie, dass es empfohlen wird, den genauen Dateinamen in Anführungszeichen anzugeben. Versuchen Sie, die Suche mit Platzhaltern zu vermeiden. Beispiel: „testfile.txt“. Beachten Sie außerdem, dass dieser Entitätsnamenfilter für kürzere Zeiträume (bis zu 3 Tage) empfohlen wird.

Für die vorangehenden Felder gelten beim Filtern folgende Punkte:

- Der genaue Wert sollte in Anführungszeichen stehen: Beispiel: „Suchtext“
- Platzhalterzeichenfolgen dürfen keine Anführungszeichen enthalten: Beispiel: Suchtext, *Suchtext*, filtert nach allen Zeichenfolgen, die „Suchtext“ enthalten.
- Zeichenfolgen mit einem Präfix, Beispiel: Suchtext*, suchen nach allen Zeichenfolgen, die mit „Suchtext“ beginnen.

Bitte beachten Sie, dass bei allen Filterfeldern die Groß- und Kleinschreibung beachtet wird. Beispiel: Wenn der angewendete Filter „Entitätstyp“ mit dem Wert „Suchtext“ ist, werden Ergebnisse mit dem Entitätstyp „Suchtext“, „Suchtext“ oder „SUCHTEXT“ zurückgegeben.

Beispiele für Aktivitätsforensikfilter:

Vom Benutzer angewendeter Filterausdruck	Erwartetes Ergebnis	Leistungsbeurteilung	Kommentar
Pfad = "/home/userX/nested1/nested2/"	Rekursive Suche aller Dateien und Ordner unter einem bestimmten Verzeichnis	Schnell	Verzeichnissuchen in bis zu 4 Verzeichnissen sind schnell.
Pfad = "/home/userX/nested1/"	Rekursive Suche aller Dateien und Ordner unter einem bestimmten Verzeichnis	Schnell	Verzeichnissuchen in bis zu 4 Verzeichnissen sind schnell.
Pfad = "/home/userX/nested1/test"	Exakte Übereinstimmung, wenn der Pfadwert mit /home/userX/nested1/test übereinstimmt	Langsamer	Die exakte Suche ist im Vergleich zur Verzeichnissuche langsamer.
Pfad = "/home/userX/nested1/nested2/nested3/"	Rekursive Suche aller Dateien und Ordner unter einem bestimmten Verzeichnis	Langsamer	Die Suche in mehr als 4 Verzeichnissen ist langsamer.
Alle anderen nicht pfadbasierten Filter. Es wird empfohlen, Benutzer- und Entitätstypfilter in Anführungszeichen zu setzen, z. B. „Benutzer="Administrator" Entitätstyp="txt"		Schnell	
Entitätsname = "test.log"	Genaue Übereinstimmung, wenn der Dateiname „test.log“ lautet	Schnell	Da es sich um eine exakte Übereinstimmung handelt
Entitätsname = *test.log	Dateinamen, die mit test.log enden	Langsam	Aufgrund von Platzhaltern kann es langsam sein.

Vom Benutzer angewendeter Filterausdruck	Erwartetes Ergebnis	Leistungsbeurteilung	Kommentar
Entitätsname = test*.log	Dateinamen, die mit „test“ beginnen und mit „.log“ enden	Langsam	Aufgrund von Platzhaltern kann es langsam sein.
Entitätsname = test.lo	Dateinamen, die mit test.lo beginnen. Beispiel: Es entspricht test.log, test.log.1, test.log1	Langsamer	Aufgrund des Platzhalters am Ende kann es langsam sein.
Entitätsname = Test	Dateinamen, die mit „test“ beginnen	Am langsamsten	Aufgrund des Platzhalters am Ende und der Verwendung allgemeinerer Werte kann es langsam sein.

NOTIZ:

1. Die neben dem Symbol „Alle Aktivitäten“ angezeigte Aktivitätsanzahl wird auf 30 Minuten gerundet, wenn der ausgewählte Zeitraum mehr als 3 Tage umfasst. Beispielsweise zeigt ein Zeitraum vom 1. September, 10:15 Uhr bis 7. September, 10:15 Uhr die Aktivitätsanzahl vom 1. September, 10:00 Uhr bis 7. September, 10:30 Uhr an.
2. Ebenso werden die im Diagramm „Aktivitätsverlauf“ angezeigten Zählmetriken auf 30 Minuten gerundet, wenn der ausgewählte Zeitraum mehr als 3 Tage umfasst.

Sortieren von Daten zum forensischen Aktivitätsverlauf

Sie können die Aktivitätsverlaufsdaten nach *Zeit, Benutzer, Quell-IP, Aktivität*, *Entitätstyp*, Ordner der 1. Ebene (Stamm), Ordner der 2. Ebene, Ordner der 3. Ebene und Ordner der 4. Ebene sortieren. Standardmäßig ist die Tabelle in absteigender Zeitreihenfolge sortiert, d. h. die neuesten Daten werden zuerst angezeigt. Die Sortierung ist für die Felder *Gerät* und *Protokoll* deaktiviert.

Benutzerhandbuch für asynchrone Exporte

Überblick

Die Funktion „Asynchrone Exporte“ in Storage Workload Security ist für die Verarbeitung großer Datenexporte konzipiert.

Schritt-für-Schritt-Anleitung: Daten mit asynchronen Exporten exportieren

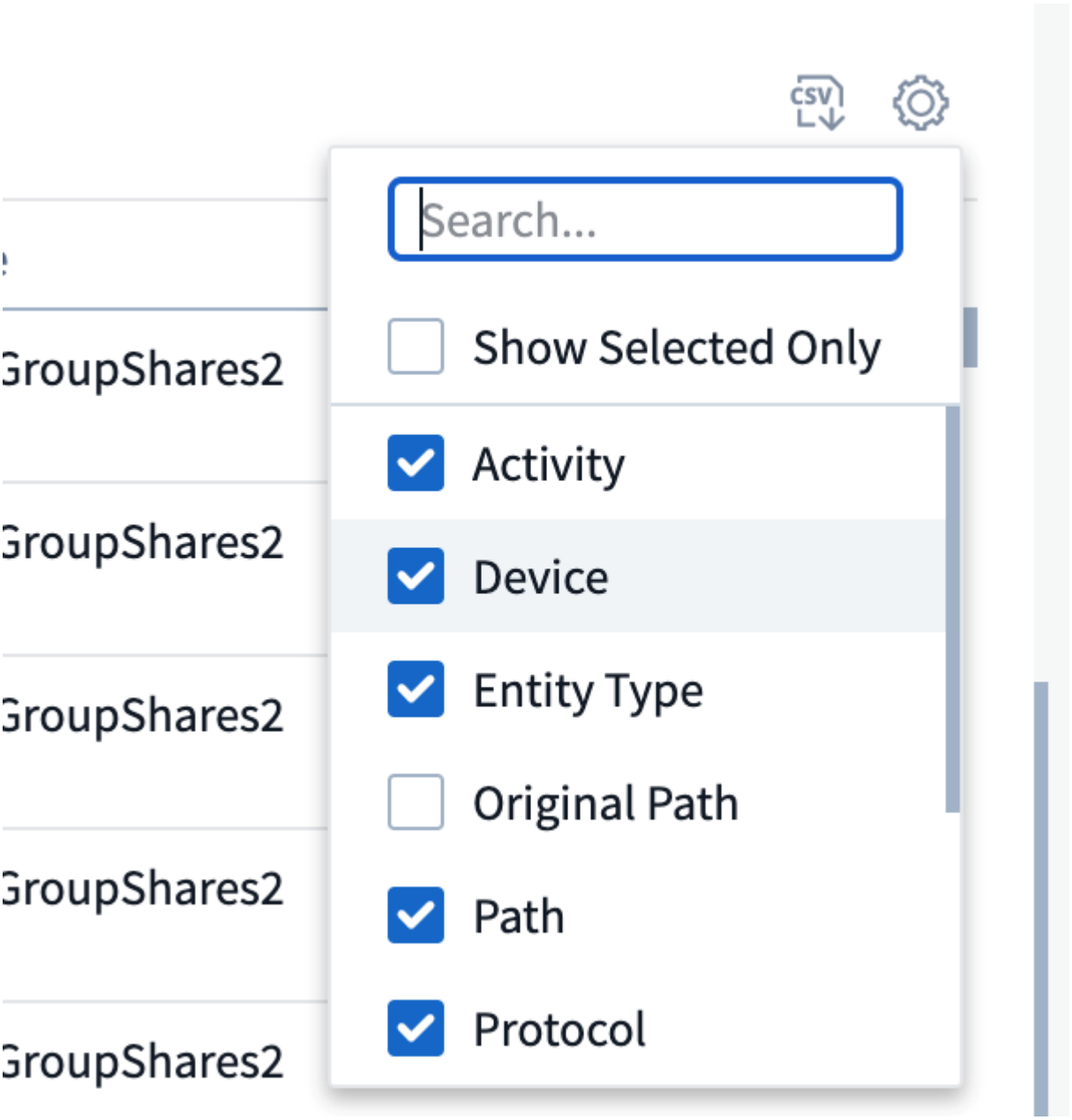
1. **Export starten**: Wählen Sie die gewünschte Zeitdauer und Filter für den Export aus und klicken Sie auf die Schaltfläche „Exportieren“.
2. **Warten Sie, bis der Export abgeschlossen ist**: Die Verarbeitungszeit kann zwischen einigen Minuten und einigen Stunden liegen. Möglicherweise müssen Sie die Forensikseite einige Male aktualisieren. Sobald der Exportauftrag abgeschlossen ist, wird die Schaltfläche „Letzte CSV-Exportdatei herunterladen“ aktiviert.
3. **Herunterladen**: Klicken Sie auf die Schaltfläche „Zuletzt erstellte Exportdatei herunterladen“, um die exportierten Daten im ZIP-Format zu erhalten. Diese Daten stehen zum Download zur Verfügung, bis der Benutzer einen weiteren asynchronen Export initiiert oder drei Tage vergangen sind, je nachdem, was zuerst eintritt. Die Schaltfläche bleibt aktiviert, bis ein weiterer asynchroner Export gestartet wird.

4. **Einschränkungen**:
    - Die Anzahl der asynchronen Downloads ist derzeit auf 1 pro Benutzer für jede Aktivitäts- und Aktivitätsanalysetabelle und 3 pro Mandant begrenzt.
    - Die exportierten Daten sind für die Aktivitätentabelle auf maximal 1 Million Datensätze begrenzt, während für „Gruppieren nach“ die Begrenzung auf eine halbe Million Datensätze liegt.

Ein Beispielskript zum Extrahieren forensischer Daten über die API befindet sich unter */opt/netapp/cloudsecure/agent/export-script/* auf dem Agenten. Weitere Einzelheiten zum Skript finden Sie in der Readme-Datei an dieser Stelle.

Spaltenauswahl für alle Aktivitäten

Die Tabelle „Alle Aktivitäten“ zeigt standardmäßig ausgewählte Spalten an. Um Spalten hinzuzufügen, zu entfernen oder zu ändern, klicken Sie auf das Zahnradsymbol rechts neben der Tabelle und wählen Sie aus der Liste der verfügbaren Spalten aus.



Aufbewahrung des Aktivitätsverlaufs

Der Aktivitätsverlauf wird für aktive Workload Security-Umgebungen 13 Monate lang aufbewahrt.

Anwendbarkeit von Filtern in der Forensik-Seite

Filter	Was es bewirkt	Beispiel	Anwendbar für diese Filter	Gilt nicht für diese Filter	Ergebnis
* (Sternchen)	ermöglicht Ihnen die Suche nach allem	Auto*03172022 Wenn der Suchtext Bindestriche oder Unterstriche enthält, geben Sie den Ausdruck in Klammern ein. zB (svm*) für die Suche nach svm-123	Benutzer, Entitätstyp, Gerät, Volume, Originalpfad, Ordner der 1. Ebene, Ordner der 2. Ebene, Ordner der 3. Ebene, Ordner der 4. Ebene, Entitätsname, Quell-IP		Gibt alle Ressourcen zurück, die mit „Auto“ beginnen und mit „03172022“ enden.
? (Fragezeichen)	ermöglicht die Suche nach einer bestimmten Anzahl von Zeichen	AutoSabotageUser1_03172022?	Benutzer, Entitätstyp, Gerät, Volume, Ordner der 1. Ebene, Ordner der 2. Ebene, Ordner der 3. Ebene, Ordner der 4. Ebene, Entitätsname, Quell-IP		gibt AutoSabotageUser1_03172022A, AutoSabotageUser1_03172022B, AutoSabotageUser1_031720225 usw. zurück
ODER	ermöglicht Ihnen die Angabe mehrerer Entitäten	AutoSabotageUser1_03172022 ODER AutoRansomUser4_03162022	Benutzer, Domäne, Entitätstyp, ursprünglicher Pfad, Entitätsname, Quell-IP		gibt entweder AutoSabotageUser1_03172022 oder AutoRansomUser4_03162022 zurück.
NICHT	ermöglicht es Ihnen, Text aus den Suchergebnissen auszuschließen	NOT AutoRansomUser4_03162022	Benutzer, Domäne, Entitätstyp, Originalpfad, Ordner der 1. Ebene, Ordner der 2. Ebene, Ordner der 3. Ebene, Ordner der 4. Ebene, Entitätsname, Quell-IP	Gerät	gibt alles zurück, was nicht mit „AutoRansomUser4_03162022“ beginnt

Filter	Was es bewirkt	Beispiel	Anwendbar für diese Filter	Gilt nicht für diese Filter	Ergebnis
Keine	sucht in allen Feldern nach NULL-Werten	Keine	Domain		gibt Ergebnisse zurück, bei denen das Zielfeld leer ist

Pfadsuche

Suchergebnisse mit und ohne / werden unterschiedlich sein

"/AutoDir1/AutoFile03242022"	Nur die exakte Suche funktioniert; gibt alle Aktivitäten mit dem exakten Pfad als /AutoDir1/AutoFile03242022 zurück (ohne Berücksichtigung der Groß-/Kleinschreibung).
"/AutoDir1/ "	Funktioniert; gibt alle Aktivitäten mit Verzeichnis der 1. Ebene zurück, das mit AutoDir1 übereinstimmt (ohne Berücksichtigung der Groß-/Kleinschreibung)
"/AutoDir1/AutoFile03242022/"	Funktioniert; gibt alle Aktivitäten zurück, bei denen das Verzeichnis der 1. Ebene mit AutoDir1 übereinstimmt und das Verzeichnis der 2. Ebene mit AutoFile03242022 übereinstimmt (ohne Berücksichtigung der Groß-/Kleinschreibung).
/AutoDir1/AutoFile03242022 ODER /AutoDir1/AutoFile03242022	Funktioniert nicht
NICHT /AutoDir1/AutoFile03242022	Funktioniert nicht
NICHT /AutoDir1	Funktioniert nicht
NICHT /AutoFile03242022	Funktioniert nicht
*	Funktioniert nicht

Änderungen der Aktivität des lokalen Root-SVM-Benutzers

Wenn ein lokaler Root-SVM-Benutzer eine Aktivität ausführt, wird jetzt die IP des Clients, auf dem die NFS-Freigabe gemountet ist, im Benutzernamen berücksichtigt. Dieser wird sowohl auf der Seite mit der forensischen Aktivität als auch auf der Seite mit der Benutzeraktivität als root@<IP-Adresse des Clients> angezeigt.

Beispiel:

- Wenn SVM-1 von Workload Security überwacht wird und der Root-Benutzer dieses SVM die Freigabe auf einem Client mit der IP-Adresse 10.197.12.40 bereitstellt, lautet der auf der Seite mit der forensischen Aktivität angezeigte Benutzername *root@10.197.12.40*.
- Wenn derselbe SVM-1 in einen anderen Client mit der IP-Adresse 10.197.12.41 eingebunden wird, lautet der auf der forensischen Aktivitätsseite angezeigte Benutzername *root@10.197.12.41*.

*• Dies geschieht, um die NFS-Root-Benutzeraktivität nach IP-Adresse zu trennen. Zuvor wurde davon ausgegangen, dass alle Aktivitäten nur vom Root-Benutzer ohne IP-Unterscheidung ausgeführt werden konnten.

Fehlerbehebung

Problem	Versuchen Sie Folgendes
In der Tabelle „Alle Aktivitäten“ wird der Benutzername in der Spalte „Benutzer“ wie folgt angezeigt: „ldap:HQ.COMPANYNAME.COM:S-1-5-21-3577637-1906459482-1437260136-1831817“ oder „ldap:default:80038003“.	Mögliche Gründe könnten sein: 1. Es wurden noch keine Benutzerverzeichnis-Sammler konfiguriert. Um einen hinzuzufügen, gehen Sie zu **Workload Security > Collectors > User Directory Collectors** und klicken Sie auf **+User Directory Collector**. Wählen Sie *Active Directory* oder *LDAP-Verzeichnisserver*. 2. Ein User Directory Collector wurde konfiguriert, wurde jedoch gestoppt oder befindet sich in einem Fehlerzustand. Gehen Sie bitte zu **Sammler > Benutzerverzeichnissammler** und überprüfen Sie den Status. Weitere Informationen finden Sie im"Fehlerbehebung beim User Directory Collector" Tipps zur Fehlerbehebung finden Sie im Abschnitt der Dokumentation. Nach der ordnungsgemäßen Konfiguration wird der Name innerhalb von 24 Stunden automatisch aufgelöst. Wenn das Problem immer noch nicht behoben ist, überprüfen Sie, ob Sie den richtigen Benutzerdatensammler hinzugefügt haben. Stellen Sie sicher, dass der Benutzer tatsächlich Teil des hinzugefügten Active Directory/LDAP-Verzeichnisservers ist.
Einige NFS-Ereignisse werden in der Benutzeroberfläche nicht angezeigt.	Überprüfen Sie Folgendes: 1. Ein Benutzerverzeichnis-Collector für AD-Server mit festgelegten POSIX-Attributen sollte mit dem über die Benutzeroberfläche aktivierten UnixID-Attribut ausgeführt werden. 2. Jeder Benutzer mit NFS-Zugriff sollte bei der Suche auf der Benutzerseite von UI 3 angezeigt werden. Rohereignisse (Ereignisse, bei denen der Benutzer noch nicht erkannt wurde) werden für NFS 4 nicht unterstützt. Anonyme Zugriffe auf den NFS-Export werden nicht überwacht. 5. Stellen Sie sicher, dass die verwendete NFS-Version 4.1 oder niedriger ist. (Beachten Sie, dass NFS 4.1 mit ONTAP 9.15 oder höher unterstützt wird.)

Nachdem ich in den Filtern auf den Seiten „Alle Aktivitäten“ oder „Entitäten“ der Forensik einige Buchstaben mit Platzhalterzeichen wie einem Sternchen (*) eingegeben habe, werden die Seiten sehr langsam geladen.	Ein Sternchen (*) im Suchstring sucht nach allem. Führende Platzhalterzeichenfolgen wie *<*Suchbegriff*> oder *<*Suchbegriff*>* führen jedoch zu einer langsamen Abfrage. Um eine bessere Leistung zu erzielen, verwenden Sie stattdessen Präfixzeichenfolgen im Format <*Suchbegriff*>* (mit anderen Worten: Fügen Sie das Sternchen (*) *nach* einem Suchbegriff an). Beispiel: Verwenden Sie die Zeichenfolge *testvolume** anstelle von **testvolume* oder **test*volume*. Verwenden Sie eine Verzeichnissuche, um alle Aktivitäten unter einem bestimmten Ordner rekursiv anzuzeigen (hierarchische Suche). Beispielsweise listet „/Pfad1/Pfad2/Pfad3/“ alle Aktivitäten unter /Pfad1/Pfad2/Pfad3 rekursiv auf. Alternativ können Sie die Option „Zum Filter hinzufügen“ unter der Registerkarte „Alle Aktivitäten“ verwenden.
Beim Verwenden eines Pfadfilters tritt die Fehlermeldung „Anforderung fehlgeschlagen mit Statuscode 500/503“ auf.	Versuchen Sie, zum Filtern der Datensätze einen kleineren Datumsbereich zu verwenden.
Die forensische Benutzeroberfläche lädt Daten langsam, wenn der *Pfad*-Filter verwendet wird.	Für schnellere Ergebnisse werden Verzeichnispfadfilter (Pfadzeichenfolge endet mit /) mit einer Tiefe von bis zu 4 Verzeichnissen empfohlen. Wenn der Verzeichnispfad beispielsweise /Aaa/Bbb/Ccc/Ddd lautet, versuchen Sie, nach „/Aaa/Bbb/Ccc/Ddd/“ zu suchen, um die Daten schneller zu laden.
Die Forensics-Benutzeroberfläche lädt Daten langsam und weist Fehler auf, wenn der Entitätsnamenfilter verwendet wird.	Bitte versuchen Sie es mit kleineren Zeiträumen und mit einer genauen Wertesuche mit Anführungszeichen. Wenn der EntityPath beispielsweise „/home/userX/nested1/nested2/nested3/testfile.txt“ ist, versuchen Sie es mit „testfile.txt“ als Entity-Namensfilter.

Forensische Benutzerübersicht

Informationen zu jedem Benutzer finden Sie in der Benutzerübersicht. Verwenden Sie diese Ansichten, um Benutzermerkmale, zugehörige Entitäten und aktuelle Aktivitäten zu verstehen.

Benutzerprofil

Zu den Benutzerprofilinformationen gehören Kontaktinformationen und Standort des Benutzers. Das Profil enthält die folgenden Informationen:

- Name des Benutzers
- E-Mail-Adresse des Nutzers
- Benutzermanager

- Telefonkontakt für den Benutzer
- Standort des Benutzers

Nutzerverhalten

Die Informationen zum Benutzerverhalten identifizieren die letzten Aktivitäten und Vorgänge, die der Benutzer durchgeführt hat. Zu diesen Informationen gehören:

- Letzte Aktivität
  - Letzter Zugriffsort
  - Aktivitätsdiagramm
  - Warnungen
- Operationen der letzten sieben Tage
  - Anzahl der Operationen

Aktualisierungsintervall

Die Benutzerliste wird alle 12 Stunden aktualisiert.

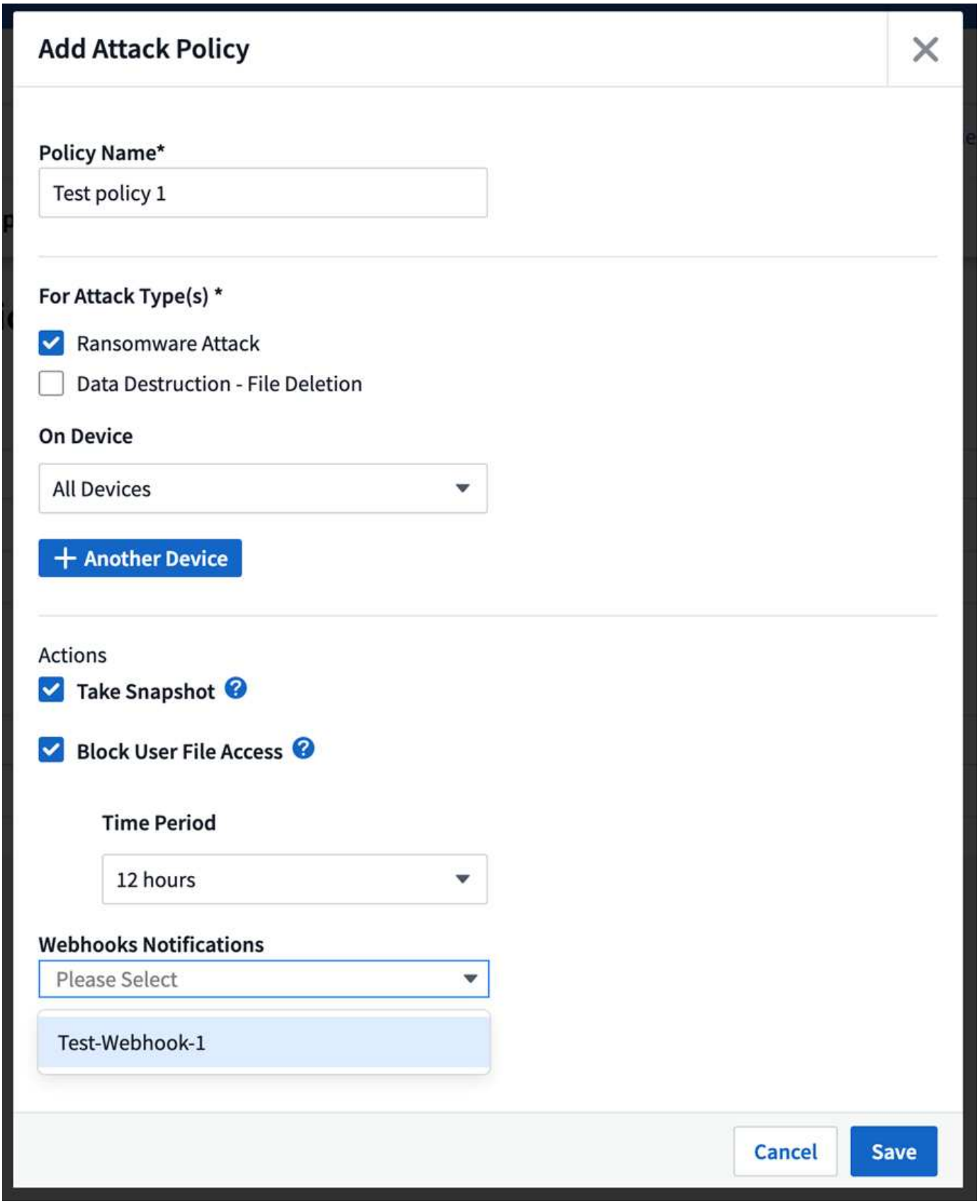
Aufbewahrungsrichtlinie

Wenn die Benutzerliste nicht erneut aktualisiert wird, bleibt sie 13 Monate lang erhalten. Nach 13 Monaten werden die Daten gelöscht. Wenn Ihre Workload Security-Umgebung gelöscht wird, werden alle mit der Umgebung verknüpften Daten gelöscht.

Richtlinien für automatisierte Antworten

Reaktionsrichtlinien lösen im Falle eines Angriffs oder abnormalen Benutzerverhaltens Aktionen aus, beispielsweise das Erstellen eines Snapshots oder die Einschränkung des Benutzerzugriffs.

Sie können Richtlinien für bestimmte oder alle Geräte festlegen. Um eine Antwortrichtlinie festzulegen, wählen Sie **Admin > Automatisierte Antwortrichtlinien** und klicken Sie auf die entsprechende Schaltfläche **+Richtlinie**. Sie können Richtlinien für Angriffe oder Warnungen erstellen.



Sie müssen die Richtlinie unter einem eindeutigen Namen speichern.

Um eine automatisierte Antwortaktion (z. B. „Snapshot erstellen“) zu deaktivieren, deaktivieren Sie einfach die Aktion und speichern Sie die Richtlinie.

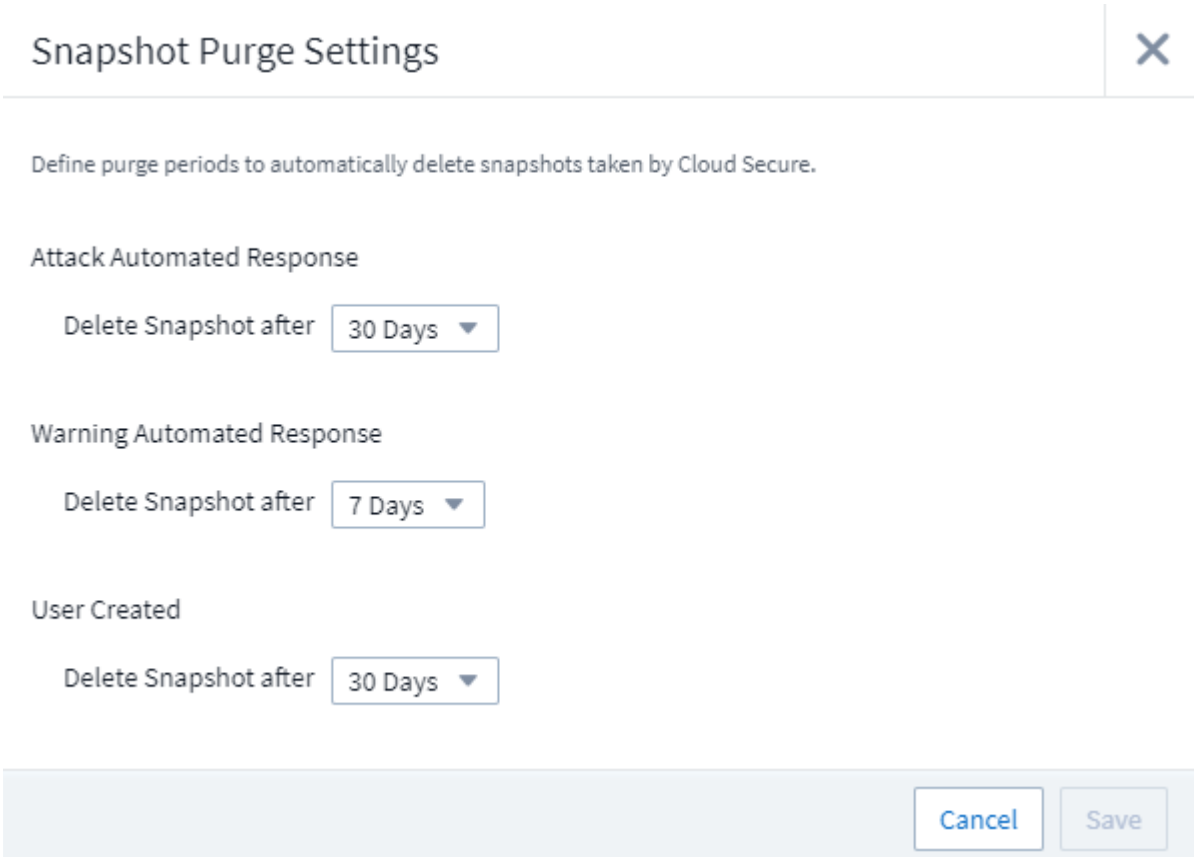
Wenn für die angegebenen Geräte (oder alle Geräte, falls ausgewählt) eine Warnung ausgelöst wird, erstellt die Richtlinie für automatisierte Antworten einen Snapshot Ihrer Daten. Sie können den Snapshot-Status auf der"Seite mit den Alarmdetails" .

Siehe die"Benutzerzugriff einschränken" Weitere Informationen zum Einschränken des Benutzerzugriffs per IP finden Sie auf der Seite.

Sie können einer Richtlinie einen oder mehrere Webhooks hinzufügen, um benachrichtigt zu werden, wenn eine Warnung erstellt und eine Aktion ausgeführt wird. Es wird empfohlen, einer Richtlinie nicht mehr als 10 Webhooks hinzuzufügen. Beachten Sie, dass keine Webhook-Benachrichtigungen ausgelöst werden, wenn eine Richtlinie angehalten wird.

Sie können eine Richtlinie für automatisierte Antworten ändern oder anhalten, indem Sie die Option im Dropdown-Menü der Richtlinie auswählen.

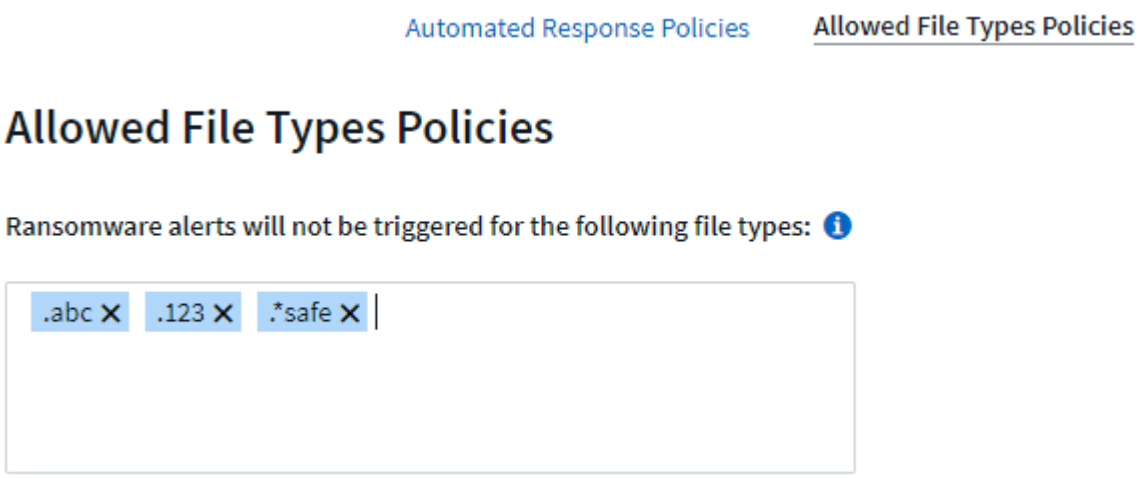
Workload Security löscht Snapshots basierend auf den Snapshot-Bereinigungseinstellungen automatisch einmal pro Tag.



Richtlinien für zulässige Dateitypen

Wenn ein Ransomware-Angriff für eine bekannte Dateierweiterung erkannt wird und auf dem Bildschirm „Warnungen“ Warnungen generiert werden, kann diese Dateierweiterung einer Liste *zulässiger Dateitypen* hinzugefügt werden, um unnötige Warnungen zu vermeiden.

Navigieren Sie zu **Workload-Sicherheit > Richtlinien** und wechseln Sie zur Registerkarte *Richtlinien für zulässige Dateitypen*.



Sobald der zulässige Dateityp zur Liste der *zulässigen Dateitypen* hinzugefügt wurde, wird für ihn kein Alarm mehr vor einem Ransomware-Angriff generiert. Beachten Sie, dass die Richtlinie „Zulässige Dateitypen“ nur für die Ransomware-Erkennung gilt.

Wenn beispielsweise eine Datei mit dem Namen *test.txt* in *test.txt.abc* umbenannt wird und Workload Security aufgrund der Erweiterung *.abc* einen Ransomware-Angriff erkennt, kann die Erweiterung *.abc* zur Liste der *zulässigen Dateitypen* hinzugefügt werden. Nach der Aufnahme in die Liste werden keine Ransomware-Angriffe mehr gegen Dateien mit der Erweiterung *.abc* ausgeführt.

Zulässige Dateitypen können exakte Übereinstimmungen (z. B. „.abc“) oder Ausdrücke (z. B. „.**Typ“, „.Typ**“ oder „**Typ**“) sein. Ausdrücke der Typen „.a*c“, „.p*f“ werden nicht unterstützt.

Integration mit ONTAP Autonomous Ransomware Protection

Die Funktion ONTAP Autonomous Ransomware Protection (ARP) nutzt Workload-Analysen in NAS-Umgebungen (NFS und SMB), um proaktiv ungewöhnliche Aktivitäten in Dateien zu erkennen und davor zu warnen, die auf einen Ransomware-Angriff hindeuten könnten.

Weitere Details und Lizenzanforderungen zu ARP finden Sie"hier," .

Workload Security lässt sich in ONTAP integrieren, um ARP-Ereignisse zu empfangen und eine zusätzliche Analyse- und automatische Antwortebene bereitzustellen.

Workload Security empfängt die ARP-Ereignisse von ONTAP und führt die folgenden Aktionen aus:

1. Korreliert Volume-Verschlüsselungsereignisse mit der Benutzeraktivität, um zu ermitteln, wer den Schaden verursacht.
2. Implementiert automatische Antwortrichtlinien (falls definiert)
3. Bietet forensische Funktionen:
    - Ermöglichen Sie Kunden die Durchführung von Untersuchungen zu Datenschutzverletzungen.
    - Ermitteln Sie, welche Dateien betroffen waren, und beschleunigen Sie so die Wiederherstellung und die Durchführung von Untersuchungen zu Datenschutzverletzungen.

Voraussetzungen

1. Mindestversion von ONTAP : 9.11.1
2. ARP-fähige Volumes. Details zur Aktivierung von ARP finden Sie"hier," . ARP muss über OnCommand System Manager aktiviert werden. Workload Security kann ARP nicht aktivieren.
3. Der Workload Security Collector sollte über die Cluster-IP hinzugefügt werden.
4. Damit diese Funktion funktioniert, sind Anmeldeinformationen auf Clusterebene erforderlich. Mit anderen Worten: Beim Hinzufügen der SVM müssen Anmeldeinformationen auf Clusterebene verwendet werden.

Erforderliche Benutzerberechtigungen

Wenn Sie Anmeldeinformationen für die Clusterverwaltung verwenden, sind keine neuen Berechtigungen erforderlich.

Wenn Sie einen benutzerdefinierten Benutzer (z. B. *csuser*) mit dem Benutzer erteilten Berechtigungen verwenden, führen Sie die folgenden Schritte aus, um Workload Security die Berechtigung zum Sammeln von ARP-bezogenen Informationen von ONTAP zu erteilen.

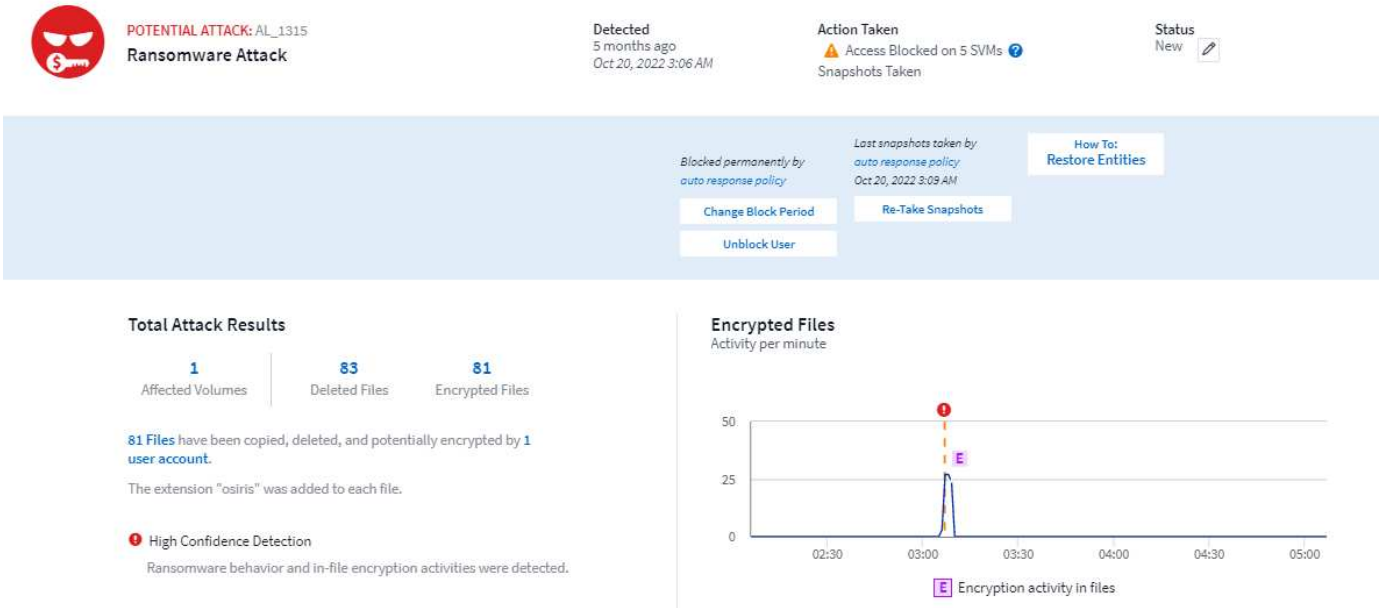
Führen Sie für *csuser* mit Cluster-Anmeldeinformationen Folgendes über die ONTAP Befehlszeile aus:

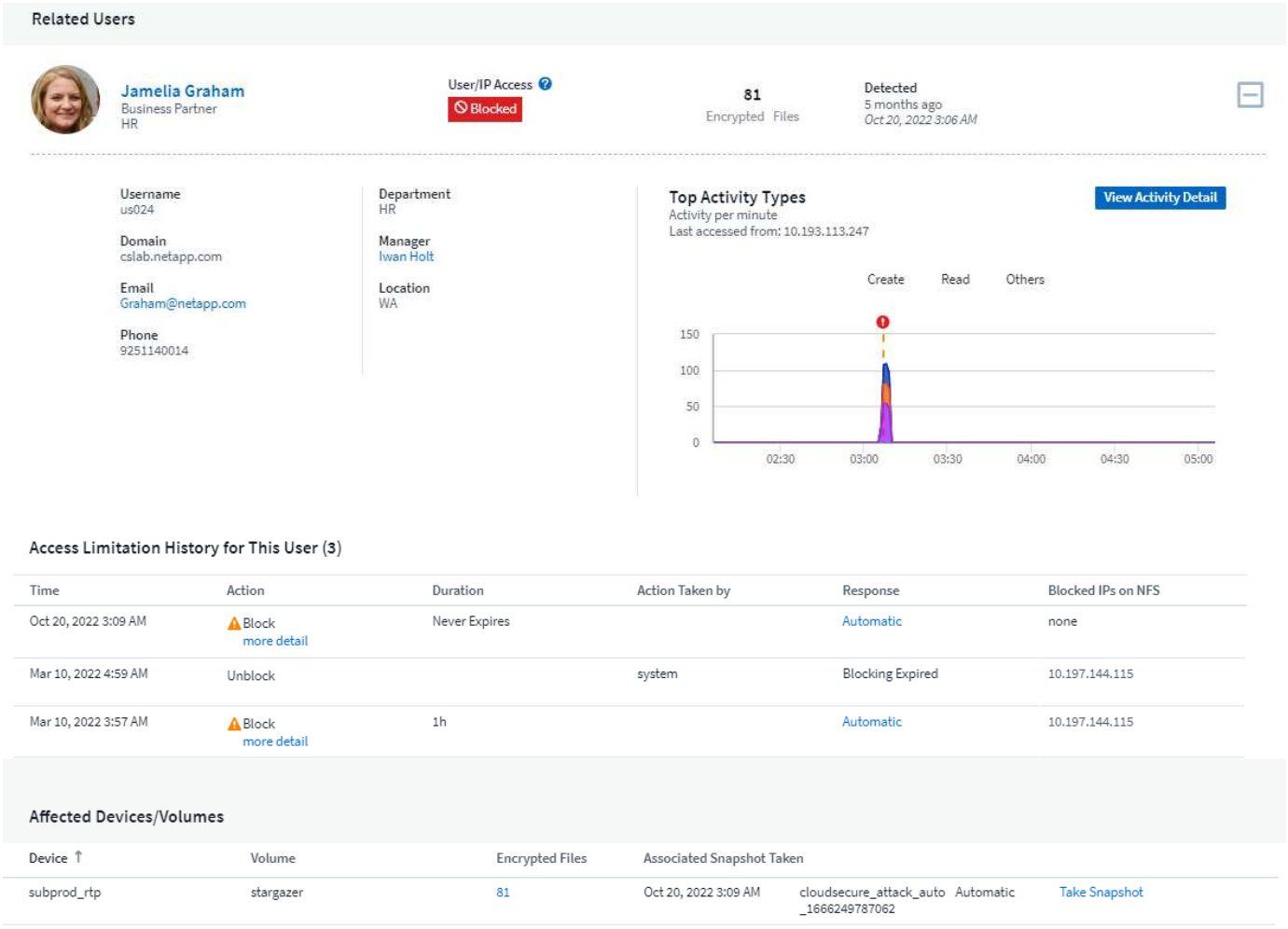
```
security login role create -role csrole -cmddirname "volume" -access
readonly
security login role create -role csrole -cmddirname "security anti-
ransomware volume" -access readonly
```

Lesen Sie mehr über die Konfiguration anderer"ONTAP-Berechtigungen" .

Beispielwarnung

Nachfolgend sehen Sie ein Beispiel für eine Warnung, die aufgrund eines ARP-Ereignisses generiert wurde:





Ein Banner mit hoher Vertrauenswürdigkeit weist darauf hin, dass der Angriff neben Dateiverschlüsselungsaktivitäten auch Ransomware-Verhalten gezeigt hat. Das Diagramm der verschlüsselten Dateien zeigt den Zeitstempel an, zu dem die Volume-Verschlüsselungsaktivität von der ARP-Lösung erkannt wurde.

Einschränkungen

Falls eine SVM nicht von Workload Security überwacht wird, aber von ONTAP ARP-Ereignisse generiert werden, werden die Ereignisse dennoch von Workload Security empfangen und angezeigt. Forensische Informationen im Zusammenhang mit der Warnung sowie die Benutzerzuordnung werden jedoch nicht erfasst oder angezeigt.

Fehlerbehebung

Bekannte Probleme und deren Lösungen werden in der folgenden Tabelle beschrieben.

Problem:	Auflösung:
E-Mail-Benachrichtigungen werden 24 Stunden nach Erkennung eines Angriffs empfangen. In der Benutzeroberfläche werden die Warnungen 24 Stunden vorher angezeigt, wenn die E-Mails von Data Infrastructure Insights Workload Security empfangen werden.	Wenn ONTAP das Ereignis *Ransomware erkannt* an Data Infrastructure Insights Workload Security (d. h. Workload Security) sendet, wird die E-Mail gesendet. Das Ereignis enthält eine Liste der Angriffe und deren Zeitstempel. Die Workload Security-Benutzeroberfläche zeigt den Alarmzeitstempel der ersten angegriffenen Datei an. ONTAP sendet das Ereignis *Ransomware erkannt* an Data Infrastructure Insights, wenn eine bestimmte Anzahl von Dateien verschlüsselt ist. Daher kann es zu einer Differenz zwischen dem Zeitpunkt, zu dem die Warnung in der Benutzeroberfläche angezeigt wird, und dem Zeitpunkt, zu dem die E-Mail gesendet wird, kommen.

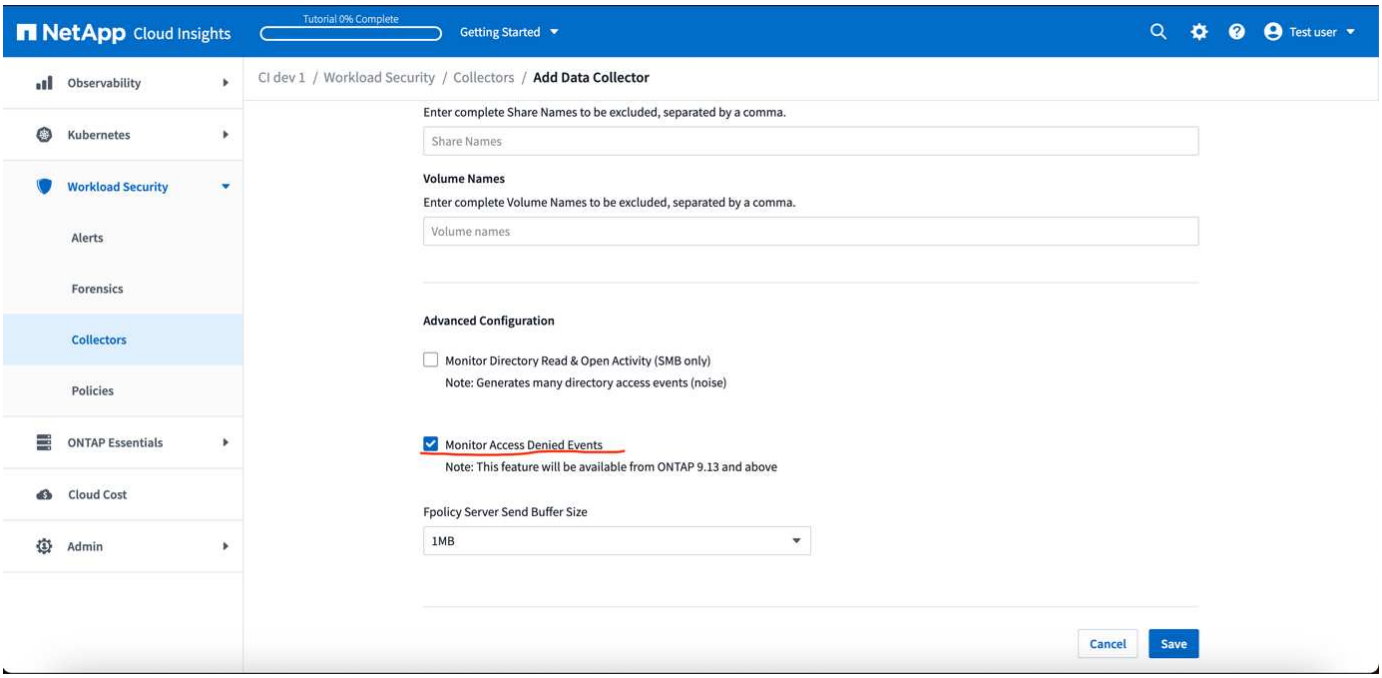
Integration mit ONTAP Access Denied

Die ONTAP Access Denied-Funktion verwendet eine Workload-Analyse in NAS-Umgebungen (NFS und SMB), um fehlgeschlagene Dateivorgänge (z. B. wenn ein Benutzer versucht, einen Vorgang auszuführen, für den er keine Berechtigung hat) proaktiv zu erkennen und davor zu warnen. Diese Benachrichtigungen über fehlgeschlagene Dateivorgänge – insbesondere bei sicherheitsrelevanten Fehlern – tragen zusätzlich dazu bei, Insider-Angriffe bereits im Frühstadium zu blockieren.

Data Infrastructure Insights Workload Security lässt sich in ONTAP integrieren, um Zugriffsverweigerungsereignisse zu empfangen und eine zusätzliche Analyse- und automatische Reaktionsebene bereitzustellen.

Voraussetzungen

- Mindestversion von ONTAP : 9.13.0.
- Ein Workload-Sicherheitsadministrator muss die Funktion „Zugriff verweigert“ aktivieren, wenn er einen neuen Collector hinzufügt oder einen vorhandenen Collector bearbeitet, indem er unter „Erweiterte Konfiguration“ das Kontrollkästchen „Ereignisse „Zugriff verweigert“ überwachen“ aktiviert.



Erforderliche Benutzerberechtigungen

Wenn der Datensammler mithilfe der Clusteradministrationsanmeldeinformationen hinzugefügt wird, sind keine neuen Berechtigungen erforderlich.

Wenn der Collector mithilfe eines benutzerdefinierten Benutzers (z. B. *csuser*) mit dem Benutzer erteilten Berechtigungen hinzugefügt wird, führen Sie die folgenden Schritte aus, um Workload Security die erforderliche Berechtigung zum Registrieren für Zugriffsverweigerungsereignisse bei ONTAP zu erteilen.

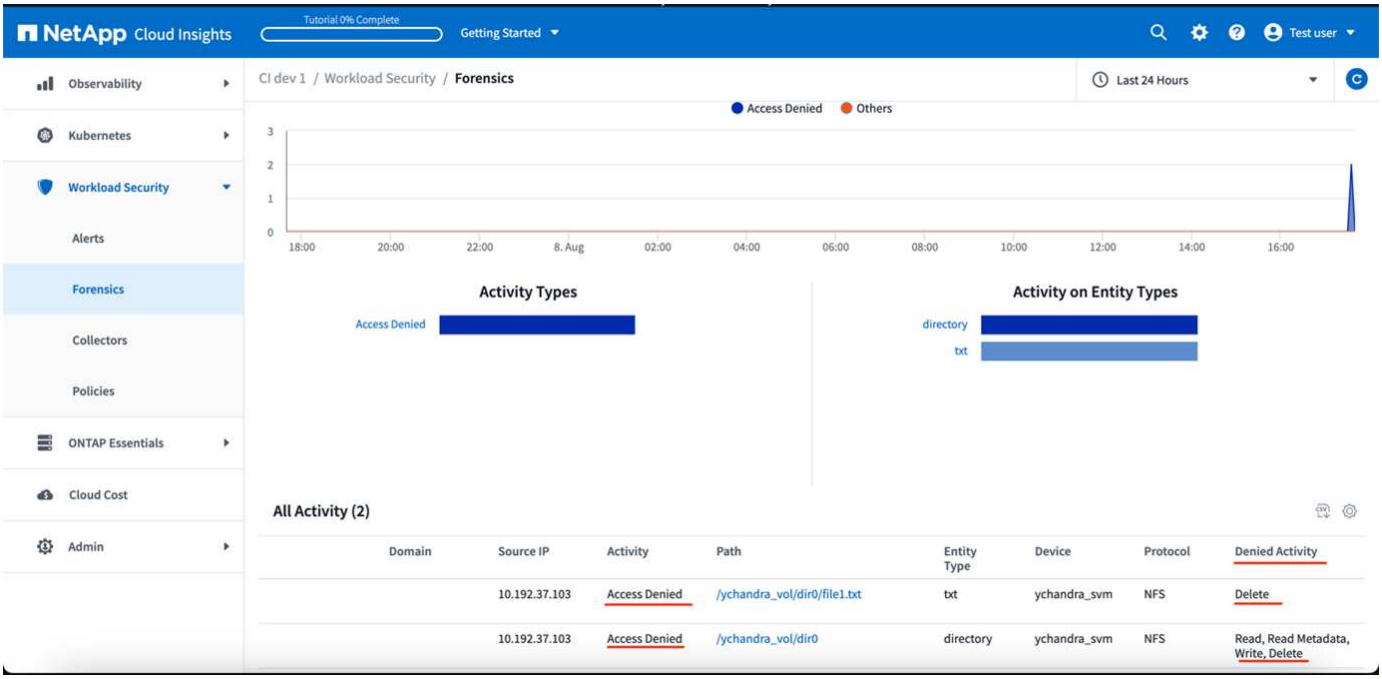
Führen Sie für csuser mit *cluster*-Anmeldeinformationen die folgenden Befehle über die ONTAP -Befehlszeile aus. Beachten Sie, dass diese Berechtigung möglicherweise bereits vorhanden ist.

```
 security login role create -role csrole -cmddirname "vserver fpolicy"
-access all
Führen Sie für csuser mit _SVM_-Anmeldeinformationen die folgenden Befehle
über die ONTAP -Befehlszeile aus.  Beachten Sie, dass diese Berechtigung
möglicherweise bereits vorhanden ist.
```

```
 security login role create -vserver <vservername> -role csrole
-cmddirname "vserver fpolicy" -access all
Lesen Sie mehr über die Konfiguration
andererlink:task_add_collector_svm.html["ONTAP-Berechtigungen"] .
```

Ereignisse vom Typ „Zugriff verweigert“

Sobald Ereignisse vom ONTAP System abgerufen wurden, werden auf der Seite „Workload Security Forensics“ Ereignisse mit dem Status „Zugriff verweigert“ angezeigt. Zusätzlich zu den angezeigten Informationen können Sie die fehlenden Benutzerberechtigungen für einen bestimmten Vorgang anzeigen, indem Sie der Tabelle über das Zahnradsymbol die Spalte *Gewünschte Aktivität* hinzufügen.



Blockieren des Benutzerzugriffs

Sobald ein Angriff erkannt wird, kann Workload Security den Angriff stoppen, indem es den Benutzerzugriff auf das Dateisystem blockiert. Der Zugriff kann automatisch mithilfe automatisierter Antwortrichtlinien oder manuell über die Warn- oder Benutzerdetailseiten blockiert werden.

Beim Sperren des Benutzerzugriffs sollten Sie einen Sperrzeitraum festlegen. Nach Ablauf des ausgewählten Zeitraums wird der Benutzerzugriff automatisch wiederhergestellt. Die Zugriffsblockierung wird sowohl für SMB- als auch für NFS-Protokolle unterstützt.

Der Benutzer wird direkt für SMB blockiert und die IP-Adresse der Host-Computer, die den Angriff verursachen, wird für NFS blockiert. Den IP-Adressen dieser Maschinen wird der Zugriff auf alle von Workload Security überwachten Storage Virtual Machines (SVMs) verweigert.

Nehmen wir beispielsweise an, dass Workload Security 10 SVMs verwaltet und die Richtlinie für automatische Antworten für vier dieser SVMs konfiguriert ist. Wenn der Angriff von einer der vier SVMs ausgeht, wird der Zugriff des Benutzers auf allen 10 SVMs blockiert. Auf der ursprünglichen SVM wird weiterhin ein Snapshot erstellt.

Wenn vier SVMs vorhanden sind und eine SVM für SMB, eine für NFS und die beiden anderen sowohl für NFS als auch für SMB konfiguriert sind, werden alle SVMs blockiert, wenn der Angriff von einer der vier SVMs ausgeht.

Voraussetzungen für die Benutzerzugriffssperre

Damit diese Funktion funktioniert, sind Anmeldeinformationen auf Clusterebene erforderlich.

Wenn Sie Anmeldeinformationen für die Clusterverwaltung verwenden, sind keine neuen Berechtigungen erforderlich.

Wenn Sie einen benutzerdefinierten Benutzer (z. B. *csuser*) mit dem Benutzer erteilten Berechtigungen

verwenden, führen Sie die folgenden Schritte aus, um Workload Security die Berechtigung zum Blockieren des Benutzers zu erteilen.

Führen Sie für csuser mit Cluster-Anmeldeinformationen Folgendes über die ONTAP -Befehlszeile aus:

```
security login role create -role csrole -cmddirname "vserver export-policy
rule" -access all
security login role create -role csrole -cmddirname set -access all
security login role create -role csrole -cmddirname "vserver cifs session"
-access all
security login role create -role csrole -cmddirname "vserver services
access-check authentication translate" -access all
security login role create -role csrole -cmddirname "vserver name-mapping"
-access all
```

Lesen Sie unbedingt den Abschnitt „Berechtigungen“ der"Konfigurieren des ONTAP SVM-Datenkollektors" Seite auch.

Wie aktiviere ich die Funktion?

- Navigieren Sie in Workload Security zu **Workload Security > Richtlinien > Richtlinien für automatisierte Antworten**. Wählen Sie **+Angriffsrichtlinie**.
- Wählen (aktivieren) Sie „Dateizugriff des Benutzers blockieren“.

Wie richte ich die automatische Sperrung des Benutzerzugriffs ein?

- Erstellen Sie eine neue Angriffsrichtlinie oder bearbeiten Sie eine vorhandene Angriffsrichtlinie.
- Wählen Sie die SVMs aus, auf denen die Angriffsrichtlinie überwacht werden soll.
- Klicken Sie auf das Kontrollkästchen „Dateizugriff des Benutzers blockieren“. Die Funktion wird aktiviert, wenn diese Option ausgewählt ist.
- Wählen Sie unter „Zeitraum“ den Zeitraum aus, bis zu dem die Sperre gelten soll.
- Um die automatische Benutzerblockierung zu testen, können Sie einen Angriff über eine"simuliertes Skript" .

Wie kann ich feststellen, ob es im System blockierte Benutzer gibt?

- Auf der Seite mit den Warnlisten wird oben auf dem Bildschirm ein Banner angezeigt, falls ein Benutzer blockiert wird.
- Durch Klicken auf das Banner gelangen Sie zur Seite „Benutzer“, auf der die Liste der blockierten Benutzer angezeigt wird.
- Auf der Seite „Benutzer“ gibt es eine Spalte mit der Bezeichnung „Benutzer-/IP-Zugriff“. In dieser Spalte wird der aktuelle Status der Benutzerblockierung angezeigt.

Manuelles Einschränken und Verwalten des Benutzerzugriffs

- Sie können zum Bildschirm mit den Alarmdetails oder Benutzerdetails gehen und dann von diesen Bildschirmen aus einen Benutzer manuell sperren oder wiederherstellen.

Verlauf der Benutzerzugriffsbeschränkungen

Auf der Seite mit den Alarmdetails und Benutzerdetails im Benutzerbereich können Sie eine Prüfung des Zugriffsbeschränkungsverlaufs des Benutzers anzeigen: Zeit, Aktion (Blockieren, Entsperren), Dauer, durchgeführte Aktion, manuell/automatisch und betroffene IPs für NFS.

Wie deaktiviere ich die Funktion?

Sie können die Funktion jederzeit deaktivieren. Wenn im System eingeschränkte Benutzer vorhanden sind, müssen Sie deren Zugriff zuerst wiederherstellen.

- Navigieren Sie in Workload Security zu **Workload Security > Richtlinien > Richtlinien für automatisierte Antworten**. Wählen Sie **+Angriffsrichtlinie**.
- Deaktivieren Sie „Benutzerdateizugriff blockieren“.

Die Funktion wird auf allen Seiten ausgeblendet.

Manuelles Wiederherstellen von IPs für NFS

Führen Sie die folgenden Schritte aus, um alle IPs von ONTAP manuell wiederherzustellen, wenn Ihre Workload Security-Testversion abläuft oder der Agent/Collector ausgefallen ist.

1. Listen Sie alle Exportrichtlinien auf einer SVM auf.

```
contrail-qa-fas8020:> export-policy rule show -vserver <svm name>
             Policy          Rule    Access   Client                RO
Vserver      Name            Index   Protocol Match                 Rule
------------ --------------- ------  -------- ---------------------
---------
svm0         default         1       nfs3,    cloudsecure_rule,     never
                                     nfs4,    10.11.12.13
                                     cifs
svm1         default         4       cifs,    0.0.0.0/0             any
                                     nfs
svm2         test            1       nfs3,    cloudsecure_rule,     never
                                     nfs4,    10.11.12.13
                                     cifs
svm3         test            3       cifs,    0.0.0.0/0             any
                                     nfs,
                                     flexcache
4 entries were displayed.
```

2. Löschen Sie die Regeln für alle Richtlinien auf der SVM, die „cloudsecure_rule“ als Client-Übereinstimmung haben, indem Sie den entsprechenden RuleIndex angeben. Die Workload-Sicherheitsregel steht normalerweise auf 1.

```
 contrail-qa-fas8020:*> export-policy rule delete -vserver <svm name>
-policyname * -ruleindex 1
. Stellen Sie sicher, dass die Workload-Sicherheitsregel gelöscht ist
(optionaler Schritt zur Bestätigung).
```

```
contrail-qa-fas8020:*> export-policy rule show -vserver <svm name>
             Policy          Rule    Access   Client                RO
Vserver      Name            Index   Protocol Match                 Rule
------------ --------------- ------  -------- ---------------------
---------
svm0         default         4       cifs,    0.0.0.0/0             any
                                     nfs
svm2         test            3       cifs,    0.0.0.0/0             any
                                     nfs,
                                     flexcache
2 entries were displayed.
```

Manuelles Wiederherstellen von Benutzern für SMB

Führen Sie die folgenden Schritte aus, um alle Benutzer von ONTAP manuell wiederherzustellen, wenn Ihre Workload Security-Testversion abläuft oder der Agent/Collector ausgefallen ist.

Sie können die Liste der in Workload Security blockierten Benutzer auf der Benutzerlistenseite abrufen.

1. Melden Sie sich mit den Cluster-Admin-Anmeldeinformationen beim ONTAP -Cluster an (wo Sie die Blockierung der Benutzer aufheben möchten). (Melden Sie sich bei Amazon FSx mit Ihren FSx-Anmeldeinformationen an.)
2. Führen Sie den folgenden Befehl aus, um alle von Workload Security für SMB blockierten Benutzer in allen SVMs aufzulisten:

```
vserver name-mapping show -direction win-unix -replacement " "
```

```
Vserver:   <vservername>
Direction: win-unix
Position Hostname         IP Address/Mask
-------- ---------------- ----------------
1       -                -                    Pattern: CSLAB\\US040
                                          Replacement:
2       -                -                    Pattern: CSLAB\\US030
                                          Replacement:
2 entries were displayed.
```

In der obigen Ausgabe wurden 2 Benutzer (US030, US040) mit der Domäne CSLAB blockiert.

1. Sobald wir die Position anhand der obigen Ausgabe identifiziert haben, führen Sie den folgenden Befehl aus, um die Blockierung des Benutzers aufzuheben:

```
 vserver name-mapping delete -direction win-unix -position <position>
. Bestätigen Sie die Blockierung der Benutzer, indem Sie den folgenden
Befehl ausführen:
```

```
vserver name-mapping show -direction win-unix -replacement " "
```

Für die zuvor gesperrten Benutzer sollen keine Einträge mehr angezeigt werden.

Fehlerbehebung

Problem	Versuchen Sie Folgendes
Einige Benutzer werden nicht eingeschränkt, obwohl es einen Angriff gibt.	1. Stellen Sie sicher, dass sich der Datensammler und der Agent für die SVMs im Status „Ausführen“ befinden. Workload Security kann keine Befehle senden, wenn der Datensammler und der Agent gestoppt sind. 2. Dies liegt daran, dass der Benutzer möglicherweise von einem Computer mit einer neuen IP auf den Speicher zugegriffen hat, die zuvor nicht verwendet wurde. Die Einschränkung erfolgt über die IP-Adresse des Hosts, über den der Benutzer auf den Speicher zugreift. Suchen Sie in der Benutzeroberfläche (Alarmdetails > Zugriffsbeschränkungsverlauf für diesen Benutzer > Betroffene IPs) nach der Liste der eingeschränkten IP-Adressen. Wenn der Benutzer auf den Speicher von einem Host aus zugreift, dessen IP-Adresse sich von den eingeschränkten IP-Adressen unterscheidet, kann der Benutzer dennoch über die nicht eingeschränkte IP-Adresse auf den Speicher zugreifen. Wenn der Benutzer versucht, von Hosts aus zuzugreifen, deren IPs eingeschränkt sind, ist der Speicher nicht zugänglich.
Wenn Sie manuell auf „Zugriff einschränken“ klicken, wird die Meldung „Die IP-Adressen dieses Benutzers wurden bereits eingeschränkt“ angezeigt.	Die einzuschränkende IP wird bereits von einem anderen Benutzer eingeschränkt.
Die Richtlinie konnte nicht geändert werden. Grund: Für diesen Befehl nicht autorisiert.	Überprüfen Sie, ob bei Verwendung von csuser dem Benutzer die oben genannten Berechtigungen erteilt wurden.

Problem	Versuchen Sie Folgendes
Die Benutzerblockierung (IP-Adresse) für NFS funktioniert, aber für SMB/CIFS wird eine Fehlermeldung angezeigt: „Die Umwandlung von SID in Domänenname ist fehlgeschlagen.“ Grund für Timeout: Socket ist nicht eingerichtet“	Dies kann passieren, wenn *csuser* keine Berechtigung zum Ausführen von SSH hat. (Stellen Sie die Verbindung auf Clusterebene sicher und stellen Sie dann sicher, dass der Benutzer SSH ausführen kann.) Die Rolle *csuser* erfordert diese Berechtigungen. https://docs.netapp.com/us-en/cloudinsights/cs_restrict_user_access.html#prerequisites-for-user-access-blocking Für *csuser* mit Cluster-Anmeldeinformationen führen Sie Folgendes von der ONTAP Befehlszeile aus: security login role create -role csrole -cmddirname "vserver export-policy rule" -access all security login role create -role csrole -cmddirname set -access all security login role create -role csrole -cmddirname "vserver cifs session" -access all security login role create -role csrole -cmddirname "vserver services access-check authentication translate" -access all security login role create -role csrole -cmddirname "vserver name-mapping" -access all Wenn *csuser* nicht verwendet wird und der Administratorbenutzer auf Clusterebene verwendet wird, stellen Sie sicher, dass der Administratorbenutzer über SSH-Berechtigungen für ONTAP verfügt.
Ich erhalte die Fehlermeldung *SID-Übersetzung fehlgeschlagen. Grund:255:Fehler: Befehl fehlgeschlagen: für diesen Befehl nicht autorisiert.Fehler: „access-check“ ist kein erkannter Befehl*, obwohl ein Benutzer hätte gesperrt werden sollen.	Dies kann passieren, wenn *csuser* nicht über die richtigen Berechtigungen verfügt. Sehen "Voraussetzungen für die Benutzerzugriffssperre" für weitere Informationen. Nach dem Anwenden der Berechtigungen wird empfohlen, den ONTAP Datensammler und den Benutzerverzeichnis-Datensammler neu zu starten. Die erforderlichen Berechtigungsbefehle sind unten aufgeführt. ---- Sicherheits-Login-Rolle erstellen -role csrole -cmddirname "vServer-Exportrichtlinienregel" -alles zugreifen Sicherheits-Login-Rolle erstellen -role csrole -cmddirname festlegen -alles zugreifen Sicherheits-Login-Rolle erstellen -role csrole -cmddirname "vServer-CIFS-Sitzung" -alles zugreifen Sicherheits-Login-Rolle erstellen -role csrole -cmddirname "vServer-Dienste-Zugriffsprüfung, Authentifizierungsübersetzung" -alles zugreifen Sicherheits-Login-Rolle erstellen -role csrole -cmddirname "vServer-Namenszuordnung" -alles zugreifen ----

Workload-Sicherheit: Simulation eines Angriffs

Sie können die Anweisungen auf dieser Seite verwenden, um einen Angriff zum Testen oder Demonstrieren der Workload-Sicherheit mithilfe des enthaltenen Ransomware-Simulationsskripts zu simulieren.

Dinge, die Sie vor dem Beginn beachten sollten

- Das Ransomware-Simulationsskript funktioniert nur unter Linux. Das Simulationsskript sollte auch Warnmeldungen mit hoher Zuverlässigkeit generieren, falls der Benutzer ONTAP ARP mit Workload Security integriert hat.
- Workload Security erkennt mit NFS 4.1 generierte Ereignisse und Warnungen nur, wenn die ONTAP Version 9.15 oder höher ist.
- Das Skript wird mit den Installationsdateien des Workload Security-Agenten bereitgestellt. Es ist auf jedem Computer verfügbar, auf dem ein Workload Security-Agent installiert ist.
- Sie können das Skript auf der Workload Security-Agent-Maschine selbst ausführen. Es ist nicht erforderlich, eine weitere Linux-Maschine vorzubereiten. Wenn Sie das Skript jedoch lieber auf einem anderen System ausführen möchten, kopieren Sie das Skript einfach und führen Sie es dort aus.
- Benutzer können sich je nach ihren Präferenzen und Systemanforderungen entweder für das Python- oder das Shell-Skript entscheiden.
- Für das Python-Skript sind Installationen erforderlich. Wenn Sie Python nicht verwenden möchten, verwenden Sie das Shell-Skript.

Richtlinien:

Dieses Skript sollte auf einer SVM ausgeführt werden, die einen Ordner mit einer beträchtlichen Anzahl zu verschlüsselnder Dateien enthält, idealerweise 100 oder mehr, einschließlich Dateien in Unterordnern. Stellen Sie sicher, dass die Dateien nicht leer sind.

Um die Warnung zu generieren, halten Sie den Collector vor der Erstellung der Testdaten vorübergehend an. Sobald die Beispieldateien generiert sind, setzen Sie den Collector fort und starten Sie den Verschlüsselungsprozess.

Schritte:

Bereiten Sie das System vor:

Mounten Sie zunächst das Zielvolume auf der Maschine. Sie können entweder einen NFS- oder einen CIFS-Export mounten.

So mounten Sie den NFS-Export unter Linux:

```
mount -t nfs -o vers=4.0 10.193.177.158:/svmvol1 /mntpt
mount -t nfs -o vers=4.0 Vserver data IP>:/nfsvol /destinationlinuxfolder
```

Mounten Sie NFS Version 4.1 nicht, da es von Fpolicy nicht unterstützt wird.

So mounten Sie CIFS unter Linux:

```
mount -t cifs //10.193.77.91/sharedfolderincluster
/root/destinationfolder/ -o username=raisa
```

Aktivieren Sie den autonomen ONTAP Ransomware-Schutz (optional):

Wenn Ihre ONTAP Clusterversion 9.11.1 oder höher ist, können Sie den ONTAP Ransomware Protection-Dienst aktivieren, indem Sie den folgenden Befehl auf der ONTAP Befehlskonsole ausführen.

```
 security anti-ransomware volume enable -volume [volume_name] -vserver
[svm_name]
Richten Sie als Nächstes einen Datensammler ein:
```

1. Konfigurieren Sie den Workload Security-Agenten, falls dies noch nicht geschehen ist.
2. Konfigurieren Sie einen SVM-Datensammler, falls dies noch nicht geschehen ist.
3. Stellen Sie sicher, dass beim Konfigurieren des Datensammlers das Mount-Protokoll ausgewählt ist.

Generieren Sie die Beispieldateien programmgesteuert:

Bevor Sie die Dateien erstellen, müssen Sie zuerst stoppen oder"den Datensammler anhalten" Verarbeitung.

Bevor Sie die Simulation ausführen, müssen Sie zunächst zu verschlüsselnde Dateien hinzufügen. Sie können die zu verschlüsselnden Dateien entweder manuell in den Zielordner kopieren oder eines der enthaltenen Skripte verwenden, um die Dateien programmgesteuert zu erstellen. Unabhängig davon, welche Methode Sie verwenden, stellen Sie sicher, dass mindestens 100 Dateien zum Verschlüsseln vorhanden sind.

Wenn Sie die Dateien programmgesteuert erstellen möchten, können Sie die Shell oder Python verwenden:

Hülse:

1. Melden Sie sich beim Agentenfeld an.
2. Mounten Sie eine NFS- oder CIFS-Freigabe vom SVM des Filers auf der Agent-Maschine. Wechseln Sie mit CD in diesen Ordner.
3. Kopieren Sie das Skript aus dem Agent-Installationsverzeichnis (%AGENT_INSTALL_DIR/ agent/install/ransomware_simulation/shell/create_dataset.sh) an den Ziel-Mount-Speicherort.
4. Führen Sie den folgenden Befehl mithilfe der Skripts im bereitgestellten Verzeichnis (z. B. /root/demo) aus, um den Ordner und die Dateien des Testdatensatzes zu erstellen:

   ```
    './create_dataset.sh'
   . Dadurch werden 100 nicht leere Dateien mit verschiedenen Erweiterungen
   im Mount-Ordner unter einem Verzeichnis namens „test_dataset“ erstellt.
   ```

Python:

Python-Skript Voraussetzung:

- Installieren Sie Python (falls noch nicht installiert).
  - Laden Sie Python 3.5.2 oder höher herunter von https://www.python.org/ .
  - Um die Python-Installation zu überprüfen, führen Sie `python --version` .
  - Das Python-Skript wurde bereits in Versionen ab 3.5.2 getestet.

- Installieren Sie pip, falls es noch nicht installiert ist:
  - Laden Sie das Skript get-pip.py herunter von https://bootstrap.pypa.io/ .
  - Installieren Sie pip mit `python get-pip.py` .
  - Überprüfen Sie die Pip-Installation mit `pip --version` .
- PyCryptodome-Bibliothek:
  - Das Skript verwendet die PyCryptodome-Bibliothek.
  - Installieren Sie PyCryptodome mit `pip install pycryptodome` .
  - Bestätigen Sie die Installation von PyCryptodome durch Ausführen `pip show pycryptodome` .

Python-Skript zum Erstellen von Dateien:

1. Melden Sie sich beim Agentenfeld an.
2. Mounten Sie eine NFS- oder CIFS-Freigabe vom SVM des Filers auf der Agent-Maschine. Wechseln Sie mit CD in diesen Ordner.
3. Kopieren Sie das Skript aus dem Agent-Installationsverzeichnis (%AGENT_INSTALL_DIR/agent/install/ransomware_simulation/python/create_dataset.py) an den Ziel-Mount-Speicherort.
4. Führen Sie den folgenden Befehl mithilfe der Skripts im bereitgestellten Verzeichnis (z. B. /root/demo) aus, um den Ordner und die Dateien für den Testdatensatz zu erstellen:

```
 'python create_dataset.py'
. Dadurch werden 100 nicht leere Dateien mit verschiedenen Erweiterungen
im Mount-Ordner unter einem Verzeichnis namens „test_dataset“ erstellt.
```

Fortsetzen des Collectors

Wenn Sie den Collector vor dem Ausführen dieser Schritte angehalten haben, denken Sie bitte daran, den Collector wieder aufzunehmen, sobald die Beispieldateien erstellt wurden.

Generieren Sie die Beispieldateien programmgesteuert:

Bevor Sie die Dateien erstellen, müssen Sie zuerst stoppen oder"den Datensammler anhalten" Verarbeitung.

Um eine Ransomware-Warnung zu generieren, können Sie das enthaltene Skript ausführen, das eine Ransomware-Warnung in Workload Security simuliert.

Hülse:

1. Kopieren Sie das Skript aus dem Agent-Installationsverzeichnis (%AGENT_INSTALL_DIR/agent/install/ransomware_simulation/shell/simulate_attack.sh) an den Ziel-Mount-Speicherort.
2. Führen Sie den folgenden Befehl mithilfe der Skripte im bereitgestellten Verzeichnis (z. B. /root/demo) aus, um den Testdatensatz zu verschlüsseln:

```
 './simulate_attack.sh'
. Dadurch werden die im Verzeichnis „test_dataset“ erstellten
Beispieldateien verschlüsselt.
```

Python:

1. Kopieren Sie das Skript aus dem Agent-Installationsverzeichnis (%AGENT_INSTALL_DIR/agent/install/ransomware_simulation/python/simulate_attack.py) an den Ziel-Mount-Speicherort.
2. Bitte beachten Sie, dass die Python-Voraussetzungen gemäß dem Abschnitt „Voraussetzungen für Python-Skripte“ installiert werden.
3. Führen Sie den folgenden Befehl mithilfe der Skripte im bereitgestellten Verzeichnis (z. B. /root/demo) aus, um den Testdatensatz zu verschlüsseln:

```
 'python simulate_attack.py'
. Dadurch werden die im Verzeichnis „test_dataset“ erstellten
Beispieldateien verschlüsselt.
```

Generieren einer Warnung in Workload Security

Sobald die Ausführung des Simulatorskripts abgeschlossen ist, wird innerhalb weniger Minuten eine Warnung auf der Web-Benutzeroberfläche angezeigt.

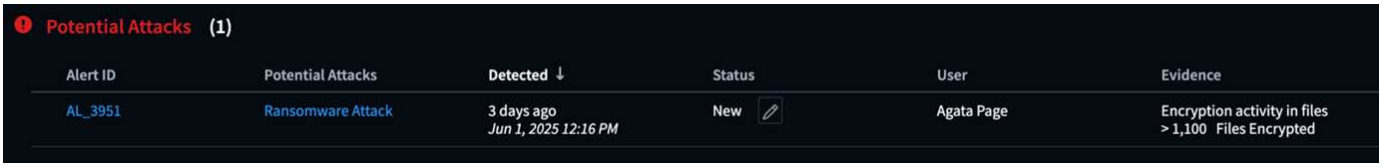
Hinweis: Falls alle der folgenden Bedingungen erfüllt sind, wird eine Warnung mit hoher Zuverlässigkeit generiert.

1. Überwachte SVM- ONTAP Version höher als 9.11.1
2. ONTAP Autonomous Ransomware Protection konfiguriert
3. Der Workload Security Data Collector wird im Clustermodus hinzugefügt.

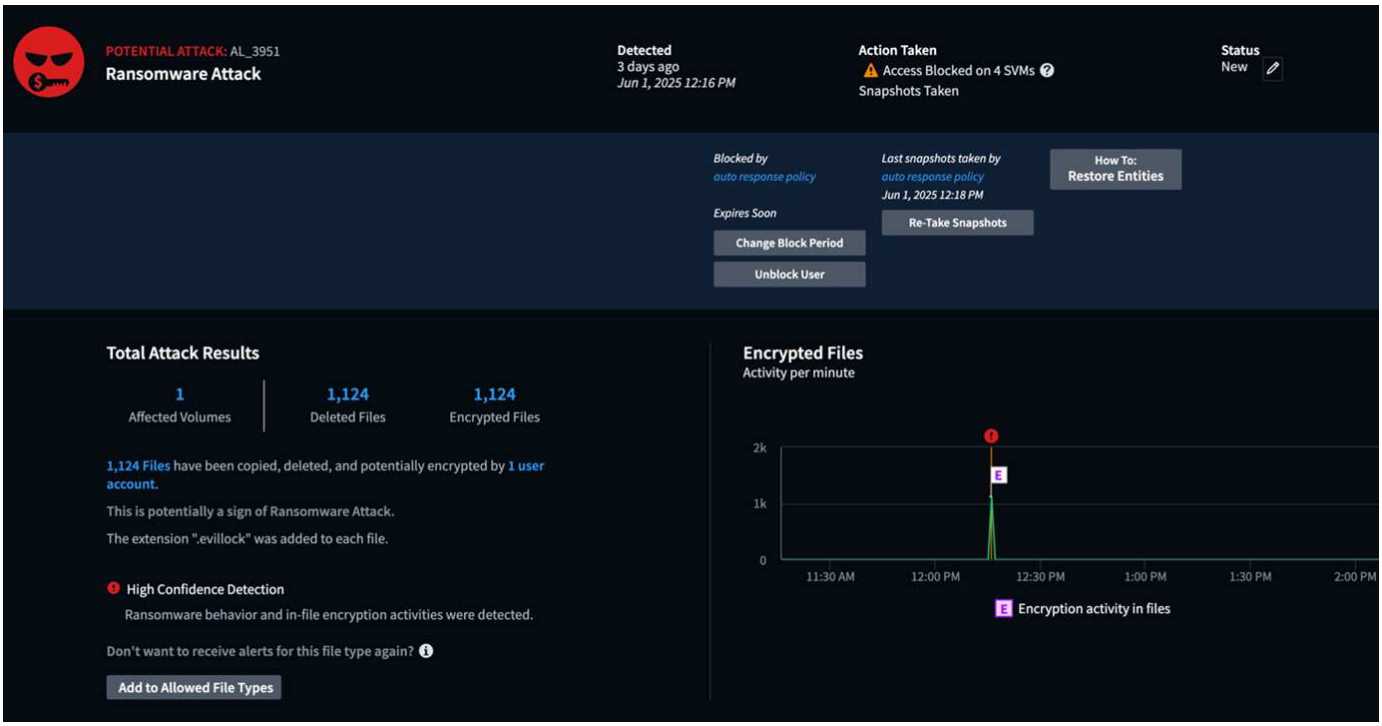
Workload Security erkennt Ransomware-Muster basierend auf dem Benutzerverhalten, während ONTAP ARP Ransomware-Aktivitäten basierend auf Verschlüsselungsaktivitäten in Dateien erkennt.

Wenn die Bedingungen erfüllt sind, kennzeichnet Workload Security die Warnungen als Warnungen mit hoher Zuverlässigkeit.

Beispiel für eine Warnung mit hoher Zuverlässigkeit auf der Seite mit der Warnungsliste:



Beispiel für Details einer Warnung mit hoher Zuverlässigkeit:



Alarm wird mehrmals ausgelöst

Workload Security lernt das Benutzerverhalten und generiert keine Warnungen bei wiederholten Ransomware-Angriffen innerhalb von 24 Stunden für denselben Benutzer.

Um einen neuen Alarm mit einem anderen Benutzer zu generieren, führen Sie bitte dieselben Schritte erneut aus (Erstellen von Testdaten und anschließendes Verschlüsseln der Testdaten).

Konfigurieren von E-Mail-Benachrichtigungen für Alarme, Warnungen und den Zustand von Agenten/Datenquellen-Sammlern

Um die Empfänger von Workload Security-Warnmeldungen zu konfigurieren, klicken Sie auf **Admin > Benachrichtigungen** und geben Sie in den entsprechenden Abschnitten für jeden Empfänger eine E-Mail-Adresse ein.

Alarme und Warnungen vor potenziellen Angriffen

Um Warnmeldungen zu *potenziellen Angriffen* zu senden, geben Sie die E-Mail-Adressen der Empfänger im Abschnitt *Warnmeldungen zu potenziellen Angriffen senden* ein. Für jede Aktion im Zusammenhang mit der Warnung werden E-Mail-Benachrichtigungen an die Empfängerliste der Warnung gesendet.

Um *Warnbenachrichtigungen* zu senden, geben Sie die E-Mail-Adressen der Empfänger im Abschnitt *Warnmeldungen senden* ein.

Integritätsüberwachung für Agenten und Datensammler

Sie können den Zustand von Agenten und Datenquellen durch Benachrichtigungen überwachen.

Um Benachrichtigungen zu erhalten, falls ein Agent oder Datenquellensammler nicht funktioniert, geben Sie

die E-Mail-Adressen der Empfänger im Abschnitt „Warnungen zum Zustand der Datensammlung“ ein.

Beachten Sie Folgendes:

- Gesundheitswarnungen werden erst gesendet, wenn der Agent/Sammler mindestens eine Stunde lang keine Berichte mehr sendet.
- Innerhalb eines Zeitraums von 24 Stunden wird nur eine E-Mail-Benachrichtigung an die vorgesehenen Empfänger gesendet, selbst wenn die Verbindung zum Agenten oder Datensammler für einen längeren Zeitraum unterbrochen ist.
- Im Falle eines Agentenfehlers wird eine Warnung gesendet (nicht eine pro Collector). Die E-Mail enthält eine Liste aller betroffenen SVMs.
- Ein Fehler bei der Active Directory-Sammlung wird als Warnung gemeldet und hat keinen Einfluss auf die Ransomware-Erkennung.
- Die Setup-Liste „Erste Schritte“ enthält jetzt eine neue Phase „E-Mail-Benachrichtigungen konfigurieren“.

Empfangen von Agent- und Data Collector-Upgrade-Benachrichtigungen

- Geben Sie die E-Mail-ID(s) in den „Health Alerts zur Datenerfassung“ ein.
- Das Kontrollkästchen „Upgrade-Benachrichtigungen aktivieren“ wird aktiviert.
- E-Mail-Benachrichtigungen zu Agent- und Data Collector-Upgrades werden einen Tag vor dem geplanten Upgrade an die E-Mail-IDs gesendet.

Fehlerbehebung

Problem:	Versuchen Sie Folgendes:
In den „Data Collector Health Alerts“ sind E-Mail-IDs vorhanden, ich erhalte jedoch keine Benachrichtigungen.	Benachrichtigungs-E-Mails werden von der NetApp Data Infrastructure Insights Domäne gesendet, d. h. von *accounts@service.cloudinsights.netapp.com*. Einige Unternehmen blockieren eingehende E-Mails, wenn diese von einer externen Domäne stammen. Stellen Sie sicher, dass externe Benachrichtigungen von NetApp Data Infrastructure Insights -Domänen auf die Whitelist gesetzt werden.

Webhook-Benachrichtigungen

Workload-Sicherheitsbenachrichtigungen mithilfe von Webhooks

Mithilfe von Webhooks können Benutzer über einen benutzerdefinierten Webhook-Kanal kritische Warnmeldungen oder Warnmeldungen an verschiedene Anwendungen senden.

Viele kommerzielle Anwendungen unterstützen Webhooks als Standardeingabeschnittstelle, zum Beispiel: Slack, PagerDuty, Teams und Discord. Durch die Unterstützung eines generischen, anpassbaren Webhook-Kanals kann Workload Security viele dieser Bereitstellungskanäle unterstützen. Informationen zur Konfiguration der Webhooks finden Sie auf den Webseiten der jeweiligen Anwendungen. Slack bietet beispielsweise"dieser nützliche Leitfaden" .

Sie können mehrere Webhook-Kanäle erstellen, wobei jeder Kanal einem anderen Zweck, separaten Anwendungen, verschiedenen Empfängern usw. dient.

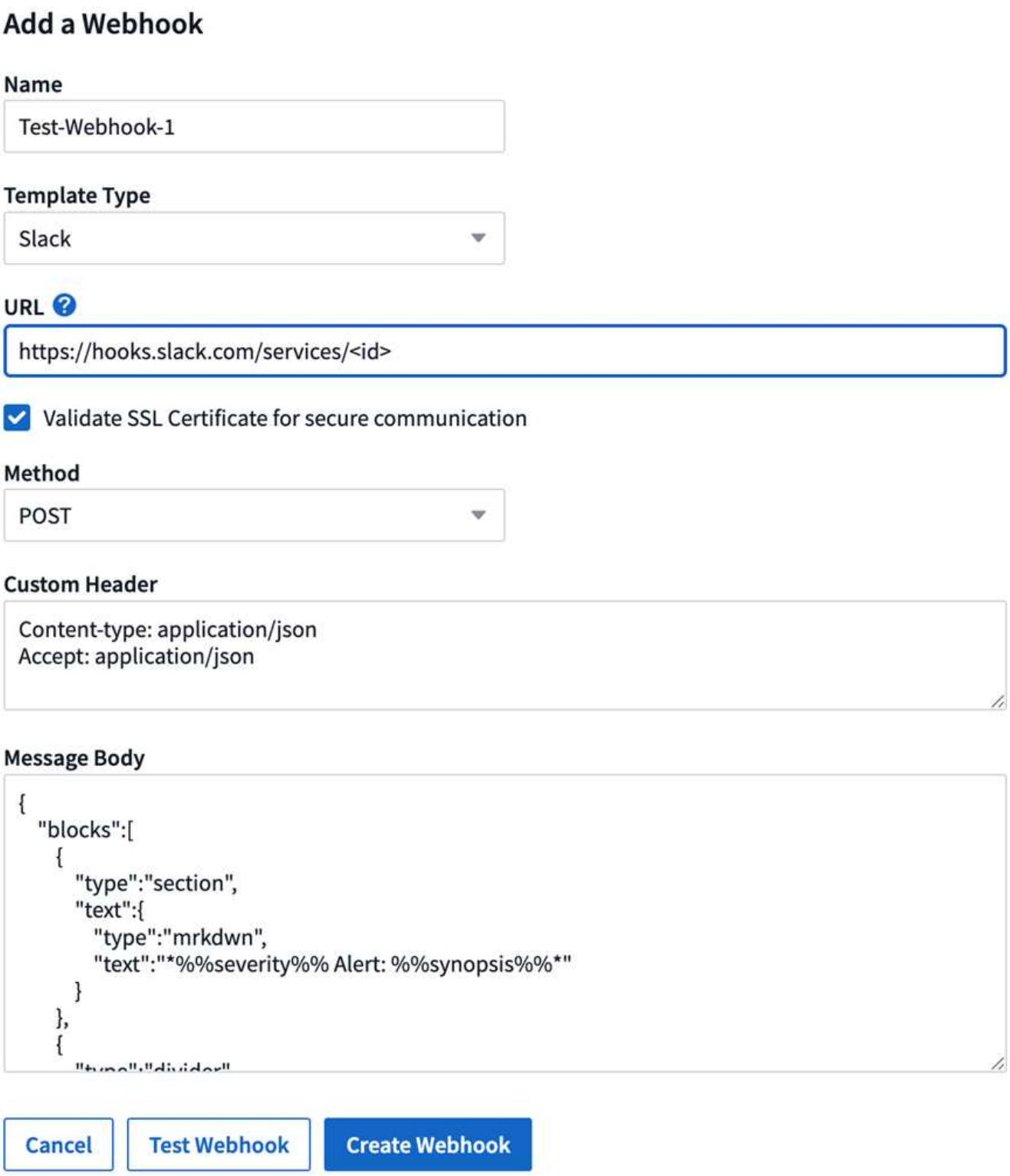
Die Webhook-Kanalinstanz besteht aus den folgenden Elementen

Name	Beschreibung
URL	Webhook-Ziel-URL, einschließlich des Präfixes http:// oder https:// zusammen mit den URL-Parametern
Verfahren	GET/POST – Standard ist POST
Benutzerdefinierter Header	Geben Sie hier alle benutzerdefinierten Header an
Nachrichtentext	Geben Sie hier den Text Ihrer Nachricht ein
Standard-Alarmparameter	Listet die Standardparameter für den Webhook auf
Benutzerdefinierte Parameter und Geheimnisse	Benutzerdefinierte Parameter und Geheimnisse ermöglichen Ihnen das Hinzufügen einzigartiger Parameter und sicherer Elemente wie Passwörter

Erstellen eines Webhooks

Um einen Workload Security Webhook zu erstellen, gehen Sie zu Admin > Benachrichtigungen und wählen Sie die Registerkarte „Workload Security Webhooks“. Das folgende Bild zeigt einen Beispielbildschirm zum Erstellen eines Slack-Webhooks.

Hinweis: Der Benutzer muss ein Workload Security-Administrator sein, um Workload Security-Webhooks erstellen und verwalten zu können.



- Geben Sie in jedes Feld die entsprechenden Informationen ein und klicken Sie auf „Speichern“.
- Sie können auch auf die Schaltfläche „Webhook testen“ klicken, um die Verbindung zu testen. Beachten Sie, dass dadurch der „Nachrichtentext“ (ohne Ersetzungen) gemäß der ausgewählten Methode an die definierte URL gesendet wird.
- SWS-Webhooks umfassen eine Reihe von Standardparametern. Darüber hinaus können Sie Ihre eigenen benutzerdefinierten Parameter oder Geheimnisse erstellen.

Parameter: Was sind sie und wie werden sie verwendet?

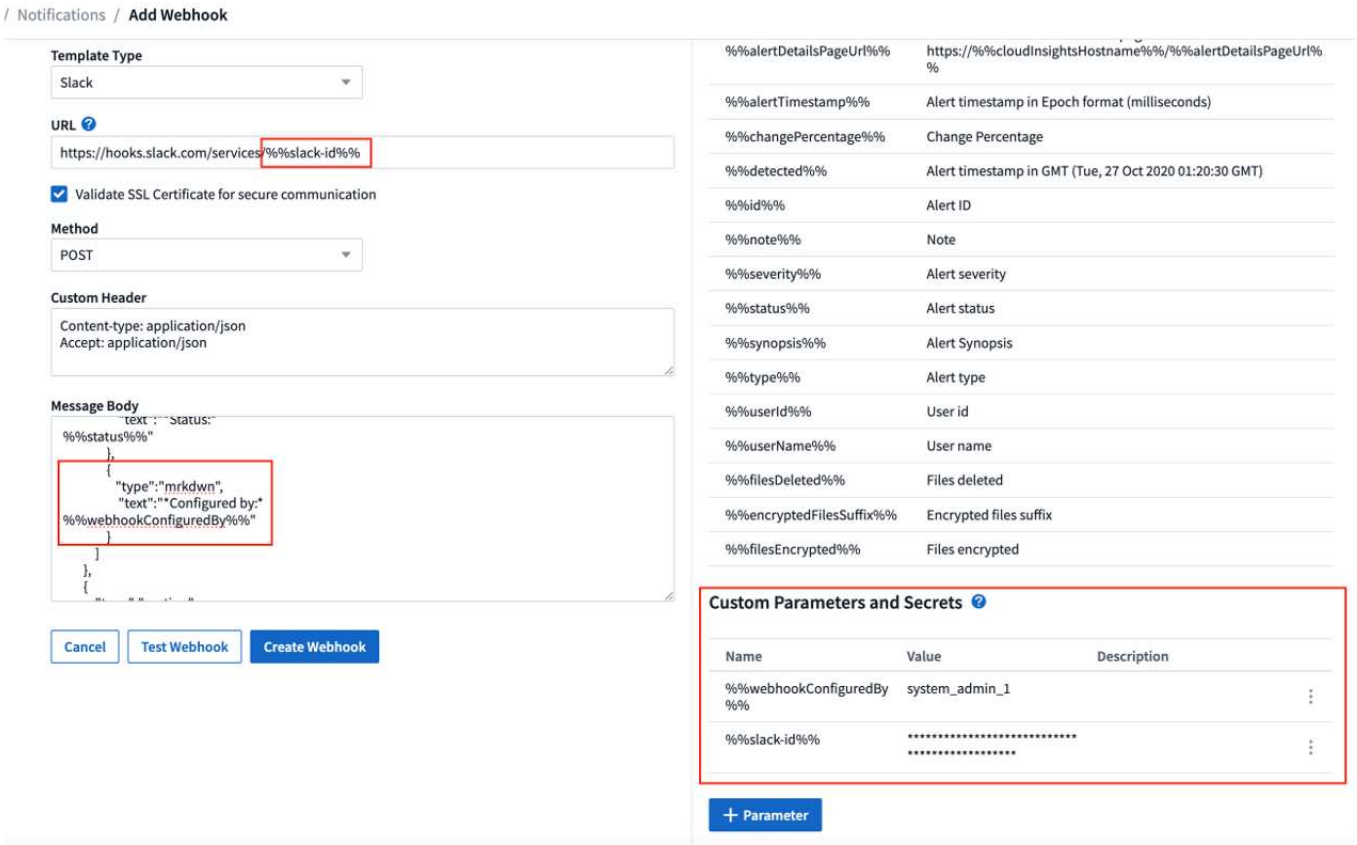
Alarmparameter sind dynamische Werte, die pro Alarm ausgefüllt werden. Beispielsweise wird der Parameter *%%severity%%* durch den Schweregradtyp der Warnung ersetzt.

Beachten Sie, dass beim Klicken auf die Schaltfläche „Webhook testen“ keine Ersetzungen durchgeführt werden. Der Test sendet eine Nutzlast, die die Platzhalter des Parameters (*%%<param-name>%%*) anzeigt, diese jedoch nicht durch Daten ersetzt.

Benutzerdefinierte Parameter und Geheimnisse

In diesem Abschnitt können Sie beliebige benutzerdefinierte Parameter und/oder Geheimnisse hinzufügen. Ein benutzerdefinierter Parameter oder ein Geheimnis kann in der URL oder im Nachrichtentext enthalten sein. Mithilfe von Geheimnissen können Benutzer sichere benutzerdefinierte Parameter wie Kennwort, API-Schlüssel usw. konfigurieren.

Das folgende Beispielbild zeigt, wie benutzerdefinierte Parameter bei der Webhook-Erstellung verwendet werden.



Seite „Workload Security Webhooks – Liste“

Auf der Webhook-Listenseite werden die Felder „Name“, „Erstellt von“, „Erstellt am“, „Status“, „Sicher“ und „Zuletzt gemeldet“ angezeigt. Hinweis: Der Wert der Spalte „Status“ ändert sich ständig basierend auf dem Ergebnis des letzten Webhook-Triggers. Nachfolgend finden Sie Beispiele für Statusergebnisse.

Status	Beschreibung
OK	Benachrichtigung erfolgreich gesendet.

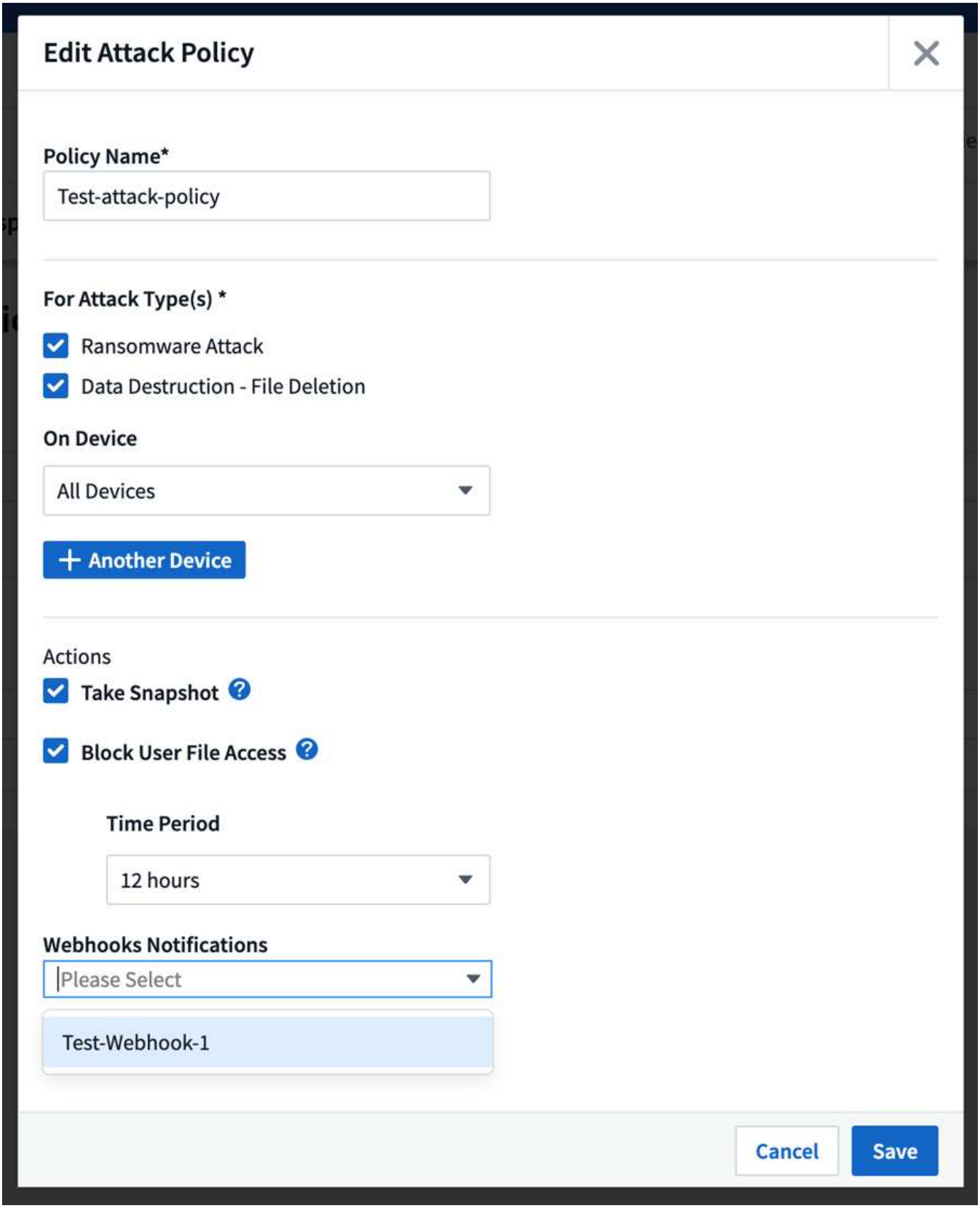
403	Verboten.
404	URL nicht gefunden.
400	Ungültige Anforderung. Dieser Status wird möglicherweise angezeigt, wenn im Nachrichtentext ein Fehler vorliegt, beispielsweise: • Schlecht formatiertes JSON. • Bereitstellung eines ungültigen Werts für reservierte Schlüssel. Beispielsweise akzeptiert PagerDuty für „Schweregrad“ nur „kritisch“/„Warnung“/„Fehler“/„Info“. Jedes andere Ergebnis kann zu einem 400-Status führen. • Anwendungsspezifische Validierungsfehler. Beispielsweise erlaubt Slack maximal 10 Felder innerhalb eines Abschnitts. Wenn Sie mehr als 10 angeben, kann dies zu einem 400-Status führen.
410	Ressource ist nicht mehr verfügbar

Die Spalte „Zuletzt gemeldet“ gibt den Zeitpunkt an, zu dem der Webhook zuletzt ausgelöst wurde.

Auf der Webhook-Listenseite können Benutzer Webhooks auch bearbeiten/duplizieren/löschen.

Konfigurieren der Webhook-Benachrichtigung in der Warnrichtlinie

Um einer Warnrichtlinie eine Webhook-Benachrichtigung hinzuzufügen, gehen Sie zu -Workload-Sicherheit > Richtlinien- und wählen Sie eine vorhandene Richtlinie aus oder fügen Sie eine neue Richtlinie hinzu. Wählen Sie im Abschnitt „Aktionen“ > Dropdown-Menü „Webhook-Benachrichtigungen“ die erforderlichen Webhooks aus.



Webhook-Benachrichtigungen sind an Richtlinien gebunden. Wenn der Angriff (RW/DD/WARN) stattfindet, wird die konfigurierte Aktion (Snapshot erstellen/Benutzer blockieren) ausgeführt und anschließend die zugehörige Webhook-Benachrichtigung ausgelöst.

Hinweis: E-Mail-Benachrichtigungen sind unabhängig von Richtlinien und werden wie gewohnt ausgelöst.

- Wenn eine Richtlinie angehalten wird, werden keine Webhook-Benachrichtigungen ausgelöst.
- An eine einzelne Richtlinie können mehrere Webhooks angehängt werden. Es wird jedoch empfohlen, nicht mehr als 5 Webhooks an eine Richtlinie anzuhängen.

Beispiele für Workload-Sicherheits-Webhooks

Webhooks für"Locker"

Webhooks für"PagerDuty" Webhooks für"Teams" Webhooks für"Zwietracht"

Workload Security Webhook-Beispiel für Discord

Mithilfe von Webhooks können Benutzer über einen benutzerdefinierten Webhook-Kanal Warnbenachrichtigungen an verschiedene Anwendungen senden. Diese Seite bietet ein Beispiel zum Einrichten von Webhooks für Discord.

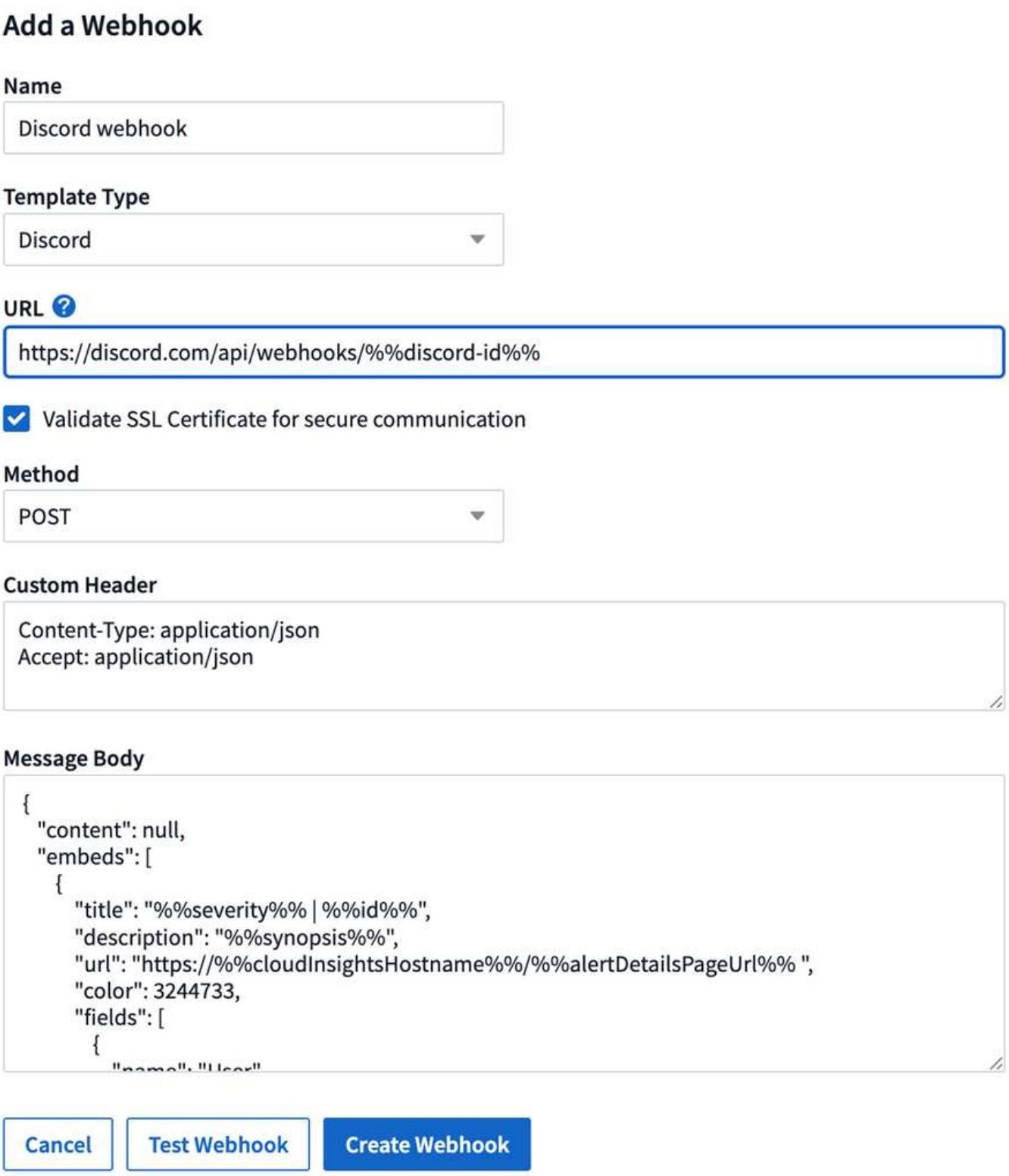
Diese Seite verweist auf Anweisungen von Drittanbietern, die Änderungen unterliegen. Weitere Informationen finden Sie im"Discord-Dokumentation" für die aktuellsten Informationen.

Discord-Setup:

- Wählen Sie in Discord den Server aus und wählen Sie unter „Textkanäle“ die Option „Kanal bearbeiten“ (Zahnradsymbol).
- Wählen Sie **Integrationen > Webhooks anzeigen** und klicken Sie auf **Neuer Webhook**
- Kopieren Sie die Webhook-URL. Sie müssen dies in die Workload Security-Webhook-Konfiguration einfügen.

Erstellen Sie einen Workload-Sicherheits-Webhook:

1. Navigieren Sie zu „Admin > Benachrichtigungen“ und wählen Sie die Registerkarte „Workload Security Webhooks“ aus. Klicken Sie auf „+ Webhook“, um einen neuen Webhook zu erstellen.
2. Geben Sie dem Webhook einen aussagekräftigen Namen.
3. Wählen Sie im Dropdown-Menü „Vorlagentyp“ **Discord** aus.
4. Fügen Sie die Discord-URL von oben in das Feld *URL* ein.



Um den Webhook zu testen, ersetzen Sie den URL-Wert im Nachrichtentext vorübergehend durch eine beliebige gültige URL (z. B. *https://netapp.com*) und klicken Sie dann auf die Schaltfläche *Webhook testen*. Discord erfordert die Angabe einer gültigen URL, damit die Test-Webhook-Funktionalität funktioniert.

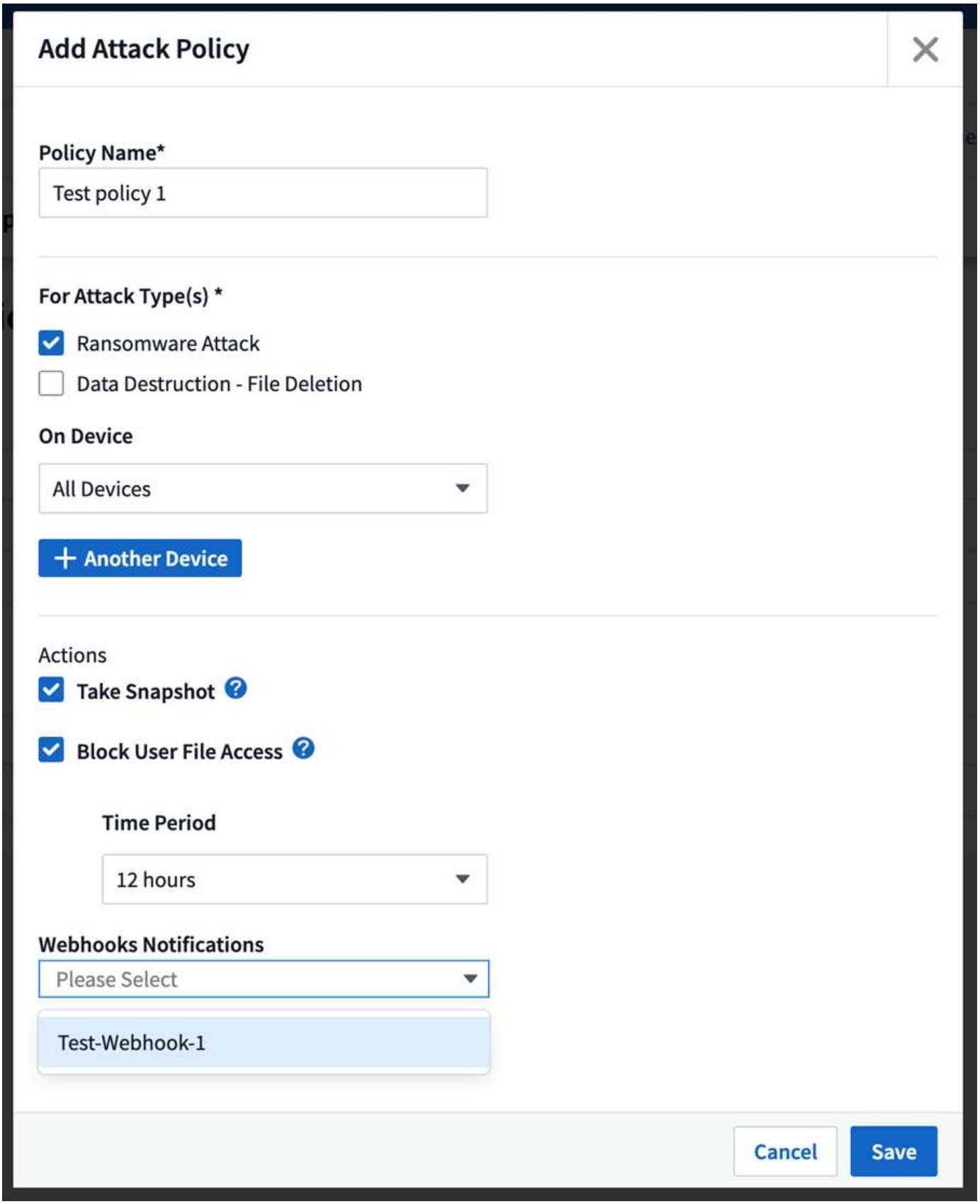
Denken Sie daran, den Nachrichtentext nach Abschluss des Tests wiederherzustellen.

Benachrichtigungen per Webhook

Um über Ereignisse per Webhook benachrichtigt zu werden, navigieren Sie zu *Workload-Sicherheit > Richtlinien*. Klicken Sie auf *+Angriffsrichtlinie* oder *+Warnrichtlinie*.

- Geben Sie einen aussagekräftigen Richtliniennamen ein.
- Wählen Sie die erforderlichen Angriffstypen, Geräte, denen die Richtlinie zugeordnet werden soll, und erforderliche Aktionen aus.
- Wählen Sie im Dropdown-Menü „Webhook-Benachrichtigungen“ die gewünschten Discord-Webhooks aus und speichern Sie.

Hinweis: Webhooks können auch an vorhandene Richtlinien angehängt werden, indem diese bearbeitet werden.



Workload Security Webhook-Beispiel für PagerDuty

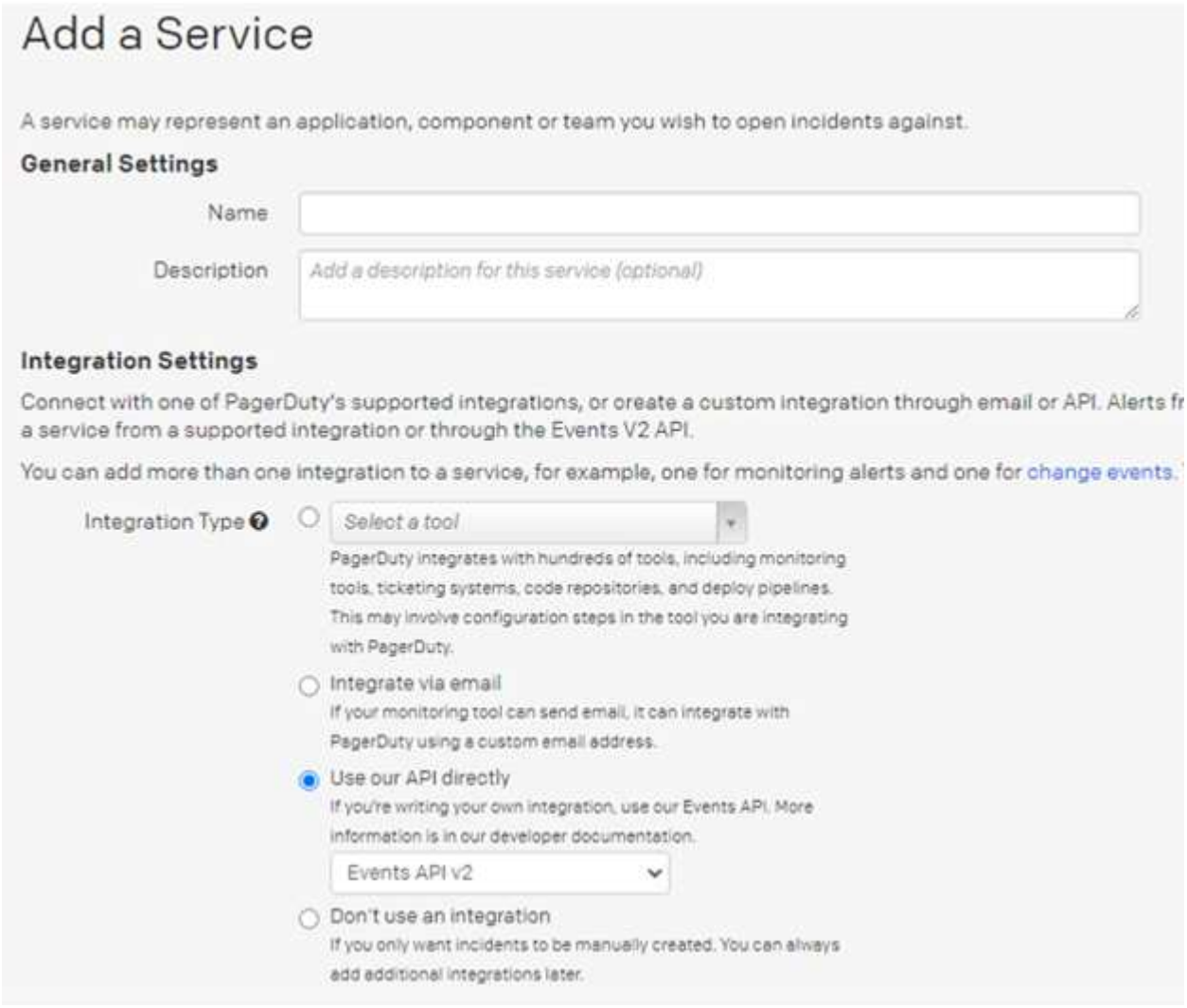
Mithilfe von Webhooks können Benutzer über einen benutzerdefinierten Webhook-Kanal Warnbenachrichtigungen an verschiedene Anwendungen senden. Diese Seite bietet ein

Beispiel zum Einrichten von Webhooks für PagerDuty.

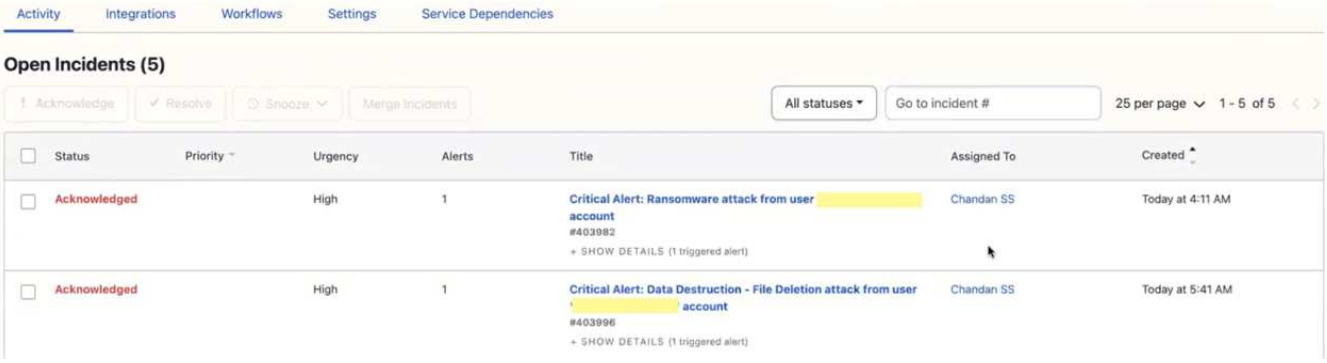
Diese Seite verweist auf Anweisungen von Drittanbietern, die Änderungen unterliegen. Weitere Informationen finden Sie im"PagerDuty-Dokumentation" für die aktuellsten Informationen.

PagerDuty-Setup:

1. Navigieren Sie in PagerDuty zu **Dienste > Dienstverzeichnis** und klicken Sie auf die Schaltfläche **+Neuer Dienst**.
2. Geben Sie einen *Namen* ein und wählen Sie *Unsere API direkt verwenden*. Wählen Sie *Dienst hinzufügen*.

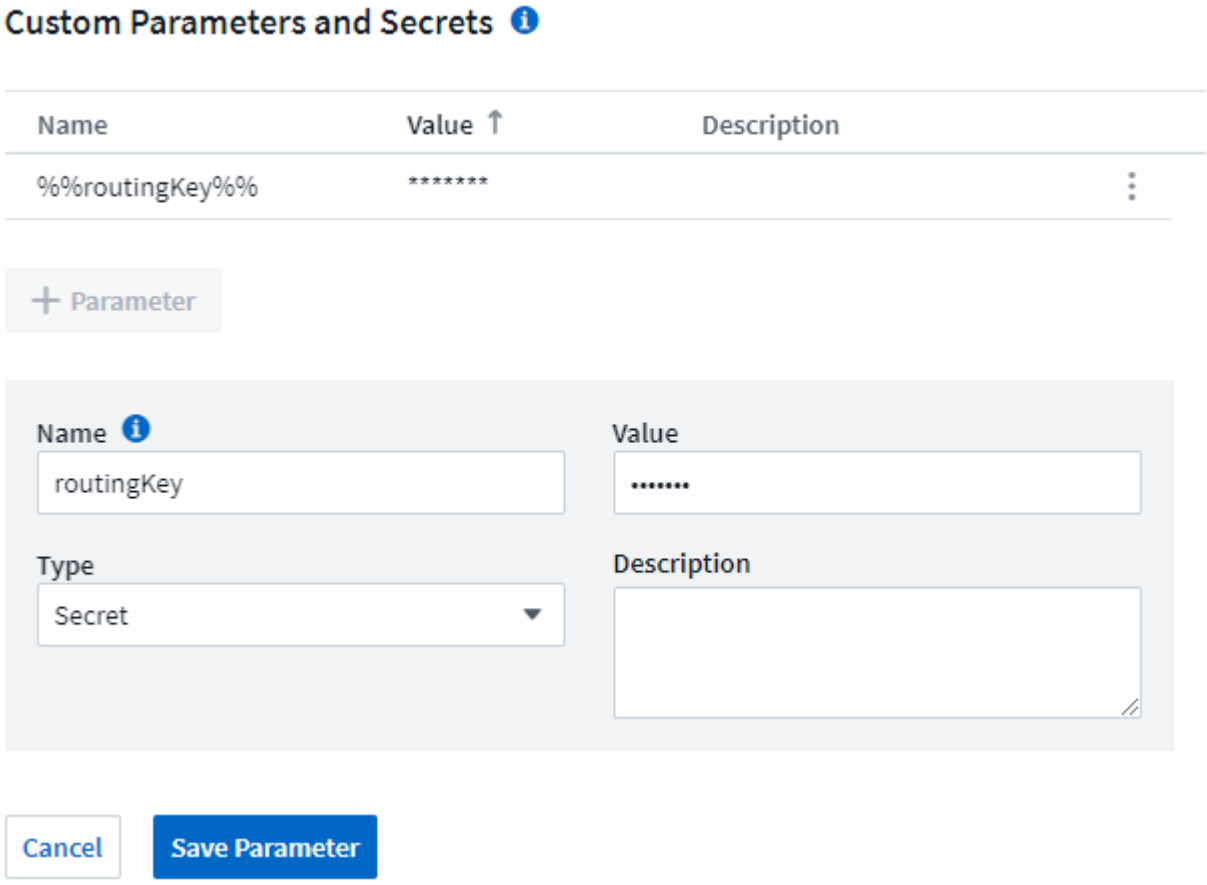


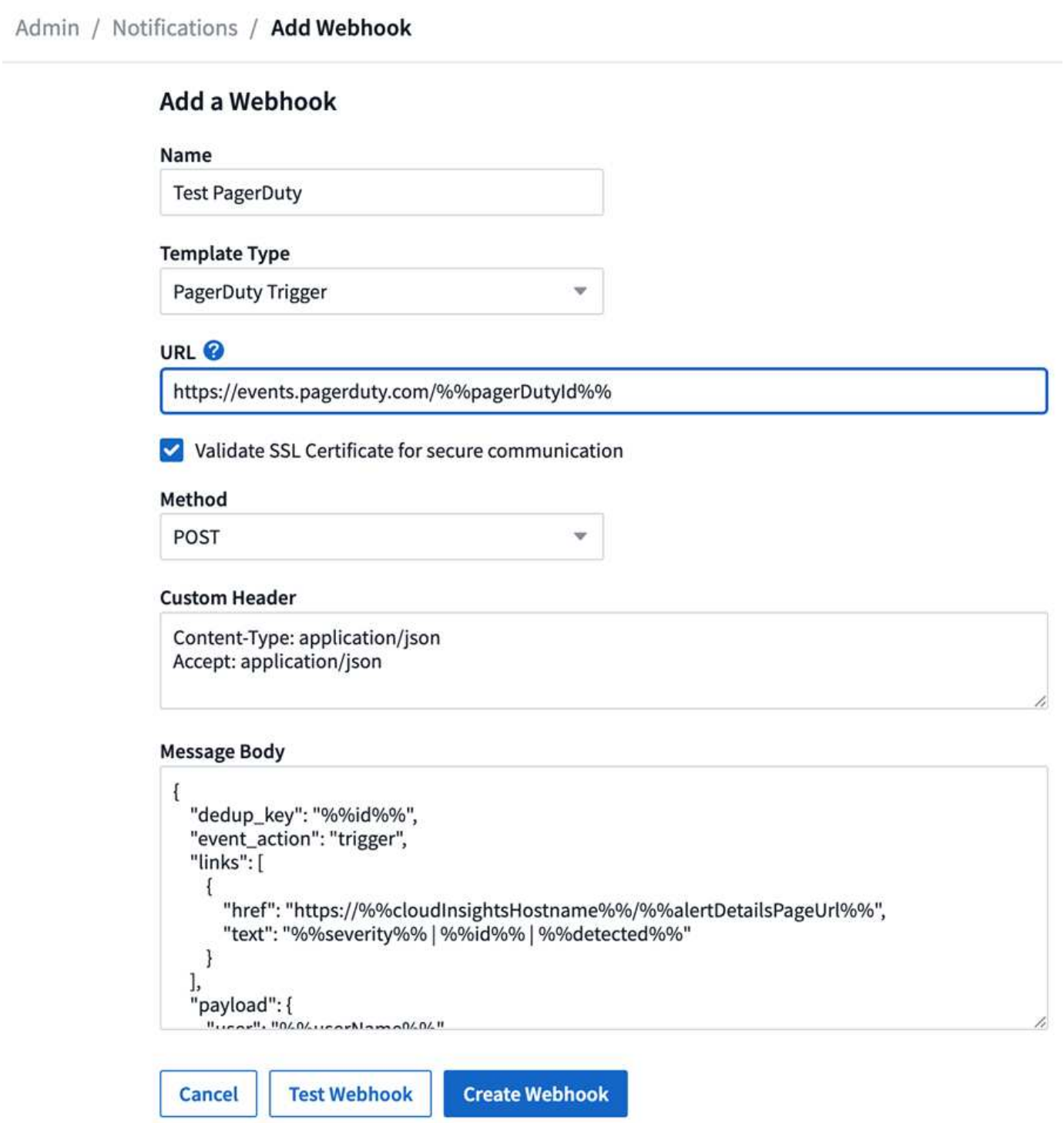
3. Wählen Sie die Registerkarte *Integrationen*, um den **Integrationsschlüssel** anzuzeigen. Sie benötigen diesen Schlüssel, wenn Sie unten den Workload Security-Webhook erstellen.
4. Gehen Sie zu **Vorfälle** oder **Dienste**, um Warnungen anzuzeigen.



Erstellen Sie einen Workload Security PagerDuty-Webhook:

- Navigieren Sie zu „Admin > Benachrichtigungen“ und wählen Sie die Registerkarte „Workload Security Webhooks“ aus. Wählen Sie „+ Webhook“, um einen neuen Webhook zu erstellen.
- Geben Sie dem Webhook einen aussagekräftigen Namen.
- Wählen Sie im Dropdown-Menü *Vorlagentyp* die Option *PagerDuty-Trigger* aus.
- Erstellen Sie ein benutzerdefiniertes Parametergeheimnis mit dem Namen *routingKey* und legen Sie den Wert auf den oben erstellten PagerDuty-*Integrationsschlüssel* fest.

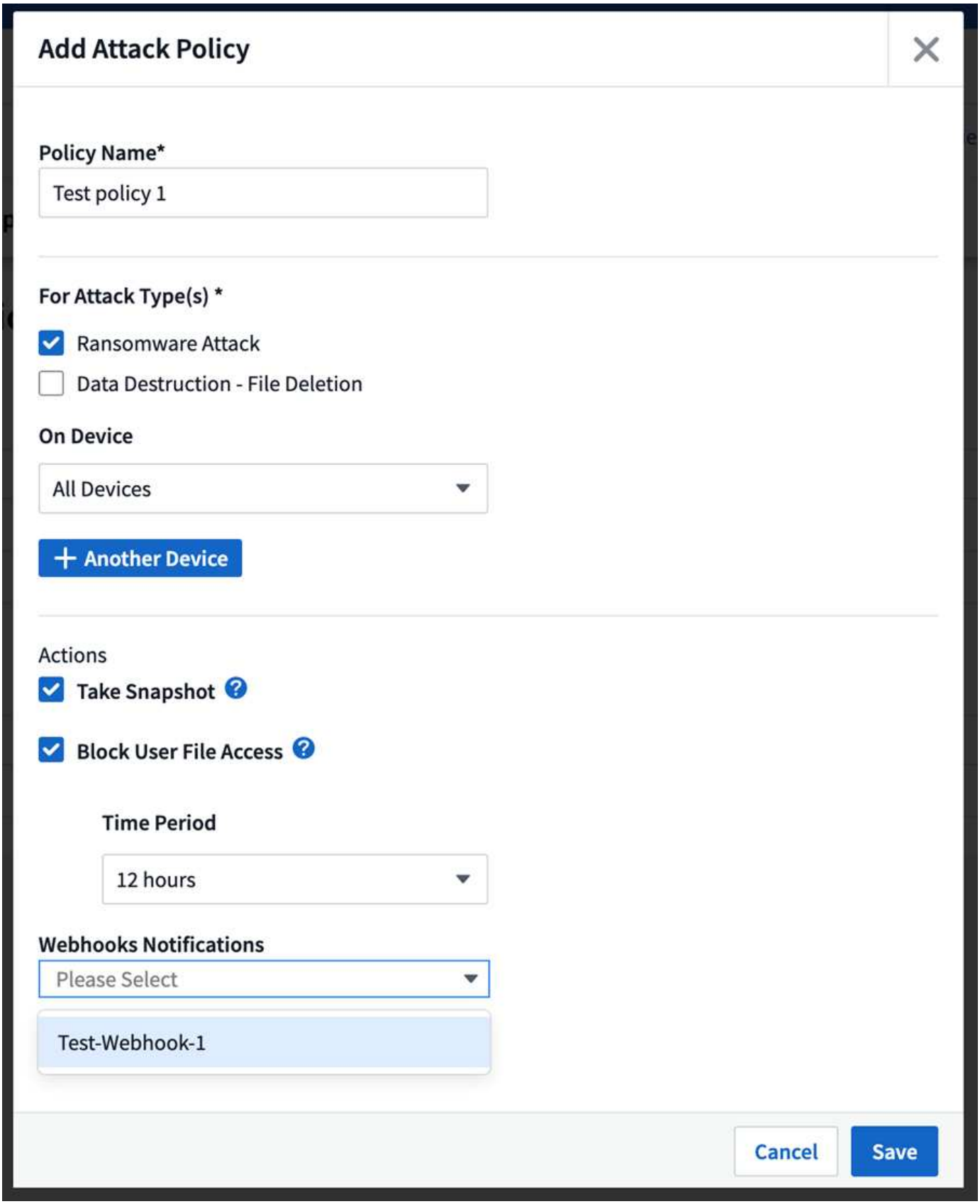




Benachrichtigungen per Webhook

- Um über Ereignisse per Webhook benachrichtigt zu werden, navigieren Sie zu *Workload-Sicherheit > Richtlinien*. Wählen Sie *+Angriffsrichtlinie* oder *+Warnrichtlinie*.
- Geben Sie einen aussagekräftigen Richtliniennamen ein.
- Wählen Sie die erforderlichen Angriffstypen, Geräte, an die die Richtlinie angehängt werden soll, und die erforderlichen Aktionen aus.
- Wählen Sie im Dropdown-Menü „Webhook-Benachrichtigungen“ die erforderlichen PagerDuty-Webhooks aus. Speichern Sie die Richtlinie.

Hinweis: Webhooks können auch an vorhandene Richtlinien angehängt werden, indem diese bearbeitet werden.



Workload Security Webhook-Beispiel für Slack

Mithilfe von Webhooks können Benutzer über einen benutzerdefinierten Webhook-Kanal Warnbenachrichtigungen an verschiedene Anwendungen senden. Diese Seite bietet ein Beispiel zum Einrichten von Webhooks für Slack.

Diese Seite verweist auf Anweisungen von Drittanbietern, die Änderungen unterliegen. Die aktuellsten Informationen finden Sie in der Slack-Dokumentation.

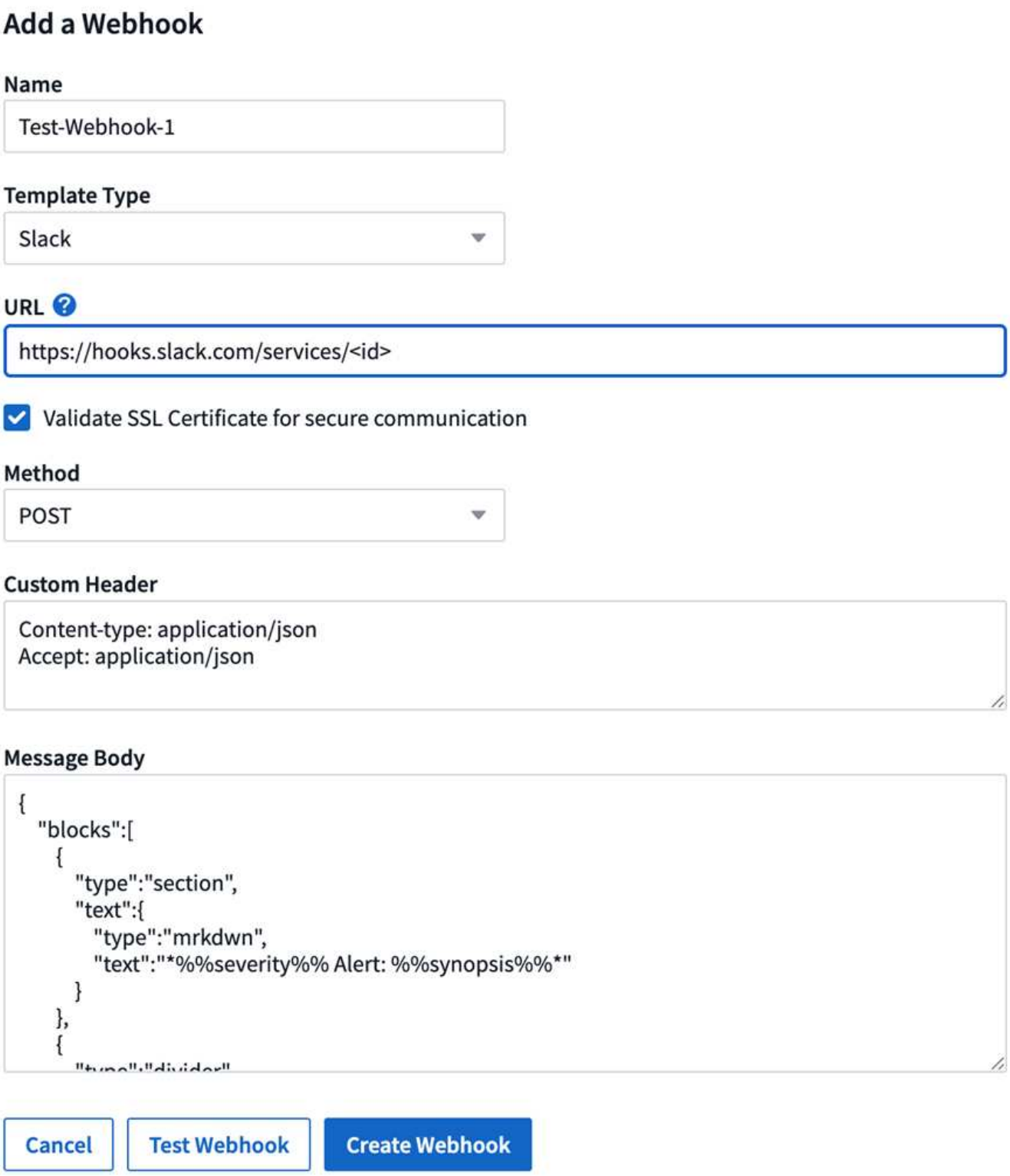
Slack-Beispiel

- Gehe zu https://api.slack.com/apps und erstellen Sie eine neue App. Geben Sie ihm einen aussagekräftigen Namen und wählen Sie einen Arbeitsbereich aus.

- Gehen Sie zu „Eingehende Webhooks“, klicken Sie auf „Eingehende Webhooks aktivieren“, wählen Sie „Neuen Webhook hinzufügen“ und wählen Sie den Kanal aus, auf dem gepostet werden soll.
- Kopieren Sie die Webhook-URL. Diese URL wird beim Erstellen eines Workload Security-Webhooks angegeben.

Erstellen Sie einen Slack-Webhook für die Workload-Sicherheit

1. Navigieren Sie zu „Admin > Benachrichtigungen“ und wählen Sie die Registerkarte „Workload Security Webhooks“ aus. Wählen Sie + *Webhook*, um einen neuen Webhook zu erstellen.
2. Geben Sie dem Webhook einen aussagekräftigen Namen.
3. Wählen Sie im Dropdown-Menü *Vorlagentyp* die Option *Slack* aus.
4. Fügen Sie die oben kopierte URL ein.

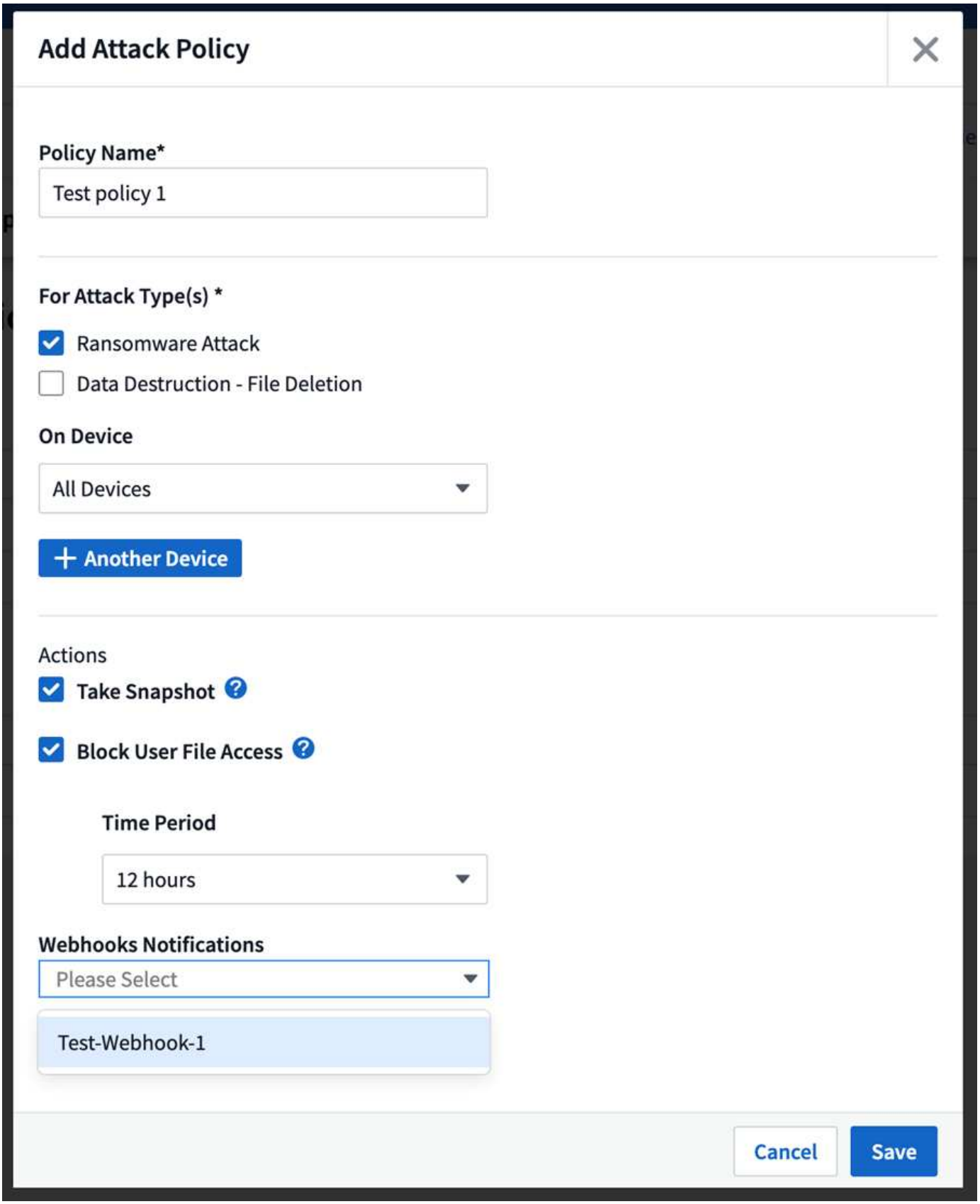


Benachrichtigungen per Webhook

- Um über Ereignisse per Webhook benachrichtigt zu werden, navigieren Sie zu *Workload-Sicherheit > Richtlinien*. Klicken Sie auf *+Angriffsrichtlinie* oder *+Warnrichtlinie*.
- Geben Sie einen aussagekräftigen Richtliniennamen ein.
- Wählen Sie die erforderlichen Angriffstypen, Geräte, an die die Richtlinie angehängt werden soll, und erforderliche Aktionen aus.

- Wählen Sie im Dropdown-Menü „Webhook-Benachrichtigungen“ die erforderlichen Webhooks aus. Speichern Sie die Richtlinie.

Hinweis: Webhooks können auch an vorhandene Richtlinien angehängt werden, indem diese bearbeitet werden.



Beispiel für einen Workload-Sicherheits-Webhook für Microsoft Teams

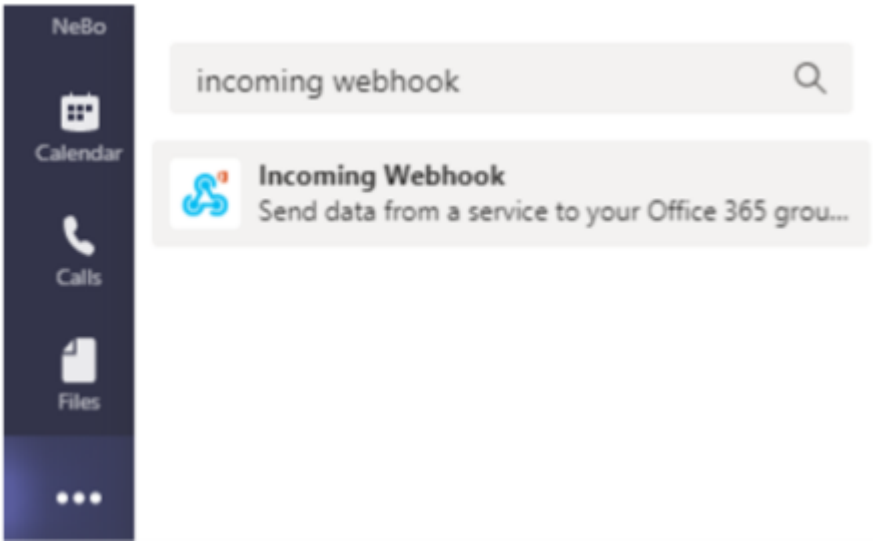
Mithilfe von Webhooks können Benutzer über einen benutzerdefinierten Webhook-Kanal Warnbenachrichtigungen an verschiedene Anwendungen senden. Diese Seite bietet ein

Beispiel zum Einrichten von Webhooks für Teams.

Diese Seite verweist auf Anweisungen von Drittanbietern, die Änderungen unterliegen. Weitere Informationen finden Sie im"Teams-Dokumentation" für die aktuellsten Informationen.

Teams-Setup:

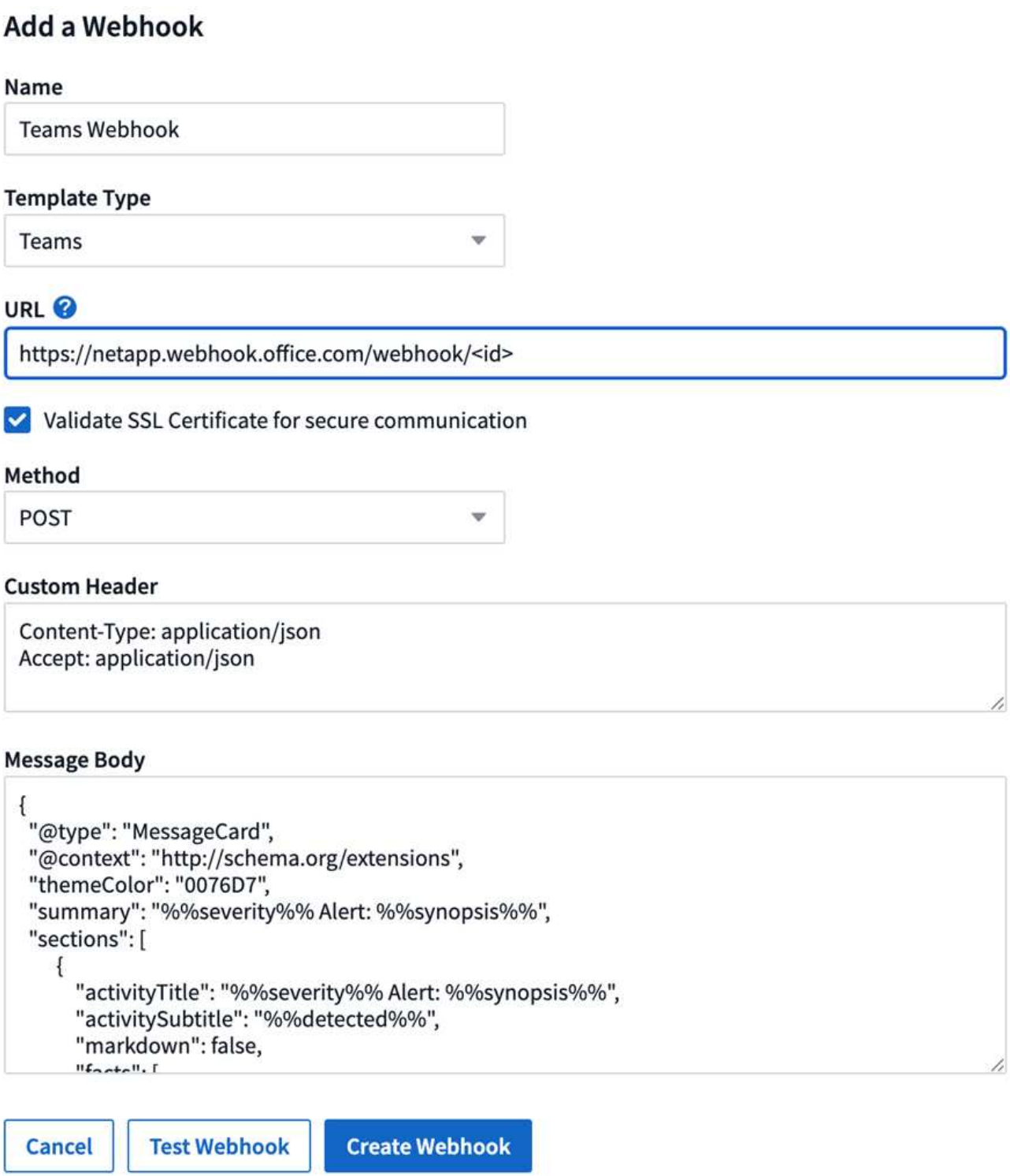
1. Wählen Sie in Teams den Kebab aus und suchen Sie nach „Eingehender Webhook“.



2. Wählen Sie **Zu einem Team hinzufügen > Ein Team auswählen > Einen Connector einrichten**.
3. Kopieren Sie die Webhook-URL. Sie müssen dies in die Workload Security-Webhook-Konfiguration einfügen.

Erstellen Sie einen Workload Security Teams-Webhook:

1. Navigieren Sie zu „Admin > Benachrichtigungen“ und wählen Sie die Registerkarte „Workload Security Webhooks“ aus. Wählen Sie + *Webhook*, um einen neuen Webhook zu erstellen.
2. Geben Sie dem Webhook einen aussagekräftigen Namen.
3. Wählen Sie im Dropdown-Menü „Vorlagentyp“ die Option „Teams“ aus.



4. Fügen Sie die URL von oben in das Feld *URL* ein.

Benachrichtigungen per Webhook

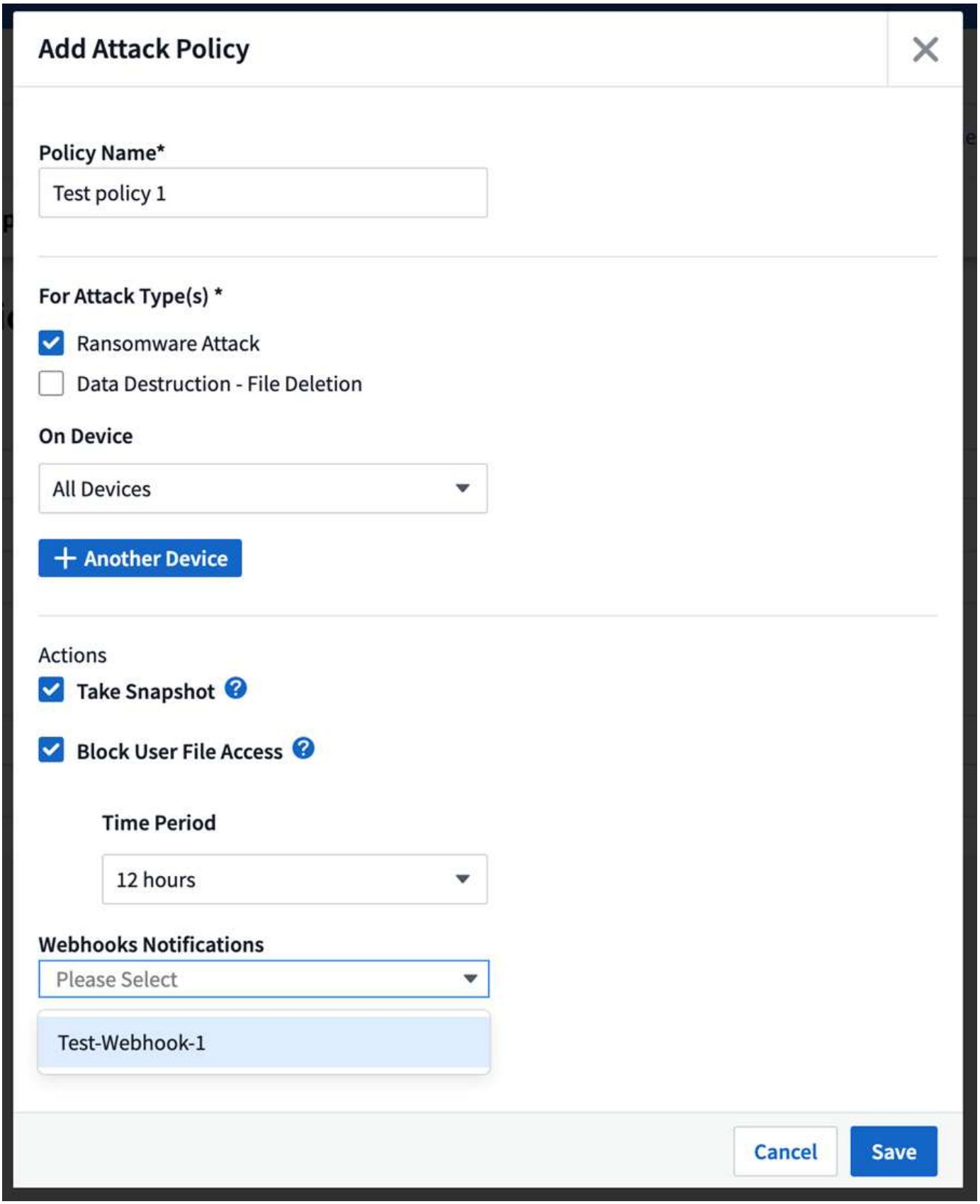
Um über Ereignisse per Webhook benachrichtigt zu werden, navigieren Sie zu *Workload-Sicherheit* > *Richtlinien*. Wählen Sie *+Angriffsrichtlinie* oder *+Warnrichtlinie*.

- Geben Sie einen aussagekräftigen Richtliniennamen ein.
- Wählen Sie die erforderlichen Angriffstypen, Geräte, an die die Richtlinie angehängt werden soll, und die

erforderlichen Aktionen aus.

- Wählen Sie im Dropdown-Menü „Webhook-Benachrichtigungen“ die erforderlichen Teams-Webhooks aus. Speichern Sie die Richtlinie.

Hinweis: Webhooks können auch an vorhandene Richtlinien angehängt werden, indem diese bearbeitet werden.



Workload-Sicherheits-API

Die Workload Security API ermöglicht es NetApp Kunden und unabhängigen

Softwareanbietern (ISVs), Workload Security in andere Anwendungen wie CMDBs oder andere Ticketsysteme zu integrieren.

Voraussetzungen für den API-Zugriff:

- Zum Gewähren des Zugriffs wird ein API-Zugriffstokenmodell verwendet.
- Die API-Token-Verwaltung wird von Workload Security-Benutzern mit der Administratorrolle durchgeführt.

API-Dokumentation (Swagger)

Die neuesten API-Informationen finden Sie, indem Sie sich bei Workload Security anmelden und zu **Admin > API-Zugriff** navigieren. Klicken Sie auf den Link **API-Dokumentation**. Die API-Dokumentation basiert auf Swagger und bietet eine kurze Beschreibung und Nutzungsinformationen für die API. Sie können sie auch auf Ihrem Mandanten ausprobieren.

Wenn Sie die Forensics Activity API aufrufen, verwenden Sie die API cloudsecure_forensics.activities.**v2**. Wenn Sie diese API mehrfach aufrufen, stellen Sie sicher, dass die Aufrufe nacheinander und nicht parallel erfolgen. Mehrere parallele Aufrufe können zu einem Timeout der API führen.

API-Zugriffstoken

Bevor Sie die Workload Security API verwenden, müssen Sie ein oder mehrere **API-Zugriffstoken** erstellen. Zugriffstoken gewähren Leseberechtigungen. Sie können auch das Ablaufdatum für jedes Zugriffstoken festlegen.

So erstellen Sie ein Zugriffstoken:

- Klicken Sie auf **Admin > API-Zugriff**
- Klicken Sie auf **+API-Zugriffstoken**
- Geben Sie **Token-Name** ein
- Geben Sie **Token-Ablauf** an

Ihr Token steht Ihnen während des Erstellungsprozesses nur zum Kopieren in die Zwischenablage und zum Speichern zur Verfügung. Token können nach ihrer Erstellung nicht abgerufen werden. Es wird daher dringend empfohlen, das Token zu kopieren und an einem sicheren Ort zu speichern. Sie werden aufgefordert, auf die Schaltfläche „API-Zugriffstoken kopieren“ zu klicken, bevor Sie den Bildschirm zur Token-Erstellung schließen können.

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

Token gewähren aus Kundensicht allgemeinen Zugriff auf APIs und verwalten den Zugriff auf APIs im Rahmen ihres eigenen Mandanten.

Die Anwendung erhält ein Zugriffstoken, nachdem ein Benutzer den Zugriff erfolgreich authentifiziert und autorisiert hat, und übergibt das Zugriffstoken dann als Anmeldeinformation, wenn sie die Ziel-API aufruft. Das übergebene Token informiert die API darüber, dass der Inhaber des Tokens autorisiert wurde, auf die API zuzugreifen und basierend auf dem bei der Autorisierung gewährten Umfang bestimmte Aktionen auszuführen.

Der HTTP-Header, an den das Zugriffstoken übergeben wird, lautet **X-CloudInsights-ApiKey:**

Verwenden Sie beispielsweise Folgendes, um Speicherressourcen abzurufen:

```
 curl https://<Workload Security tenant>/rest/v1/cloudsecure/activities -H
'X-CloudInsights-ApiKey: <API_Access_Token>'
Dabei ist _<API_Access_Token>_ das Token, das Sie während der Erstellung
des API-Zugriffsschlüssels gespeichert haben, und _<Workload Security
Tenant>_ die Tenant-URL Ihrer Workload Security-Umgebung.
```

Detaillierte Informationen finden Sie im Link *API-Dokumentation* unter **Admin > API-Zugriff**.

Skript zum Extrahieren von Daten über die API

Workload Security-Agenten enthalten ein Exportskript, um parallele Aufrufe der v2-API zu ermöglichen, indem der angeforderte Zeitbereich in kleinere Stapel aufgeteilt wird.

Das Skript befindet sich unter */opt/netapp/cloudsecure/agent/export-script*. Eine README-Datei im selben Verzeichnis enthält Verwendungsanweisungen.

Hier ist ein Beispielbefehl zum Aufrufen des Skripts:

```
python3 data-export.py --tenant_url <Workload Security tenant>
--access_key %ACCESS_KEY% --path_filter "<dir path>" --user_name "<user>"
--from_time "01-08-2024 00:00:00" --to_time "31-08-2024 23:59:59"
--iteration_interval 12 --num_workers 3
```

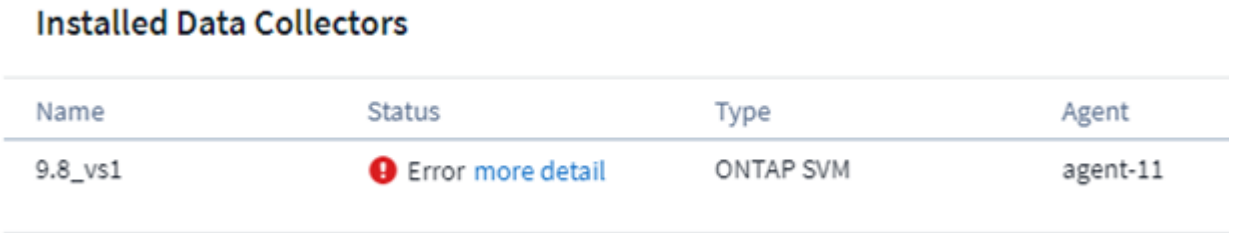
Schlüsselparameter: - `--iteration_interval 12` : Teilt den angeforderten Zeitbereich in Intervalle von 12 Stunden auf. - `--num_workers 3` : Ruft diese Intervalle parallel mithilfe von 3 Threads ab.

Fehlerbehebung beim ONTAP SVM Data Collector

Workload Security verwendet Datensammler, um Datei- und Benutzerzugriffsdaten von Geräten zu erfassen. Hier finden Sie Tipps zur Behebung von Problemen mit diesem Collector.

Siehe die"Konfigurieren des SVM-Collectors" Seite für Anweisungen zum Konfigurieren dieses Collectors.

Im Falle eines Fehlers können Sie auf der Seite „Installierte Datensammler“ in der Spalte „Status“ auf „Weitere Details“ klicken, um Einzelheiten zum Fehler anzuzeigen.



Bekannte Probleme und deren Lösungen werden unten beschrieben.

Problem: Der Datensammler läuft eine Zeit lang und stoppt nach einer zufälligen Zeit mit der Fehlermeldung: „Fehlermeldung: Connector befindet sich im Fehlerzustand.“ Dienstname: Audit. Grund für den Fehler: Externer fpolicy-Server überlastet."

Versuchen Sie Folgendes: Die Ereignisrate von ONTAP war viel höher als das, was die Agent-Box verarbeiten kann. Daher wurde die Verbindung beendet.

Überprüfen Sie den Spitzenverkehr in CloudSecure, als die Verbindung getrennt wurde. Dies können Sie auf der Seite **CloudSecure > Aktivitätsforensik > Alle Aktivitäten** überprüfen.

Wenn der aggregierte Spitzenverkehr höher ist als das, was die Agent Box verarbeiten kann, lesen Sie auf der Seite „Event Rate Checker“ nach, wie Sie die Größe für die Collector-Bereitstellung in einer Agent Box festlegen.

Wenn der Agent vor dem 4. März 2021 in der Agent-Box installiert wurde, führen Sie die folgenden Befehle in der Agent-Box aus:

```
echo 'net.core.rmem_max=8388608' >> /etc/sysctl.conf
echo 'net.ipv4.tcp_rmem = 4096 2097152 8388608' >> /etc/sysctl.conf
sysctl -p
```

Starten Sie den Collector nach der Größenänderung über die Benutzeroberfläche neu.

Problem: Der Collector meldet die Fehlermeldung: „Auf dem Connector wurde keine lokale IP-Adresse gefunden, die die Datenschnittstellen der SVM erreichen kann.“ **Versuchen Sie Folgendes:** Dies liegt höchstwahrscheinlich an einem Netzwerkproblem auf der ONTAP Seite. Bitte befolgen Sie diese Schritte:

1. Stellen Sie sicher, dass auf der SVM-Daten- oder Verwaltungsebene keine Firewalls vorhanden sind, die die Verbindung von der SVM blockieren.
2. Wenn Sie eine SVM über eine Cluster-Management-IP hinzufügen, stellen Sie sicher, dass die Datenlebensdauer und die Managementlebensdauer der SVM von der Agent-VM aus pingbar sind. Überprüfen Sie bei Problemen das Gateway, die Netzmaske und die Routen für das Leben.

   Sie können auch versuchen, sich über SSH mit der Cluster-Verwaltungs-IP beim Cluster anzumelden und die Agent-IP anzupingen. Stellen Sie sicher, dass die Agent-IP pingbar ist:

   ```
   network ping -vserver <vserver name> -destination <Agent IP> -lif
   <Lif Name> -show-detail
   ```

   Wenn kein Ping möglich ist, stellen Sie sicher, dass die Netzwerkeinstellungen in ONTAP korrekt sind, sodass der Agent-Computer pingbar ist.
3. Wenn Sie versucht haben, eine Verbindung über die Cluster-IP herzustellen, und dies nicht funktioniert hat, versuchen Sie, eine direkte Verbindung über die SVM-IP herzustellen. Die Schritte zum Herstellen einer Verbindung über die SVM-IP finden Sie oben.
4. Überprüfen Sie beim Hinzufügen des Collectors über die SVM-IP und die VSadmin-Anmeldeinformationen, ob für SVM Lif die Rolle „Data plus Mgmt“ aktiviert ist. In diesem Fall funktioniert ein Ping zum SVM Lif, ein SSH zum SVM Lif funktioniert jedoch nicht. Wenn ja, erstellen Sie ein SVM Mgmt Only Lif und versuchen Sie, über dieses SVM Management Only Lif eine Verbindung herzustellen.
5. Wenn es immer noch nicht funktioniert, erstellen Sie ein neues SVM-Lif und versuchen Sie, über dieses Lif eine Verbindung herzustellen. Stellen Sie sicher, dass die Subnetzmaske richtig eingestellt ist.
6. Erweitertes Debuggen:
   a. Starten Sie eine Paketverfolgung in ONTAP.
   b. Versuchen Sie, einen Datensammler über die CloudSecure-Benutzeroberfläche mit dem SVM zu verbinden.
   c. Warten Sie, bis der Fehler auftritt. Stoppen Sie die Paketverfolgung in ONTAP.
   d. Öffnen Sie die Paketverfolgung von ONTAP. Es ist an diesem Standort verfügbar

```
 https://<cluster_mgmt_ip>/spi/<clustername>/etc/log/packet_traces/
.. Stellen Sie sicher, dass ein SYN von ONTAP zur Agent-Box vorhanden ist.
.. Wenn kein SYN von ONTAP vorhanden ist, liegt ein Problem mit der Firewall in ONTAP vor.
.. Öffnen Sie die Firewall in ONTAP, damit ONTAP eine Verbindung zur Agent-Box herstellen kann.
```

7. Wenn es immer noch nicht funktioniert, wenden Sie sich bitte an das Netzwerkteam, um sicherzustellen, dass keine externe Firewall die Verbindung von ONTAP zur Agent-Box blockiert.
8. Wenn keine der oben genannten Maßnahmen das Problem löst, eröffnen Sie einen Fall bei"Netapp-Support" für weitere Unterstützung.

Problem: Meldung: „ ONTAP -Typ für [Hostname: <IP-Adresse>] konnte nicht ermittelt werden. Grund: Verbindungsfehler zum Speichersystem <IP-Adresse>: Host ist nicht erreichbar (Host nicht erreichbar)"
Versuchen Sie Folgendes:

1. Überprüfen Sie, ob die richtige SVM-IP-Verwaltungsadresse oder Cluster-Verwaltungs-IP angegeben wurde.
2. Stellen Sie per SSH eine Verbindung zum SVM oder Cluster her, zu dem Sie eine Verbindung herstellen möchten. Sobald Sie verbunden sind, stellen Sie sicher, dass der SVM- oder Clustername korrekt ist.

Problem: Fehlermeldung: „Connector befindet sich im Fehlerzustand. Dienstname: Audit. Grund für den Fehler: Externer fpolicy-Server beendet." **Versuchen Sie Folgendes:**

1. Höchstwahrscheinlich blockiert eine Firewall die erforderlichen Ports auf dem Agent-Computer. Überprüfen Sie, ob der Portbereich 35000–55000/TCP für die Agent-Maschine geöffnet ist, damit sie eine Verbindung vom SVM herstellen kann. Stellen Sie außerdem sicher, dass auf der ONTAP -Seite keine Firewalls aktiviert sind, die die Kommunikation mit dem Agent-Computer blockieren.
2. Geben Sie den folgenden Befehl in das Agent-Feld ein und stellen Sie sicher, dass der Portbereich geöffnet ist.

   ```
   sudo iptables-save | grep 3500*
   ```

   Die Beispielausgabe sollte folgendermaßen aussehen:

   ```
    -A IN_public_allow -p tcp -m tcp --dport 35000 -m conntrack
   -ctstate NEW -j ACCEPT
   . Melden Sie sich bei SVM an, geben Sie die folgenden Befehle ein
   und überprüfen Sie, dass keine Firewall eingerichtet ist, die die
   Kommunikation mit ONTAP blockiert.
   ```

   ```
   system services firewall show
   system services firewall policy show
   ```

   "Firewall-Befehle prüfen"auf der ONTAP -Seite.

3. Stellen Sie per SSH eine Verbindung zum SVM/Cluster her, den Sie überwachen möchten. Pingen Sie die Agent-Box vom SVM-Datenlebenszyklus aus (mit Unterstützung für CIFS- und NFS-Protokolle) und stellen Sie sicher, dass der Ping funktioniert:

   ```
   network ping -vserver <vserver name> -destination <Agent IP> -lif
   <Lif Name> -show-detail
   ```

   Wenn kein Ping möglich ist, stellen Sie sicher, dass die Netzwerkeinstellungen in ONTAP korrekt sind, sodass der Agent-Computer pingbar ist.

4. Wenn ein einzelner SVM über zwei Datensammler zweimal zu einem Mandanten hinzugefügt wird, wird dieser Fehler angezeigt. Löschen Sie einen der Datensammler über die Benutzeroberfläche. Starten Sie dann den anderen Datensammler über die Benutzeroberfläche neu. Anschließend zeigt der Datensammler den Status „RUNNING“ an und beginnt mit dem Empfang von Ereignissen vom SVM.

   Grundsätzlich sollte in einem Mandanten 1 SVM nur einmal über 1 Datensammler hinzugefügt werden. 1 SVM sollte nicht zweimal über 2 Datensammler hinzugefügt werden.

5. In Fällen, in denen dieselbe SVM in zwei verschiedenen Workload Security-Umgebungen

(Mandanten) hinzugefügt wurde, ist die letzte immer erfolgreich. Der zweite Collector konfiguriert fpolicy mit seiner eigenen IP-Adresse und wirft den ersten raus. Der Collector im ersten empfängt also keine Ereignisse mehr und sein „Audit“-Dienst wechselt in einen Fehlerzustand. Um dies zu verhindern, konfigurieren Sie jede SVM in einer einzelnen Umgebung.

6. Dieser Fehler kann auch auftreten, wenn die Servicerichtlinien nicht richtig konfiguriert sind. Um bei ONTAP 9.8 oder höher eine Verbindung zum Data Source Collector herzustellen, ist der Dienst data-fpolicy-client zusammen mit dem Datendienst data-nfs und/oder data-cifs erforderlich. Darüber hinaus muss der Dienst „data-fpolicy-client“ mit den Datenlebensdauern für die überwachte SVM verknüpft werden.

Problem: Auf der Aktivitätsseite wurden keine Ereignisse angezeigt. **Versuchen Sie Folgendes:**

1. Überprüfen Sie, ob sich der ONTAP Collector im Status „RUNNING“ befindet. Wenn ja, stellen Sie sicher, dass einige CIFS-Ereignisse auf den CIFS-Client-VMs generiert werden, indem Sie einige Dateien öffnen.
2. Wenn keine Aktivitäten angezeigt werden, melden Sie sich bitte beim SVM an und geben Sie den folgenden Befehl ein.

   ```
   <SVM>event log show -source fpolicy
   ```

   Bitte stellen Sie sicher, dass keine Fehler im Zusammenhang mit fpolicy vorliegen.

3. Wenn keine Aktivitäten angezeigt werden, melden Sie sich bitte beim SVM an. Geben Sie den folgenden Befehl ein:

   ```
   <SVM>fpolicy show
   ```

   Überprüfen Sie, ob die fpolicy-Richtlinie mit dem Präfix „cloudsecure_“ festgelegt wurde und der Status „Ein“ ist. Wenn nicht festgelegt, kann der Agent die Befehle im SVM höchstwahrscheinlich nicht ausführen. Bitte stellen Sie sicher, dass alle Voraussetzungen, wie am Anfang der Seite beschrieben, erfüllt sind.

Problem: Der SVM-Datensammler befindet sich im Fehlerzustand und die Fehlermeldung lautet „Der Agent konnte keine Verbindung zum Sammler herstellen.“ **Versuchen Sie Folgendes:**

1. Höchstwahrscheinlich ist der Agent überlastet und kann keine Verbindung zu den Datenquellen-Sammlern herstellen.
2. Überprüfen Sie, wie viele Datenquellensammler mit dem Agenten verbunden sind.
3. Überprüfen Sie auch die Datenflussrate auf der Seite „Alle Aktivitäten“ in der Benutzeroberfläche.
4. Wenn die Anzahl der Aktivitäten pro Sekunde sehr hoch ist, installieren Sie einen anderen Agenten und verschieben Sie einige der Datenquellensammler auf den neuen Agenten.

Problem: SVM Data Collector zeigt die Fehlermeldung „fpolicy.server.connectError: Knoten konnte keine Verbindung mit dem FPolicy-Server „12.195.15.146“ herstellen (Grund: „Select Timed out“)“ an. **Versuchen Sie Folgendes:** Die Firewall ist in SVM/Cluster aktiviert. Daher kann die fpolicy-Engine keine Verbindung zum fpolicy-Server herstellen. CLIs in ONTAP , die zum Abrufen weiterer Informationen verwendet werden können, sind:

```
event log show -source fpolicy which shows the error
event log show -source fpolicy -fields event,action,description which
shows more details.
```

"Firewall-Befehle prüfen"auf der ONTAP -Seite.

Problem: Fehlermeldung: „Der Connector befindet sich im Fehlerzustand. Dienstname: Audit. Grund für den Fehler: Auf der SVM wurde keine gültige Datenschnittstelle (Rolle: Daten, Datenprotokolle: NFS oder CIFS oder beide, Status: aktiv) gefunden.“ **Versuchen Sie Folgendes:** Stellen Sie sicher, dass eine funktionsfähige Schnittstelle vorhanden ist (mit der Rolle „Daten“ und dem Datenprotokoll „CIFS/NFS“).

Problem: Der Datensammler wechselt in den Fehlerzustand und nach einiger Zeit in den RUNNING-Zustand und dann wieder zurück in den Fehlerzustand. Dieser Zyklus wiederholt sich. **Versuchen Sie Folgendes:** Dies geschieht normalerweise im folgenden Szenario:

1. Es wurden mehrere Datensammler hinzugefügt.
2. Den Datensammlern, die dieses Verhalten zeigen, wird 1 SVM hinzugefügt. Das bedeutet, dass zwei oder mehr Datensammler mit einem SVM verbunden sind.
3. Stellen Sie sicher, dass 1 Datensammler nur mit 1 SVM verbunden ist.
4. Löschen Sie die anderen Datensammler, die mit derselben SVM verbunden sind.

Problem: Der Connector befindet sich im Fehlerzustand. Dienstname: Audit. Grund für den Fehler: Fehler beim Konfigurieren (Richtlinie auf SVM svmname). Grund: Ungültiger Wert für das Element „shares-to-include“ in „fpolicy.policy.scope-modify: „Federal“ angegeben. **Versuchen Sie Folgendes:** *Die Freigabenamen müssen ohne Anführungszeichen angegeben werden. Bearbeiten Sie die ONTAP SVM DSC-Konfiguration, um die Freigabenamen zu korrigieren.

Freigaben einschließen und ausschließen ist nicht für eine lange Liste von Freigabenamen vorgesehen. Verwenden Sie stattdessen die Filterung nach Volumen, wenn Sie eine große Anzahl von Aktien ein- oder ausschließen möchten.

Problem: Es gibt im Cluster vorhandene fpolicies, die nicht verwendet werden. Was sollte vor der Installation von Workload Security damit geschehen? **Versuchen Sie Folgendes:** Es wird empfohlen, alle vorhandenen, nicht verwendeten fpolicy-Einstellungen zu löschen, auch wenn sie getrennt sind. Workload Security erstellt fpolicy mit dem Präfix „cloudsecure_“. Alle anderen nicht verwendeten fpolicy-Konfigurationen können gelöscht werden.

CLI-Befehl zum Anzeigen der fpolicy-Liste:

```
 fpolicy show
Schritte zum Löschen von fpolicy-Konfigurationen:
```

```
fpolicy disable -vserver <svmname> -policy-name <policy_name>
fpolicy policy scope delete -vserver <svmname> -policy-name
<policy_name>
fpolicy policy delete -vserver <svmname> -policy-name <policy_name>
fpolicy policy event delete -vserver <svmname> -event-name
<event_list>
fpolicy policy external-engine delete -vserver <svmname> -engine-name
<engine_name>
```

|Nach der Aktivierung der Workload-Sicherheit wird die ONTAP Leistung beeinträchtigt: Die Latenz wird sporadisch hoch, die IOPs werden sporadisch niedrig. |Bei der Verwendung von ONTAP mit Workload Security können manchmal Latenzprobleme in ONTAP auftreten. Hierfür gibt es eine Reihe möglicher Gründe, die im Folgenden aufgeführt sind:"1372994" , "1415152" , "1438207" , "1479704" , "1354659" . Alle diese Probleme wurden in ONTAP 9.13.1 und höher behoben. Es wird dringend empfohlen, eine dieser neueren Versionen zu verwenden.

Problem: Beim Datensammler liegt ein Fehler vor, diese Fehlermeldung wird angezeigt. „Fehler: Connector befindet sich im Fehlerzustand. Dienstname: Audit. Grund für den Fehler: Die Richtlinie konnte auf SVM svm_test nicht konfiguriert werden. Grund: Fehlender Wert für Zapi-Feld: Ereignisse. „ **Versuchen Sie Folgendes:**

1. Beginnen Sie mit einer neuen SVM, auf der nur der NFS-Dienst konfiguriert ist.
2. Fügen Sie in Workload Security einen ONTAP SVM-Datensammler hinzu. CIFS wird als zulässiges Protokoll für die SVM konfiguriert, während der ONTAP SVM Data Collector in Workload Security hinzugefügt wird.
3. Warten Sie, bis der Datensammler in Workload Security einen Fehler anzeigt.
4. Da der CIFS-Server NICHT auf der SVM konfiguriert ist, wird dieser links angezeigte Fehler von Workload Security angezeigt.
5. Bearbeiten Sie den ONTAP SVM-Datensammler und deaktivieren Sie CIFs als zulässiges Protokoll. Speichern Sie den Datensammler. Es wird nur mit aktiviertem NFS-Protokoll ausgeführt.

Problem: Der Datensammler zeigt die Fehlermeldung an: „Fehler: Der Zustand des Sammlers konnte innerhalb von 2 Versuchen nicht ermittelt werden. Versuchen Sie, den Sammler erneut neu zu starten (Fehlercode: AGENT008)“. **Versuchen Sie Folgendes:**

1. Scrollen Sie auf der Seite „Datensammler“ nach rechts neben den Datensammler, der den Fehler ausgibt, und klicken Sie auf das Menü mit den drei Punkten. Wählen Sie *Bearbeiten*. Geben Sie das Passwort des Datensammlers erneut ein. Speichern Sie den Datensammler, indem Sie auf die Schaltfläche *Speichern* klicken. Data Collector wird neu gestartet und der Fehler sollte behoben sein.
2. Die Agent-Maschine verfügt möglicherweise nicht über genügend CPU- oder RAM-Reserve, weshalb die DSCs ausfallen. Bitte überprüfen Sie die Anzahl der Datensammler, die dem Agenten auf der Maschine hinzugefügt wurden. Wenn es mehr als 20 sind, erhöhen Sie bitte die CPU- und RAM-Kapazität der Agent-Maschine. Sobald die CPU und der RAM erhöht werden, wechseln die DSCs automatisch in den Initialisierungs- und dann in den Ausführungszustand. Schauen Sie in die Größentabelle auf"diese Seite" .

Problem: Der Datensammler gibt einen Fehler aus, wenn der SVM-Modus ausgewählt ist. **Versuchen Sie Folgendes:** Wenn beim Verbinden im SVM-Modus die Cluster-Management-IP anstelle der SVM-Management-IP zum Verbinden verwendet wird, tritt ein Verbindungsfehler auf. Stellen Sie sicher, dass die richtige SVM-IP verwendet wird.

Problem: Der Datensammler zeigt eine Fehlermeldung an, wenn die Funktion „Zugriff verweigert“ aktiviert ist: „Connector befindet sich im Fehlerzustand. Dienstname: Audit. Grund für den Fehler: Fehler beim Konfigurieren von fpolicy auf SVM test_svm. Grund: Der Benutzer ist nicht autorisiert." **Versuchen Sie Folgendes:** Dem Benutzer fehlen möglicherweise die REST-Berechtigungen, die für die Funktion „Zugriff verweigert“ erforderlich sind. Bitte folgen Sie den Anweisungen auf"diese Seite" um die Berechtigungen festzulegen.

Starten Sie den Collector neu, sobald die Berechtigungen festgelegt sind.

Wenn weiterhin Probleme auftreten, verwenden Sie die Support-Links auf der Seite **Hilfe > Support**.

Fehlerbehebung

Fehlerbehebung bei allgemeinen Problemen mit Data Infrastructure Insights

Hier finden Sie Vorschläge zur Fehlerbehebung bei Data Infrastructure Insights.

Siehe auch"Fehlerbehebung bei Problemen mit der Linux-Erfassungseinheit" Und"Fehlerbehebung bei Problemen mit der Windows-Erfassungseinheit" .

Anmeldeprobleme

Problem:	Versuchen Sie Folgendes:
Data Infrastructure Insights meldet sich automatisch alle 6 Stunden ab	Dies liegt daran, dass im Browser Cookies von Drittanbietern deaktiviert sind. Benutzer können ihren Browser so konfigurieren, dass alle Cookies von Drittanbietern aktiviert werden, oder eine engere Ausnahmeliste verwenden, um nur diese für Data Infrastructure Insights zu aktivieren. Beispiel: Öffnen Sie die Einstellungen Ihres Browsers. Wählen Sie die Option „Alle Cookies zulassen“. **ODER** Wählen Sie „Cookies von Drittanbietern blockieren“ und fügen Sie Ausnahmen für *[*.]auth0.com* und *[*.]netapp.com* hinzu. Microsoft Edge verwendet für Ausnahmen dasselbe Format wie Chrome. In Firefox werden Cookie-Ausnahmen einfach als *auth0.com* und *netapp.com* bezeichnet.
Ich habe ein Konsolenkonto, kann mich aber nicht anmelden.	Öffnen Sie ein Ticket von https://mysupport.netapp.com/site/help . Wählen Sie die Kategorie „console.netapp.com > Konto-/Anmeldeprobleme“ oder „console.netapp.com > Föderationsprobleme“. Diese sind speziell für Probleme oder Fragen zur Konsole gedacht. Bei allen anderen technischen Supportfragen zu Data Infrastructure Insights wenden Sie sich an"NetApp -Support" .
Ich wurde zu Data Infrastructure Insights eingeladen, erhalte jedoch die Meldung „Nicht autorisiert“.	Stellen Sie sicher, dass Sie sich für ein Konsolenkonto angemeldet haben oder dass Ihre Organisation die SSO-Anmeldung mit der Konsole verwendet. Überprüfen Sie, ob die E-Mail-Adresse Ihres Konsolenprofils mit der E-Mail-Adresse in Ihrer Data Infrastructure Insights -Begrüßungs-E-Mail übereinstimmt. Wenn die E-Mail nicht übereinstimmt, fordern Sie eine neue Einladung mit der richtigen E-Mail-Adresse an.

Problem:	Versuchen Sie Folgendes:
Ich habe mich von der Konsole abgemeldet und wurde automatisch von Data Infrastructure Insights abgemeldet.	Single Sign-On (SSO) über NetApp Cloud Services meldet alle Data Infrastructure Insights Sitzungen ab. Wenn Sie Zugriff auf mehrere Data Infrastructure Insights -Konten haben, werden beim Abmelden von einem Konto alle aktiven Sitzungen abgemeldet. Melden Sie sich erneut an, um auf Ihr Konto zuzugreifen.
Ich wurde nach mehreren Tagen automatisch abgemeldet.	NetApp Cloud-Konten erfordern alle paar Tage eine erneute Authentifizierung (die aktuelle Konsoleneinstellung ist 7 Tage). Melden Sie sich erneut an, um auf Ihr Konto zuzugreifen.
Ich erhalte die Fehlermeldung „Keine Berechtigung mehr zur Anmeldung“.	Wenden Sie sich an Ihren Kontoadministrator, um den Zugriff auf Data Infrastructure Insights zu überprüfen. Überprüfen Sie, ob die E-Mail-Adresse Ihres Konsolenprofils mit der E-Mail-Adresse übereinstimmt, die in Ihrer Data Infrastructure Insights -Begrüßungs-E-Mail angezeigt wird.
Andere Anmeldefehler	Probieren Sie den Inkognito-Modus in Chrome aus oder löschen Sie den Browserverlauf, die Cookies und den Cache. Versuchen Sie es mit einem anderen Browserprofil (z. B. Chrome – Person hinzufügen).

Andere Probleme

Frage:	Antwort:
Meine Qtree-Hard-Quotas werden in Abfragen korrekt angezeigt, aber meine Soft-Quotas werden als Gesamtkapazität des Datenträgers angezeigt. Ist das richtig?	Nur feste Kontingente – entweder manuell festgelegt oder über Trident festgelegt – werden als festgelegte Kontingente angezeigt. Wenn keine festen Kontingente angegeben sind, entspricht die Qtree-Kapazität der internen Volume-Kapazität.
Ich habe sowohl eine weiche als auch eine harte Quote manuell im selben Qtree festgelegt, aber die angezeigte Gesamtkapazität ist die harte Quote. Ist das richtig?	Ja, wenn eine feste Quote angegeben ist, wird diese als Gesamtkapazität angezeigt.
Beim Eingeben einer Zeitplanzeit für einen Cognos-Bericht erhalte ich manchmal ein zusätzliches „m“ in der Zeitplanzeit. Wenn ich die Uhrzeit beispielsweise als „02:15 PM“ eingebe, wird möglicherweise ein zusätzliches Zeichen hinzugefügt: „02:15 PMM“ (oder PMm). Wenn ich nach draußen klicke, ändert sich die Anzeige in „2:15 Uhr“. Ich kann den Bericht speichern, aber wenn ich den gespeicherten Bericht erneut öffne, wird als geplante Zeit AM (also Morgen) angezeigt, unabhängig davon, ob ich in der geplanten Zeit AM oder PM eingegeben habe.	Geben Sie die geplante Zeit erneut ein und achten Sie darauf, nicht die vollständigen Zeichen „AM“ oder „PM“ einzugeben. Es reicht aus, „A“ für „AM“ oder „P“ für „PM“ einzugeben. Wenn Ihnen das zusätzliche Zeichen nicht angezeigt wird, ist die geplante Zeit korrekt eingestellt.

Ressourcen

Weitere Tipps zur Fehlerbehebung finden Sie im"NetApp Wissensdatenbank" (Support-Anmeldung erforderlich).

Weitere Supportinformationen finden Sie in den Data Infrastructure Insights"Support" Seite.

Wenn Sie über ein aktives Data Infrastructure Insights -Abonnement verfügen, können Sie diese Supportoptionen nutzen:

"Telefon" "Support-Ticket"

Weitere Informationen finden Sie im "Supportdokumentation zu Data Infrastructure Insights" .

Fehlerbehebung bei Problemen mit der Erfassungseinheit unter Linux

Hier finden Sie Vorschläge zur Behebung von Problemen mit Acquisition Units auf einem Linux-Server.

Problem:	**Versuchen Sie Folgendes:**
Der AU-Status auf der Seite **Beobachtbarkeit > Sammler** auf der Registerkarte **Erfassungseinheiten** zeigt „Zertifikat abgelaufen“ oder „Zertifikat widerrufen“ an.	Klicken Sie auf das Menü rechts neben der AU und wählen Sie **Verbindung wiederherstellen**. Befolgen Sie die Anweisungen zum Wiederherstellen Ihrer Erfassungseinheit: 1. Stoppen Sie den Acquisition Unit (AU)-Dienst. Sie können auf die Schaltfläche *Stoppbefehl kopieren* klicken, um den Befehl schnell in die Zwischenablage zu kopieren und ihn dann in eine Eingabeaufforderung auf dem Computer der Erfassungseinheit einzufügen. 2. Erstellen Sie eine Datei mit dem Namen „token“ im Ordner */var/lib/netapp/cloudinsights/acq/conf* auf der AU. 3. Klicken Sie auf die Schaltfläche *Token kopieren* und fügen Sie dieses Token in die von Ihnen erstellte Datei ein. 4. Starten Sie den AU-Dienst neu. Klicken Sie auf die Schaltfläche „Neustartbefehl kopieren“ und fügen Sie den Befehl in eine Eingabeaufforderung auf der AU ein.
Berechtigung beim Starten des Acquisition Unit Server Service verweigert	Wenn die AU auf SELINUX installiert ist, sollte SE auf den *permissiven* Modus eingestellt werden. Der *Enforcing*-Modus wird nicht unterstützt. Nachdem Sie SELINUX in den permissiven Modus versetzt haben, starten Sie den AU-Dienst neu.
Serveranforderungen nicht erfüllt	Stellen Sie sicher, dass Ihr Acquisition Unit-Server oder Ihre VM"Anforderungen"

Netzwerkanforderungen nicht erfüllt	Stellen Sie sicher, dass Ihr Acquisition Unit-Server/Ihre Acquisition Unit-VM über eine SSL-Verbindung über Port 443 auf Ihre Data Infrastructure Insights -Umgebung (<environment-name>.c01.cloudinsights.netapp.com) zugreifen kann. Versuchen Sie die folgenden Befehle: *ping <Umgebungsname>.c01.cloudinsights.netapp.com traceroute <Umgebungsname>.c01.cloudinsights.netapp.com curl https://<Umgebungsname>.c01.cloudinsights.netapp.com wget https://<Umgebungsname>.c01.cloudinsights.netapp.com* Beachten Sie, dass Port 443 von der AU zu Data Infrastructure Insights„ausgehend“ geöffnet werden muss.
Proxyserver nicht richtig konfiguriert	Überprüfen Sie Ihre Proxy-Einstellungen und deinstallieren/installieren Sie die Acquisition Unit-Software gegebenenfalls neu, um die richtigen Proxy-Einstellungen einzugeben. 1. Versuchen Sie es mit „curl“. Weitere Informationen/Dokumentation zu „man curl“ zu Proxys: --preproxy, --proxy-* (das ist ein Platzhalter „*“, da curl viele Proxy-Einstellungen unterstützt). 2. Versuchen Sie es mit „wget“. Informationen zu Proxy-Optionen finden Sie in der Dokumentation.
Die Installation der Erfassungseinheit ist in Data Infrastructure Insights mit Anmeldeinformationsfehlern beim Starten des Erfassungsdienstes fehlgeschlagen (und im acq.log sichtbar).	Dies kann durch die Einbeziehung von Sonderzeichen in die Proxy-Anmeldeinformationen verursacht werden. Deinstallieren Sie die AU (*sudo cloudinsights-uninstall.sh*) und installieren Sie sie erneut, ohne Sonderzeichen zu verwenden.
Linux: Fehlende Bibliothek / Datei nicht gefunden	Stellen Sie sicher, dass Ihr Linux Acquisition Unit-Server/Ihre Linux Acquisition Unit-VM über alle erforderlichen Bibliotheken verfügt. Beispielsweise muss die Bibliothek *unzip* auf dem Server installiert sein. Um die *unzip*-Bibliothek zu installieren, führen Sie den Befehl **sudo yum install unzip** aus, bevor Sie das Installationsskript der Erfassungseinheit ausführen
Berechtigungsprobleme	Stellen Sie sicher, dass Sie als Benutzer mit *sudo* -Berechtigungen angemeldet sind
Erfassung läuft nicht:	Sammeln Sie das acq.log aus /opt/netapp/cloudinsights/acq/logs (Linux). Starten Sie den Erfassungsdienst neu: sudo cloudinsights-service.sh restart acquisition
Probleme bei der Datenerfassung:	Senden Sie einen Fehlerbericht von der Zielseite des Datensammlers, indem Sie auf die Schaltfläche „Fehlerbericht senden“ klicken.

Status: Heartbeat fehlgeschlagen	Die Acquisition Unit (AU) sendet alle 60 Sekunden einen Heartbeat an Data Infrastructure Insights, um ihren Mietvertrag zu erneuern. Wenn der Heartbeat-Aufruf aufgrund eines Netzwerkproblems oder einer nicht reagierenden Data Infrastructure Insights fehlschlägt, wird die Lease-Zeit der AU nicht aktualisiert. Wenn die Lease-Zeit der AU abläuft, zeigt Data Infrastructure Insights den Status „Heartbeat Failed“ an. Schritte zur Fehlerbehebung: Überprüfen Sie die Netzwerkverbindung zwischen dem Acquisition Unit-Server und CloudInsights. Überprüfen Sie, ob der Acquisition Unit-Dienst ausgeführt wird. Wenn der Dienst nicht ausgeführt wird, starten Sie ihn. Überprüfen Sie das Protokoll der Erfassungseinheit (/var/log/netapp/cloudinsights/acq/acq.log), um festzustellen, ob Fehler vorliegen.
Ich sehe die Meldung „Heartbeat-Fehler:“	Dieser Fehler kann auftreten, wenn eine Netzwerkunterbrechung vorliegt, die dazu führt, dass die Kommunikation zwischen der Erfassungseinheit und der Data Infrastructure Insights -Umgebung länger als eine Minute unterbrochen wird. Überprüfen Sie, ob die Verbindung zwischen AU und Data Infrastructure Insights stabil und aktiv ist.
Beim erneuten Installieren der Erfassungseinheit wird mir „ValueError: Dateikontext für /opt/netapp/cloudinsights(/.*)? bereits definiert“ angezeigt.	Auf einem System mit SELinux kann diese Fehlermeldung nach `cloudinsights-uninstall.sh -p` wurde ausgeführt und die Erfassungseinheit soll neu installiert werden. Ausführen des Befehls `semanage fcontext -d -t usr_t "/opt/netapp/cloudinsights(/.*)?"` sollte das Problem beheben und die Nachricht entfernen.

Überlegungen zu Proxys und Firewalls

Wenn Ihre Organisation die Verwendung eines Proxys für den Internetzugang erfordert, müssen Sie möglicherweise das Proxy-Verhalten Ihrer Organisation verstehen und nach bestimmten Ausnahmen suchen, damit Data Infrastructure Insights funktioniert. Beachten Sie Folgendes:

- Erstens: Blockiert Ihre Organisation den Zugriff standardmäßig und erlaubt den Zugriff auf bestimmte Websites/Domänen nur ausnahmsweise? In diesem Fall müssen Sie die folgende Domäne zur Ausnahmeliste hinzufügen:

  ```
  *.cloudinsights.netapp.com
  ```

  Ihre Data Infrastructure Insights Acquisition Unit sowie Ihre Interaktionen in einem Webbrowser mit Data Infrastructure Insights werden alle an Hosts mit diesem Domänennamen weitergeleitet.

- Zweitens versuchen einige Proxys, eine TLS/SSL-Prüfung durchzuführen, indem sie sich mit digitalen Zertifikaten, die nicht von NetApp generiert wurden, als Data Infrastructure Insights -Websites ausgeben. Das Sicherheitsmodell der Data Infrastructure Insights Acquisition Unit ist grundsätzlich nicht mit diesen

Technologien kompatibel. Sie benötigen außerdem den oben genannten Domänennamen, der von dieser Funktion ausgenommen ist, damit sich die Data Infrastructure Insights Acquisition Unit erfolgreich bei Data Infrastructure Insights anmelden und die Datenermittlung erleichtern kann.

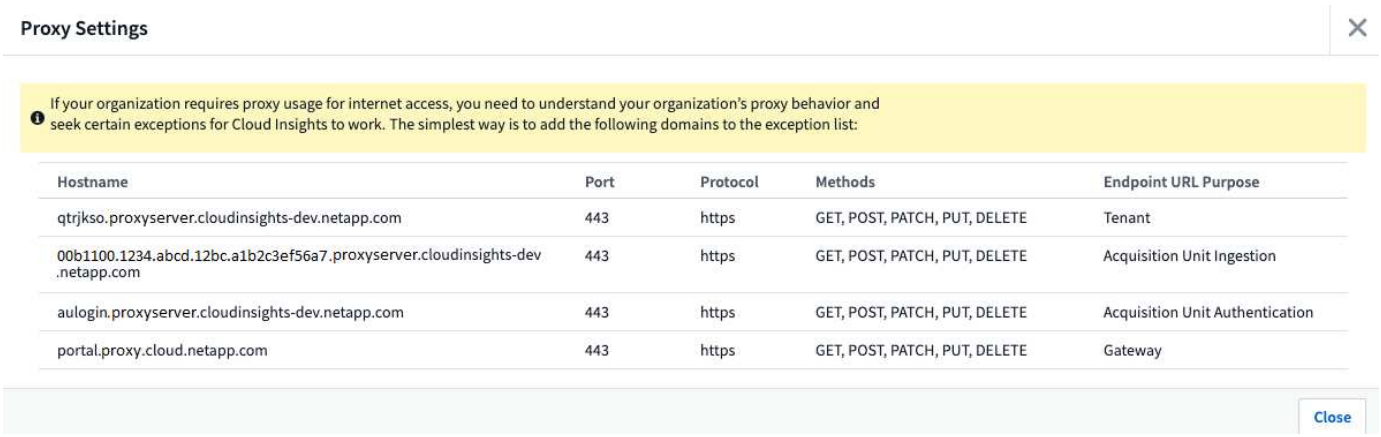
Falls der Proxy für die Verkehrsprüfung eingerichtet ist, muss die Data Infrastructure Insights Umgebung zu einer Ausnahmeliste in der Proxy-Konfiguration hinzugefügt werden. Das Format und die Einrichtung dieser Ausnahmeliste variieren je nach Ihrer Proxy-Umgebung und Ihren Tools. Im Allgemeinen müssen Sie dieser Ausnahmeliste jedoch die URLs der Data Infrastructure Insights -Server hinzufügen, damit die AU ordnungsgemäß mit diesen Servern kommunizieren kann.

Der einfachste Weg hierfür besteht darin, die Data Infrastructure Insights Domäne selbst zur Ausnahmeliste hinzuzufügen:

```
 *.cloudinsights.netapp.com
Falls der Proxy nicht für die Verkehrskontrolle eingerichtet ist, kann
eine Ausnahmeliste erforderlich sein, muss es aber nicht.  Wenn Sie nicht
sicher sind, ob Sie Data Infrastructure Insights zu einer Ausnahmeliste
hinzufügen müssen, oder wenn bei der Installation oder Ausführung von Data
Infrastructure Insights aufgrund der Proxy- und/oder Firewall-
Konfiguration Probleme auftreten, wenden Sie sich an Ihr Proxy-
Administrationsteam, um die Handhabung der SSL-Abfangung durch den Proxy
einzurichten.
```

Anzeigen von Proxy-Endpunkten

Sie können Ihre Proxy-Endpunkte anzeigen, indem Sie beim Auswählen eines Datensammlers während des Onboardings auf den Link **Proxy-Einstellungen** oder auf der Seite **Hilfe > Support** auf den Link unter *Proxy-Einstellungen* klicken. Es wird eine Tabelle wie die folgende angezeigt. Wenn Sie in Ihrer Umgebung über Workload Security verfügen, werden die konfigurierten Endpunkt-URLs auch in dieser Liste angezeigt.



Ressourcen

Weitere Tipps zur Fehlerbehebung finden Sie im"NetApp Wissensdatenbank" (Support-Anmeldung erforderlich).

Weitere Supportinformationen finden Sie in den Data Infrastructure Insights"Support" Seite.

Fehlerbehebung bei Problemen mit der Erfassungseinheit unter Windows

Hier finden Sie Vorschläge zur Behebung von Problemen mit Acquisition Units auf einem Windows-Server.

Problem:	Versuchen Sie Folgendes:
Der AU-Status auf der Seite **Beobachtbarkeit > Sammler** auf der Registerkarte **Erfassungseinheiten** zeigt „Zertifikat abgelaufen“ oder „Zertifikat widerrufen“ an.	Klicken Sie auf das Menü rechts neben der AU und wählen Sie **Verbindung wiederherstellen**. Befolgen Sie die Anweisungen zum Wiederherstellen Ihrer Erfassungseinheit: 1. Stoppen Sie den Acquisition Unit (AU)-Dienst. Sie können auf die Schaltfläche *Stoppbefehl kopieren* klicken, um den Befehl schnell in die Zwischenablage zu kopieren und ihn dann in eine Eingabeaufforderung auf dem Computer der Erfassungseinheit einzufügen. 2. Erstellen Sie eine Datei mit dem Namen „Token“ im Ordner *c:\Program Files\ Cloud Insights\Acquisition Unit\conf* auf der AU. 3. Klicken Sie auf die Schaltfläche *Token kopieren* und fügen Sie dieses Token in die von Ihnen erstellte Datei ein. 4. Starten Sie den AU-Dienst neu. Klicken Sie auf die Schaltfläche „Neustartbefehl kopieren“ und fügen Sie den Befehl in eine Eingabeaufforderung auf der AU ein.
Serveranforderungen nicht erfüllt	Stellen Sie sicher, dass Ihr Acquisition Unit-Server oder Ihre VM"Anforderungen"
Netzwerkanforderungen nicht erfüllt	Stellen Sie sicher, dass Ihr Acquisition Unit-Server/Ihre Acquisition Unit-VM über eine SSL-Verbindung über Port 443 auf Ihre Data Infrastructure Insights -Umgebung (<environment-name>.c01.cloudinsights.netapp.com) zugreifen kann. Versuchen Sie die folgenden Befehle: *ping <Umgebungsname>.c01.cloudinsights.netapp.com traceroute <Umgebungsname>.c01.cloudinsights.netapp.com curl https://<Umgebungsname>.c01.cloudinsights.netapp.com wget https://<Umgebungsname>.c01.cloudinsights.netapp.com* Beachten Sie, dass Port 443 von der AU zu Data Infrastructure Insights„ausgehend“ geöffnet werden muss.

Proxyserver nicht richtig konfiguriert	Überprüfen Sie Ihre Proxy-Einstellungen und deinstallieren/installieren Sie die Acquisition Unit-Software gegebenenfalls neu, um die richtigen Proxy-Einstellungen einzugeben. 1. Versuchen Sie es mit „curl“. Weitere Informationen/Dokumentation zu „man curl“ zu Proxys: --preproxy, --proxy-* (das ist ein Platzhalter „*“, da curl viele Proxy-Einstellungen unterstützt). 2. Versuchen Sie es mit „wget“. Informationen zu Proxy-Optionen finden Sie in der Dokumentation.
Die Installation der Erfassungseinheit ist in Data Infrastructure Insights mit Anmeldeinformationsfehlern beim Starten des Erfassungsdienstes fehlgeschlagen (und im acq.log sichtbar).	Dies kann durch die Einbeziehung von Sonderzeichen in die Proxy-Anmeldeinformationen verursacht werden. Deinstallieren Sie die AU (*sudo cloudinsights-uninstall.sh*) und installieren Sie sie erneut, ohne Sonderzeichen zu verwenden.
Berechtigungsprobleme	Stellen Sie sicher, dass Sie als Benutzer mit Administratorrechten angemeldet sind
Akquisition läuft nicht	Informationen finden Sie im acq.log im Ordner *<Installationsverzeichnis>\ Cloud Insights\Acquisition Unit\log*. Starten Sie die Erfassung über die Windows-Dienste neu
Probleme bei der Datenerfassung	Senden Sie einen Fehlerbericht von der Zielseite des Datensammlers, indem Sie auf die Schaltfläche „Fehlerbericht senden“ klicken.
Status: Heartbeat fehlgeschlagen	Die Acquisition Unit (AU) sendet alle 60 Sekunden einen Heartbeat an Data Infrastructure Insights, um ihren Mietvertrag zu erneuern. Wenn der Heartbeat-Aufruf aufgrund eines Netzwerkproblems oder einer nicht reagierenden Data Infrastructure Insights fehlschlägt, wird die Lease-Zeit der AU nicht aktualisiert. Wenn die Lease-Zeit der AU abläuft, zeigt Data Infrastructure Insights den Status „Heartbeat Failed“ an. Schritte zur Fehlerbehebung: * Überprüfen Sie die Netzwerkverbindung zwischen dem Acquisition Unit-Server und CloudInsights. * Prüfen Sie, ob der Acquisition Unit-Dienst ausgeführt wird. Wenn der Dienst nicht ausgeführt wird, starten Sie ihn. * Überprüfen Sie das Protokoll der Erfassungseinheit (<Installationsverzeichnis>:\Programme\ Cloud Insights\Acquisition Unit\log\acq.log), um festzustellen, ob Fehler vorliegen.
Ich sehe die Meldung „Heartbeat-Fehler:	Dieser Fehler kann auftreten, wenn eine Netzwerkunterbrechung vorliegt, die dazu führt, dass die Kommunikation zwischen der Erfassungseinheit und der Data Infrastructure Insights -Umgebung länger als eine Minute unterbrochen wird. Überprüfen Sie, ob die Verbindung zwischen AU und Data Infrastructure Insights stabil und aktiv ist.

Überlegungen zu Proxys und Firewalls

Wenn Ihre Organisation die Verwendung eines Proxys für den Internetzugang erfordert, müssen Sie möglicherweise das Proxy-Verhalten Ihrer Organisation verstehen und nach bestimmten Ausnahmen suchen, damit Data Infrastructure Insights funktioniert. Beachten Sie Folgendes:

- Erstens: Blockiert Ihre Organisation den Zugriff standardmäßig und erlaubt den Zugriff auf bestimmte Websites/Domänen nur ausnahmsweise? In diesem Fall müssen Sie die folgende Domäne zu Ihrer Ausnahmeliste hinzufügen:

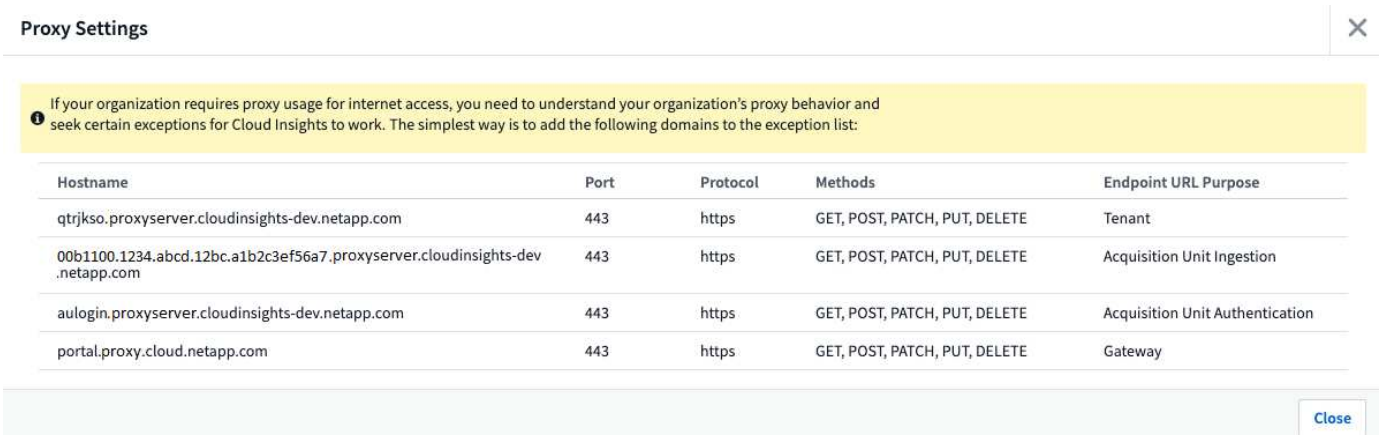
  ```
  *.cloudinsights.netapp.com
  ```

  Ihre Data Infrastructure Insights Acquisition Unit sowie Ihre Interaktionen in einem Webbrowser mit Data Infrastructure Insights werden alle an Hosts mit diesem Domänennamen weitergeleitet.

- Zweitens versuchen einige Proxys, eine TLS/SSL-Prüfung durchzuführen, indem sie sich mit digitalen Zertifikaten, die nicht von NetApp generiert wurden, als Data Infrastructure Insights -Websites ausgeben. Das Sicherheitsmodell der Data Infrastructure Insights Acquisition Unit ist grundsätzlich nicht mit diesen Technologien kompatibel. Sie benötigen außerdem den oben genannten Domänennamen, der von dieser Funktion ausgenommen ist, damit sich die Data Infrastructure Insights Acquisition Unit erfolgreich bei Data Infrastructure Insights anmelden und die Datenermittlung erleichtern kann.

Anzeigen von Proxy-Endpunkten

Sie können Ihre Proxy-Endpunkte anzeigen, indem Sie beim Auswählen eines Datensammlers während des Onboardings auf den Link **Proxy-Einstellungen** oder auf der Seite **Hilfe > Support** auf den Link unter *Proxy-Einstellungen* klicken. Es wird eine Tabelle wie die folgende angezeigt. Wenn Sie in Ihrer Umgebung über Workload Security verfügen, werden die konfigurierten Endpunkt-URLs auch in dieser Liste angezeigt.



Ressourcen

Weitere Tipps zur Fehlerbehebung finden Sie im"NetApp Wissensdatenbank" (Support-Anmeldung erforderlich).

Weitere Supportinformationen finden Sie in den Data Infrastructure Insights"Support" Seite.

Untersuchung eines gescheiterten Datensammlers

Wenn ein Datensammler eine Fehlermeldung und eine hohe oder mittlere Auswirkung aufweist, müssen Sie dieses Problem mithilfe der Übersichtsseite des Datensammlers und der darin verknüpften Informationen untersuchen.

Führen Sie die folgenden Schritte aus, um die Ursache für fehlgeschlagene Datensammler zu ermitteln. Fehlermeldungen zum Datensammler werden im Menü **Admin** und auf der Seite **Installierte Datensammler** angezeigt.

Schritte

1. Klicken Sie auf **Admin** > **Datensammler** > **Installierte Datensammler**.
2. Klicken Sie auf den verknüpften Namen des fehlerhaften Datensammlers, um die Seite „Zusammenfassung“ zu öffnen.
3. Überprüfen Sie auf der Seite „Zusammenfassung“ den Bereich „Kommentare“, um alle Notizen zu lesen, die möglicherweise von einem anderen Techniker hinterlassen wurden, der diesen Fehler möglicherweise ebenfalls untersucht.
4. Beachten Sie alle Leistungsmeldungen.
5. Bewegen Sie den Mauszeiger über die Segmente des Ereigniszeitleistendiagramms, um zusätzliche Informationen anzuzeigen.
6. Wählen Sie eine Fehlermeldung für ein Gerät aus, die unterhalb der Ereigniszeitleiste angezeigt wird, und klicken Sie auf das Symbol „Fehlerdetails“, das rechts neben der Meldung angezeigt wird.

   Die Fehlerdetails umfassen den Text der Fehlermeldung, die wahrscheinlichsten Ursachen, verwendete Informationen und Vorschläge, was zur Behebung des Problems versucht werden kann.

7. Im Bereich „Von diesem Datensammler gemeldete Geräte“ können Sie die Liste filtern, um nur die Geräte anzuzeigen, die Sie interessieren, und Sie können auf den verknüpften **Namen** eines Geräts klicken, um die Asset-Seite für dieses Gerät anzuzeigen.
8. Wenn Sie zur Übersichtsseite des Datensammlers zurückkehren, überprüfen Sie den Bereich **Letzte Änderungen anzeigen** unten auf der Seite, um festzustellen, ob das Problem durch kürzliche Änderungen verursacht worden sein könnte.

Data Infrastructure Insights Datensammler-Supportmatrix

Die Data Collector Support Matrix bietet Referenzen für von Data Infrastructure Insights unterstützte Data Collectors, einschließlich Anbieter- und Modellinformationen.

HP Enterprise 3PAR / Alletra 9000 / Primera StoreServ Storage

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
HPE Alletra 9080 HPE_3PAR 20450 HPE_3PAR 20800 HPE_3PAR 20850 HPE_3PAR 7200 HPE_3PAR 7200c HPE_3PAR 7400 HPE_3PAR 7400c HPE_3PAR 7440c HPE_3PAR 7450c HPE_3PAR 8200 HPE_3PAR 8400 HPE_3PAR 8440 HPE_3PAR 8450 HPE_3PAR 9450 HPE_3PAR A630 HPE_3PAR A650 HPE_3PAR A670 HP_3PAR 20800 HP_3PAR 7200 HP_3PAR 7200c HP_3PAR 7400 HP_3PAR 7400c HP_3PAR 7440c HP_3PAR 7450c HP_3PAR 8200 HP_3PAR 8400 HP_3PAR 8440 InServ F200 InServ F400 InServ T400 InServ T800 InServ V400 InServ V800	3.1.1 (MU1) 3.1.2 (MU3) 3.1.3 (MU1) 3.1.3 (MU2) 3.2.1 (MU2) 3.2.1 (MU3) 3.2.1 (MU5) 3.2.2 (MU4) 3.2.2 (MU6) 3.3.1 3.3.1 (MU1) 3.3.1 (MU2) 3.3.1 (MU3) 3.3.1 (MU5) 3.3.2 (MU1) 4.3.1 4.3.3 4.4.1 Versionstyp: Version mit Standardsupport 4.5.15 Versionstyp: Version mit erweitertem Support 4.5.18 Versionstyp: Version mit erweitertem Support 4.5.21 Versionstyp: Version mit erweitertem Support 4.5.24 Versionstyp: Version mit erweitertem Support 4.5.7 Versionstyp: Version mit erweitertem Support 4.6.1 Version Typ: Erweiterter Support Release 9.5.15 Release-Typ: Erweiterter Support Release 9.5.8 Release-Typ: Erweiterter Support Release 9.6.1 Release-Typ: Erweiterter Support Release

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Stiftung					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Protokoll-Controller	Implementiert	SSH	
		Speicherport	Implementiert	SSH	
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Typ	Lücke	SSH	
	Volumenmaske	Initiator	Implementiert	SSH	
		Protokoll-Controller	Implementiert	SSH	
		Speicherport	Implementiert	SSH	
		Typ	Lücke	SSH	
	Volumenreferenz	Name	Implementiert	SSH	
		Speicher-IP	Implementiert	SSH	
	WWN-Alias	Host-Aliase	Implementiert	SSH	
		Objekttyp	Implementiert	SSH	
		Quelle	Implementiert	SSH	
		WWN	Implementiert	SSH	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Leistung					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Teilweise blockiertes Verhältnis	Implementiert	SMI-S	
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Server-ID	Implementiert	SMI-S	
		Durchsatz beim Lesen	Implementiert	SMI-S	
		Durchsatz gesamt	Implementiert	SMI-S	Durchschnittliche Gesamtrate der Festplatte (Lesen und Schreiben auf allen Festplatten) in MB/s
		Durchsatz beim Schreiben	Implementiert	SMI-S	
		Schreiben ausstehend	Implementiert	SMI-S	insgesamt ausstehende Schreibvorgänge

Von diesem Datensammler verwendete Verwaltungs-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschichtprotokoll	Verwendete eingehende Ports	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur schreibgeschützte Anmeldeinformationen	Unterstützt Verschlüsselung	Firewall-freundlich (statische Ports)
3Par SMI-S	SMI-S	HTTP/HTTPS	5988/5989		true	true	true	true
3Par CLI	SSH	SSH	22		true	FALSCH	true	true

Amazon AWS EC2

Von diesem Datensammler unterstützte Modelle und Versionen: API-Versionen:

- 01.10.2014

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Stiftung					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Hersteller	Implementiert	HTTPS	
		Name	Implementiert	HTTPS	
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		OID	Implementiert	HTTPS	
	Info	API-Beschreibung	Implementiert	HTTPS	
		API-Name	Implementiert	HTTPS	
		API-Version	Implementiert	HTTPS	
		Datenquellenname	Implementiert	HTTPS	Info
		Datum	Implementiert	HTTPS	
		Absender-ID	Implementiert	HTTPS	
		Urheberschlüssel	Implementiert	HTTPS	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Leistung					

					allen Festplatten) in MB/s
Produkt	**Kategorie**	**Funktionsname/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Schreiben	Implementiert	HTTPS	
	vm	Gesamte CPU-Auslastung	Implementiert	HTTPS	
		IOPs gelesen	Implementiert	HTTPS	Anzahl der gelesenen IOPs auf der Festplatte
		diskIops.total	Implementiert	HTTPS	
		Festplatten-IOPs beim Schreiben	Implementiert	HTTPS	
		Latenz beim Lesen	Implementiert	HTTPS	
		Latenz gesamt	Implementiert	HTTPS	
		Latenz beim Schreiben	Implementiert	HTTPS	
		Festplattendurchsatz beim Lesen	Implementiert	HTTPS	
		Durchsatz beim Lesen	Implementiert	HTTPS	Gesamtdurchsatz der Festplatte beim Lesen
		Festplattendurchsatz beim Schreiben	Implementiert	HTTPS	
		IP-Durchsatz beim Lesen	Implementiert	HTTPS	
		Durchsatz gesamt	Implementiert	HTTPS	IP-Durchsatz gesamt
		ipThroughput.write	Implementiert	HTTPS	
	VM	Gesamtkapazität	Implementiert	HTTPS	
		Schlüssel	Implementiert	HTTPS	
		Server-ID	Implementiert	HTTPS	

Von diesem Datensammler verwendete Verwaltungs-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschichtprotokoll	Verwendete eingehende Ports	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur schreibgeschützte Anmeldeinformationen	Unterstützt Verschlüsselung	Firewall-freundlich (statische Ports)
EC2 API	HTTPS	HTTPS	443		true	true	true	true

Amazon AWS S3

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
S3	01.08.2010

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Stiftung					
750					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

					)
		Virtuell	Implementiert	HTTPS	Ist dies ein Gerät zur Speichervirtualisierung?
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	Speicherpool	In DWH-Kapazität einschließen	Implementiert	HTTPS	Eine Möglichkeit von ACQ, zu steuern, welche Speicherpools in der DWH-Kapazität interessant sind
		Name	Implementiert	HTTPS	
		Physische Festplattenkapazität (MB)	Implementiert	HTTPS	wird als Rohkapazität für Speicherpools verwendet
		Raid-Gruppe	Implementiert	HTTPS	gibt an, ob dieser Speicherpool eine RAID-Gruppe ist
		Verhältnis von Rohmaterial zu Nutzmaterial	Implementiert	HTTPS	Verhältnis zur Umrechnung von nutzbarer Kapazität in Rohkapazität
		Speicherpool-ID	Implementiert	HTTPS	
		Thin Provisioning wird unterstützt	Implementiert	HTTPS	Ob dieses interne Volume Thin Provisioning für die darüber liegende Volume-Schicht unterstützt
		Gesamtzugewiesene Kapazität	Implementiert	HTTPS	
		Typ	Lücke	HTTPS	
		Virtuell	Implementiert	HTTPS	Ist dies ein Gerät zur Speichervirtualisierung?

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Leistung	Internes Volumen	Gesamtkapazität	Implementiert	HTTPS	
		Verwendete Kapazität	Implementiert	HTTPS	
		Verhältnis der genutzten Kapazität	Implementiert	HTTPS	
		Schlüssel	Implementiert	HTTPS	
		Objekte insgesamt	Implementiert	HTTPS	
		Server-ID	Implementiert	HTTPS	

Von diesem Datensammler verwendete Verwaltungs-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschichtprotokoll	Verwendete eingehende Ports	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur schreibgeschützte Anmeldeinformationen	Unterstützt Verschlüsselung	Firewall-freundlich (statische Ports)
S3 API	HTTPS	HTTPS	443		true	true	true	true

Microsoft Azure NetApp Files

Von diesem Datensammler unterstützte Modelle und Versionen:

API-Versionen	Modelle
2019-06-01 2024-07-01	Azure NetApp Files

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Stiftung					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Gesamte genutzte Kapazität	Implementiert	HTTPS	Gesamtkapazität in MB
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Typ	Lücke	HTTPS	
		Virtuell	Implementiert	HTTPS	Ist dies ein Gerät zur Speichervirtualisierung?
		Kommentar	Lücke	HTTPS	Status: Freitextkommentar, der das SVM beschreibt

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Leistung					

					allen Festplatten) in MB/s
Produkt	**Kategorie**	**Funktionsname**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	StoragePool-Datenträger	IOPs gelesen	Implementiert		Anzahl der gelesenen IOPs auf der Festplatte
		IOPs Schreiben	Implementiert		
		Durchsatz beim Lesen	Implementiert		
		Durchsatz beim Schreiben	Implementiert		
		Durchsatz gesamt	Implementiert		Durchschnittliche Gesamtrate der Festplatte (Lesen und Schreiben auf allen Festplatten) in MB/s
		IOPs gesamt	Implementiert		

Von diesem Datensammler verwendete Verwaltungs-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschichtprotokoll	Verwendete eingehende Ports	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur schreibgeschützte Anmeldeinformationen	Unterstützt Verschlüsselung	Firewall-freundlich (statische Ports)
Azure Netapp Files-REST-API	HTTPS	HTTPS	443		true	true	true	true

Brocade Fibre Channel Switches

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
176,51 183,0 Brocade 200E Brocade 300E Brocade 4024 Eingebettet Brocade 5000 Brocade 5100 Brocade 5300 Brocade 5480 Eingebettet Brocade 6505 Brocade 6510 Brocade 6520 Brocade Brocade Eingebettet Brocade 6548 Brocade 6558 Brocade 7800 Brocade 7810 Erweiterungsschalter Brocade 7840 Brocade DCX Brocade DCX-4S Backbone Brocade DCX8510-4 Brocade DCX8510-8 Brocade G610 Brocade G620 Brocade G630 Brocade G720 Brocade G730 Brocade M5424 Eingebettet Brocade VA-40FC Brocade X6-4 Brocade X6-8 Brocade X7-4 Brocade X7-8	v6.2.2b v6.2.2f v6.2.2g v6.4.1b v6.4.2a v6.4.3 v6.4.3d v6.4.3f3 v7.0.1 v7.0.1b v7.0.2 v7.0.2b1 v7.0.2c v7.0.2e v7.0.2e1 v7.1.0a v7.1.0b v7.2.0a v7.2.0d v7.2.1 v7.2.1c v7.2.1c1 v7.2.1d v7.3.0a v7.3.0c v7.3.1 v7.3.1c v7.3.1d v7.3.2a v7.4.0a v7.4.1 v7.4.1d v7.4.1e v7.4.2 v7.4.2a v7.4.2a4 v7.4.2c v7.4.2d v7.4.2e v7.4.2f v7.4.2g v7.4.2g_cvr_824494_01 v7.4.2h v7.4.2j1 v8.0.2c v8.0.2d v8.0.2f v8.1.0b v8.1.1a v8.1.2a v8.1.2d v8.1.2f v8.1.2g v8.1.2h v8.1.2j v8.1.2k v8.2.0 v8.2.0a v8.2.0a1 v8.2.0b v8.2.1 v8.2.1a v8.2.1c v8.2.1d v8.2.2a v8.2.2b v8.2.2c v8.2.2d v8.2.2d4 v8.2.3 v8.2.3a v8.2.3a1 v8.2.3a_cvr_855776_01 v8.2.3b v8.2.3c v8.2.3c1 v8.2.3d v8.2.3e v8.2.3e1 v8.2.3e2 v9.0.0a v9.0.1a v9.0.1b v9.0.1b4 v9.0.1c v9.0.1d v9.0.1e v9.0.1e1 v9.1.0b v9.1.1 v9.1.1a v9.1.1b v9.1.1b_lw v9.1.1c v9.1.1d v9.1.1d1 v9.1.1d2 v9.1.1d2_lw v9.1.1d5 v9.2.0a v9.2.0b v9.2.0b1_lw v9.2.0c v9.2.0c1 v9.2.1a v9.2.1a1 v9.2.2

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Stiftung					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
	Zone	Zonenname	Implementiert	SSH	
	Zonenmitglied	Typ	Lücke	SSH	
		WWN	Implementiert	SSH	
	Zoning-Funktionen	Aktive Konfiguration	Implementiert	SSH	
		Konfigurationsname	Implementiert	SSH	
		Standardmäßiges Zoning-Verhalten	Implementiert	SSH	
		WWN	Implementiert	SSH	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Leistung					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Timeout			
		Portfehler insgesamt	Implementiert	SNMP	Portfehler insgesamt
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Server-ID	Implementiert	SNMP	
		Bildrate des Datenverkehrs	Implementiert	SNMP	
		Gesamte Bildrate des Datenverkehrs	Implementiert	SNMP	
		Bildrate des Datenverkehrs	Implementiert	SNMP	
		Durchschnittliche Rahmengröße	Implementiert	SNMP	Durchschnittliche Framegröße des Datenverkehrs
		TX-Frames	Implementiert	SNMP	Durchschnittliche Framegröße des Datenverkehrs
		Rate des empfangenen Datenverkehrs	Implementiert	SNMP	
		Gesamtverkehrsrate	Implementiert	SNMP	
		Verkehrsübertragungsrate	Implementiert	SNMP	
		Nutzung des empfangenen Datenverkehrs	Implementiert	SNMP	
		Gesamtverkehrsauslastung	Implementiert	SNMP	Gesamtverkehrsauslastung
		Verkehrsübertragungsauslastung	Implementiert	SNMP	

Von diesem Datensammler verwendete Verwaltungs-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschichtprotokoll	Verwendete eingehende Ports	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur schreibgeschützte Anmeldeinformationen	Unterstützt Verschlüsselung	Firewall-freundlich (statische Ports)
Brocade SNMP	SNMP	SNMPv1, SNMPv2, SNMPv3	161		true	true	true	true
Brocade SSH	SSH	SSH	22		FALSCH	FALSCH	true	true

API	Verwendetes Protokoll	Verwendetes Transportschichtprotokoll	Verwendete eingehende Ports	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur schreibgeschützte Anmeldeinformationen	Unterstützt Verschlüsselung	Firewall-freundlich (statische Ports)
Konfiguration des Datenquellenassistenten	Manuelle Eingabe				true	true	true	true

Brocade Network Advisor HTTP

Von diesem Datensammler unterstützte Modelle und Versionen:

API-Versionen	Modelle	Firmware-Versionen
14.4.3 14.4.4	Brocade 6520 Brocade DCX 8510-4 Brocade G620 Brocade X6-8 EMC Connectrix DS-6510B	v7.3.0b v7.4.1b v8.2.3c1 v9.0.1e1

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Stiftung					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Unbekannte Konnektivität	Implementiert	HTTP/S	
		Klinge	Implementiert	HTTP/S	
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		GBIC-Typ	Implementiert	HTTP/S	
	Schalten	WWN	Implementiert	HTTP/S	
		IP	Implementiert	HTTP/S	
		Firmware-Version	Implementiert	HTTP/S	
		Hersteller	Implementiert	HTTP/S	
		Modell	Implementiert	HTTP/S	
		Name	Implementiert	HTTP/S	
		Rolle wechseln	Implementiert	HTTP/S	
		Typ	Lücke	HTTP/S	
		Seriennummer	Implementiert	HTTP/S	
		URL verwalten	Implementiert	HTTP/S	
		Zustand wechseln	Implementiert	HTTP/S	
		Schalterstatus	Implementiert	HTTP/S	
		Domänen-ID	Implementiert	HTTP/S	
		VSAN aktiviert	Implementiert	HTTP/S	
	Unbekannt	WWN	Implementiert	HTTP/S	
		Hersteller	Implementiert	HTTP/S	
		Firmware	Implementiert	HTTP/S	
		Treiber	Implementiert	HTTP/S	
		Modell	Implementiert	HTTP/S	
	WWN-Alias	Host-Aliase	Implementiert	HTTP/S	
		Objekttyp	Implementiert	HTTP/S	
		Quelle	Implementiert	HTTP/S	
		WWN	Implementiert	HTTP/S	
	Zone	Zonenname	Implementiert	HTTP/S	
	Zonenmitglied	Typ	Lücke	HTTP/S	
		WWN	Implementiert	HTTP/S	
	Zoning-Funktionen	Aktive Konfiguration	Implementiert	HTTP/S	
		Konfigurationsname	Implementiert	HTTP/S	
		WWN	Implementiert	HTTP/S	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Leistung	Hafen	BB Credit Zero übermittelt	Implementiert	HTTP/S	BB Credit Zero übermittelt
		BB Kredit Null Gesamt	Implementiert	HTTP/S	BB Kredit Null Gesamt
		BB Credit Zero Ms Übertragen	Implementiert	HTTP/S	BB Credit Zero Ms Übertragen

Von diesem Datensammler verwendete Verwaltungs-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschichtprotokoll	Verwendete eingehende Ports	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur schreibgeschützte Anmeldeinformationen	Unterstützt Verschlüsselung	Firewall-freundlich (statische Ports)
Brocade Network Advisor REST-API	HTTP/HTTPS	HTTP/HTTPS	80/443		true	true	true	true

Brocade FOS REST

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
183,0 184,0 190,0 Brocade 6505 Brocade 6510 Brocade 6520 Brocade 7810 Erweiterungsschalter Brocade 7840 Brocade DCX8510-4 Brocade DCX8510-8 Brocade G610 Brocade G620 Brocade G630 Brocade G720 Brocade G730 Brocade X6-4 Brocade X6-8 Brocade X7-4 Brocade X7-8	v8.2.2a v8.2.2d v8.2.2d4 v8.2.3 v8.2.3a v8.2.3b v8.2.3c v8.2.3c1 v8.2.3d v8.2.3e v8.2.3e1 v9.0.0b v9.0.1a v9.0.1b v9.0.1b4 v9.0.1c v9.0.1d v9.0.1e v9.0.1e1 v9.1.0b v9.1.1a v9.1.1b v9.1.1c v9.1.1c3 v9.1.1d v9.1.1d1 v9.1.1d1_lw v9.1.1d2 v9.1.1d3_cvr_861742_01 v9.2.0a v9.2.0b v9.2.0b1 v9.2.0b_cvr_857687_01 v9.2.0c v9.2.0c3 v9.2.1 v9.2.1a v9.2.1b v9.2.2

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Stiftung					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
	Zone	Zonenname	Implementiert	HTTPS	
	Zonenmitglied	Typ	Lücke	HTTPS	
		WWN	Implementiert	HTTPS	
	Zoning-Funktionen	Aktive Konfiguration	Implementiert	HTTPS	
		Konfigurationsname	Implementiert	HTTPS	
		Standardmäßiges Zoning-Verhalten	Implementiert	HTTPS	
		WWN	Implementiert	HTTPS	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Leistung					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		insgesamt			insgesamt
		Server-ID	Implementiert	HTTPS	
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Durchschnittliche Datenverkehrs	Implementiert	HTTPS	
		Gesamte Bildrate des Datenverkehrs	Implementiert	HTTPS	
		Bildrate des Datenverkehrs	Implementiert	HTTPS	
		Durchschnittliche Rahmengröße	Implementiert	HTTPS	Durchschnittliche Framegröße des Datenverkehrs
		TX-Frames	Implementiert	HTTPS	Durchschnittliche Framegröße des Datenverkehrs
		Rate des empfangenen Datenverkehrs	Implementiert	HTTPS	
		Gesamtverkehrsrate	Implementiert	HTTPS	
		Verkehrsübertragungsrate	Implementiert	HTTPS	
		Nutzung des empfangenen Datenverkehrs	Implementiert	HTTPS	
		Gesamtverkehrsauslastung	Implementiert	HTTPS	Gesamtverkehrsauslastung
		Verkehrsübertragungsauslastung	Implementiert	HTTPS	

Von diesem Datensammler verwendete Verwaltungs-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschichtprotokoll	Verwendete eingehende Ports	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur schreibgeschützte Anmeldeinformationen	Unterstützt Verschlüsselung	Firewall-freundlich (statische Ports)
Brocade FOS REST API	HTTPS		443		true	true	true	true

Cisco MDS- und Nexus Fabric-Switches

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
DS-C9124-2-K9 DS-C9124-K9 DS-C9132T-K9 DS-C9148-16P-K9 DS-C9148-32P-K9 DS-C9148-48P-K9 DS-C9148S-K9 DS-C9148T-K9 DS-C9148V-K9 DS-C9220I-K9 DS-C9222I-K9 DS-C9250I-K9 DS-C9396S-K9 DS-C9396T-K9 DS-C9396V-K9 DS-C9506 DS-C9509 DS-C9513 DS-C9706 DS-C9710 DS-C9718 DS-HP-8GFC-K9 DS-HP-FC-K9 N5K-C5548UP N5K-C5596UP N5K-C5696Q UCS-FI-6248UP UCS-FI-6296UP UCS-FI-6332 UCS-FI-6332-16UP UCS-FI-64108 UCS-FI-6454	3.3(1c) 4.1(3a) 4.2(1a) 5.0(1a) 5.0(3)N2(3.11e) 5.0(3)N2(4.01d) 5.0(3)N2(4.13i) 5.0(3)N2(4.21e) 5.0(3)N2(4.21j) 5.0(3)N2(4.21k) 5.0(3)N2(4.22c) 5.0(3)N2(4.23f) 5.0(3)N2(4.23g) 5.0(3)N2(4.34a) 5.0(8) 5.2(2d) 5.2(8) 5.2(8a) 5.2(8b) 5.2(8c) 5.2(8d) 5.2(8f) 5.2(8g) 5.2(8h) 5.2(8i) 6.2(11) 6.2(11b) 6.2(11c) 6.2(13) 6.2(13a) 6.2(15) 6.2(17) 6.2(19) 6.2(21) 6.2(23) 6.2(25) 6.2(27) 6.2(29) 6.2(31) 6.2(33) 6.2(5a) 6.2(7) 6.2(9) 6.2(9a) 6.2(9b) 7.0(3)N2(4.04e) 7.0(3)N2(4.13b) 7,0(3)N2(4,13g) 7.3(0)D1(1) 7.3(1)DY(1) 7.3(13)N1(1) 7.3(8)N1(1) 8.1(1) 8.1(1a) 8.2(1) 8.2(2) 8.3(1) 8.3(2) 8.4(1) 8.4(1a) 8.4(2) 8.4(2a) 8.4(2b) 8.4(2c) 8.4(2d) 8.4(2e) 8.4(2f) 8.5(1) 9.2(1a) 9.2(2) 9.3(1) 9.3(2) 9.3(2a) 9.3(5)I42(1b) 9,3(5)I42(1g) 9.3(5)I42(1j) 9.3(5)I42(1k) 9.3(5)I42(3f) 9.3(5)I43(4b) 9.4(1) 9.4(1a) 9.4(2) 9.4(2a) 9.4(3)

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Stiftung					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Typ	Lücke	SNMP	
		VSAN aktiviert	Implementiert	SNMP	
		WWN	Implementiert	SNMP	
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	Unbekannt	Treiber	Implementiert	SNMP	
		Firmware	Implementiert	SNMP	
		Generiert	Implementiert	SNMP	
		Hersteller	Implementiert	SNMP	
		Modell	Implementiert	SNMP	
		Name	Implementiert	SNMP	
		WWN	Implementiert	SNMP	
	WWN-Alias	Host-Aliase	Implementiert	SNMP	
		Objekttyp	Implementiert	SNMP	
		Quelle	Implementiert	SNMP	
		WWN	Implementiert	SNMP	
	Zone	Zonenname	Implementiert	SNMP	
		Zonentyp	Implementiert	SNMP	
	Zonenmitglied	Typ	Lücke	SNMP	
		WWN	Implementiert	SNMP	
	Zoning-Funktionen	Aktive Konfiguration	Implementiert	SNMP	
		Konfigurationsname	Implementiert	SNMP	
		Standardmäßiges Zoning-Verhalten	Implementiert	SNMP	
		Zusammenführungskontrolle	Implementiert	SNMP	
		WWN	Implementiert	SNMP	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Leistung					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		insgesamt			insgesamt
		Server-ID	Implementiert	SNMP	
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Durchschnittliche Datenverkehrs	Implementiert	SNMP	
		Gesamte Bildrate des Datenverkehrs	Implementiert	SNMP	
		Bildrate des Datenverkehrs	Implementiert	SNMP	
		Durchschnittliche Rahmengröße	Implementiert	SNMP	Durchschnittliche Framegröße des Datenverkehrs
		TX-Frames	Implementiert	SNMP	Durchschnittliche Framegröße des Datenverkehrs
		Rate des empfangenen Datenverkehrs	Implementiert	SNMP	
		Gesamtverkehrsrate	Implementiert	SNMP	
		Verkehrsübertragungsrate	Implementiert	SNMP	
		Nutzung des empfangenen Datenverkehrs	Implementiert	SNMP	
		Gesamtverkehrsauslastung	Implementiert	SNMP	Gesamtverkehrsauslastung
		Verkehrsübertragungsauslastung	Implementiert	SNMP	

Von diesem Datensammler verwendete Verwaltungs-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschichtprotokoll	Verwendete eingehende Ports	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur schreibgeschützte Anmeldeinformationen	Unterstützt Verschlüsselung	Firewall-freundlich (statische Ports)
Cisco SNMP	SNMP	SNMPv1 (nur Inventar), SNMPv2, SNMPv3	161		true	true	true	true

Zusammenhalt

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
C4000 Rechenknoten C4600 C5036 C5066 C6025 C6035 C6055 CX8405 PXG1 UCS-C240M5H10 Virtueller ROBO	6.8.1_u1_release-20221022_6f58ed2a 6.8.2_u1_release-20240509_a5da4644 7.1.2_u2_release-20240925_66722648 7.1.2_u3_release-20241231_bb47fe77 7.2.1_release-20241114_794eae46 7.2.2_release-20250228_63e93ccf

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Stiftung					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

					liegende Volume-Schicht unterstützt
Produkt	**Kategorie**	**Feature/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Gesamtzugewiesene Kapazität	Implementiert		
		Gesamte genutzte Kapazität	Implementiert		Gesamtkapazität in MB
		Typ	Lücke		
		Virtuell	Implementiert		Ist dies ein Gerät zur Speichervirtualisierung?
		Verschlüsselt	Implementiert		

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Leistung	Storage	Fehlgeschlagene Rohkapazität	Implementiert		
		Rohkapazität	Implementiert		
		Freie Rohkapazität	Implementiert		Rohkapazität der Ersatzfestplatten (Summe aller Ersatzfestplatten)
		Speicherpool-Kapazität	Implementiert		
		IOPs gelesen	Implementiert		Anzahl der gelesenen IOPs auf der Festplatte
		IOPs gesamt	Implementiert		
		IOPs Schreiben	Implementiert		
		Schlüssel	Implementiert		
		Latenz beim Lesen	Implementiert		
		Latenz gesamt	Implementiert		
		Latenz beim Schreiben	Implementiert		
		Server-ID	Implementiert		
		Durchsatz beim Lesen	Implementiert		
		Durchsatz gesamt	Implementiert		Durchschnittliche Gesamtrate der Festplatte (Lesen und Schreiben auf allen Festplatten) in MB/s
		Durchsatz beim Schreiben	Implementiert		
		Auslastung gesamt	Implementiert		

Von diesem Datensammler verwendete Verwaltungs-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschichtprotokoll	Verwendete eingehende Ports	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur schreibgeschützte Anmeldeinformationen	Unterstützt Verschlüsselung	Firewall-freundlich (statische Ports)
Cohesity REST API	HTTPS	HTTPS	443		true	true	true	true

EMC Celerra (SSH)

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
NSX VG8 VNX5200 VNX5300 VNX5400 VNX5500	5.5.38-1 7.1.76-4 7.1.79-8 7.1.83-2 8.1.21-266 8.1.9-155

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Stiftung					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

					Thin Provisioning für die darüber liegende
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Schicht Informationen**
		Gesamtzugewiesene Kapazität	Implementiert	SSH	
		Gesamte genutzte Kapazität	Implementiert	SSH	Gesamtkapazität in MB
		Typ	Lücke	SSH	
		Virtuell	Implementiert	SSH	Ist dies ein Gerät zur Speichervirtualisierung?

Von diesem Datensammler verwendete Verwaltungs-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschichtprotokoll	Verwendete eingehende Ports	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur schreibgeschützte Anmeldeinformationen	Unterstützt Verschlüsselung	Firewall-freundlich (statische Ports)
Celerra-Befehlszeilenschnittstelle	SSH	SSH			true	FALSCH	true	true

EMC CLARiiON (NaviCLI)

Von diesem Datensammler unterstützte Modelle und Versionen:

API-Versionen	Modelle	Firmware-Versionen
6,26 6,28 7,32 7,33	CX3-40f CX4-480 VNX5100 VNX5200 VNX5300 VNX5400 VNX5500 VNX5600 VNX5700 VNX5800 VNX7600	04.28.000.5.710 05.32.000.5.206 05.32.000.5.218 05.32.000.5.219 05.32.000.5.221 05.32.000.5.225 05.32.000.5.249 05.33.000.5.074 05.33.008.5.119 05.33.009.5.155 05.33.009.5.184 05.33.009.5.186 05.33.009.5.231 05.33.009.5.238 05.33.021.5.256 05.33.021.5.266 05.33.021.5.322 3.26.40.5.029

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Stiftung					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Speicherpool-ID	Implementiert	Befehlszeilenschnittstelle (CLI)	
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Kapazität	Implementiert	Befehlszeilenschnittstelle (CLI)	
	WWN-Alias	Host-Aliase	Implementiert	Befehlszeilenschnittstelle (CLI)	
		IP	Implementiert	Befehlszeilenschnittstelle (CLI)	
		Objekttyp	Implementiert	Befehlszeilenschnittstelle (CLI)	
		Quelle	Implementiert	Befehlszeilenschnittstelle (CLI)	
		WWN	Implementiert	Befehlszeilenschnittstelle (CLI)	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Leistung					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Teilweise blockiertes Verhältnis	Implementiert	Befehlszeilensch nittstelle (CLI)	
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Durchsatz lesen	Implementiert	Befehlszeilensch nittstelle (CLI)	
		Durchsatz gesamt	Implementiert	Befehlszeilensch nittstelle (CLI)	Durchschnittliche Gesamtrate der Festplatte (Lesen und Schreiben auf allen Festplatten) in MB/s
		Durchsatz beim Schreiben	Implementiert	Befehlszeilensch nittstelle (CLI)	

Von diesem Datensammler verwendete Verwaltungs-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschichtprotokoll	Verwendete eingehende Ports	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur schreibgeschützte Anmeldeinformationen	Unterstützt Verschlüsselung	Firewall-freundlich (statische Ports)
Navi-Befehlszeilenschnittstelle	Befehlszeilenschnittstelle (CLI)		6389,2162,2163,443(HTTPS)/80(HTTP)		true	true	true	FALSCH

EMC-Datendomäne (SSH)

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
DD VE DD2500 DD3300 DD4200 DD6300 DD6400 DD6800 DD6900 DD7200 DD9300 DD9400 DD9410 DD9500 DD9800 DD990 DD9900 DD9910	6.0.2.30-606339 6.1.2.051-633576 6.1.2.20-606786 6.2.1.30-663869 6.2.1.40-671977 6.2.1.60-686365 7.10.0.20-1023227 7.10.1.0-1042928 7.10.1.1-1049892 7.10.1.10-1068159 7.10.1.15-1078832 7.10.1.20-1090468 7.10.1.30-1105324 7.10.1.40-1126469 7.10.1.50-1146826 7.11.0.0-1035502 7.13.0.20-1082704 7.2.0.20-658029 7.2.0.60-682124 7.2.0.70-686759 7.2.0.90-692270 7.7.4.0-1017976 7.7.5.1-1040473 7.7.5.11-1046187 7.7.5.25-1078970 7.7.5.30-1091295 8.0.0.10-1097914 8.1.0.10-1127744

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Stiftung					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Verhältnis von Rohmaterial zu Nutzmaterial	Implementiert	SSH	Verhältnis zur Umrechnung von nutzbarer
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Speicherpool-ID	Implementiert	SSH	
		Thin Provisioning wird unterstützt	Implementiert	SSH	Ob dieses interne Volume Thin Provisioning für die darüber liegende Volume-Schicht unterstützt
		Gesamtzugewiesene Kapazität	Implementiert	SSH	
		Gesamte genutzte Kapazität	Implementiert	SSH	Gesamtkapazität in MB
		Typ	Lücke	SSH	
		Virtuell	Implementiert	SSH	Ist dies ein Gerät zur Speichervirtualisierung?

Von diesem Datensammler verwendete Verwaltungs-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschichtprotokoll	Verwendete eingehende Ports	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur schreibgeschützte Anmeldeinformationen	Unterstützt Verschlüsselung	Firewall-freundlich (statische Ports)
Data Domain-CLI	SSH	SSH	22		true	true	true	true

EMV ECS

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
ECS	3.6.1.3 3.6.2.1 3.7.0.0 3.7.0.3 3.7.0.4 3.7.0.6 3.8.0.1 3.8.0.2 3.8.0.3 3.8.0.4 3.8.0.5 3.8.0.6 3.8.1.1 3.8.1.2 3.8.1.3

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Stiftung					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Nutzbar in MB			
		Verwendete Auslastung in MB	Implementiert	HTTPS	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
	Speicherpool	In DWH-Kapazität einschließen	Implementiert	HTTPS	Eine Möglichkeit von ACQ, zu steuern, welche Speicherpools in der DWH-Kapazität interessant sind
		Name	Implementiert	HTTPS	
		Physische Festplattenkapazität (MB)	Implementiert	HTTPS	wird als Rohkapazität für Speicherpools verwendet
		Raid-Gruppe	Implementiert	HTTPS	gibt an, ob dieser Speicherpool eine RAID-Gruppe ist
		Verhältnis von Rohmaterial zu Nutzmaterial	Implementiert	HTTPS	Verhältnis zur Umrechnung von nutzbarer Kapazität in Rohkapazität
		Speicherpool-ID	Implementiert	HTTPS	
		Thin Provisioning wird unterstützt	Implementiert	HTTPS	Ob dieses interne Volume Thin Provisioning für die darüber liegende Volume-Schicht unterstützt
		Gesamtzugewiesene Kapazität	Implementiert	HTTPS	
		Gesamte genutzte Kapazität	Implementiert	HTTPS	Gesamtkapazität in MB
		Typ	Lücke	HTTPS	
		Virtuell	Implementiert	HTTPS	Ist dies ein Gerät zur Speichervirtualisierung?

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Leistung					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

					Schreiben auf allen Festplatten) in MB/s
Produkt	**Kategorie**	**Funktionsattribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Durchsatz beim Schreiben	Implementiert	HTTPS	
	Speicherknotendaten	IOPs gesamt	Implementiert	HTTPS	
		Schlüssel	Implementiert	HTTPS	
		Knotenkapazitätsauslastung gesamt	Implementiert	HTTPS	
		Knotenkapazitätsauslastung Nutzbar	Implementiert	HTTPS	
		Verwendete Knotenkapazitätsauslastung	Implementiert	HTTPS	
		Server-ID	Implementiert	HTTPS	
		Durchsatz beim Lesen	Implementiert	HTTPS	
		Durchsatz gesamt	Implementiert	HTTPS	Durchschnittliche Gesamtrate der Festplatte (Lesen und Schreiben auf allen Festplatten) in MB/s
		Durchsatz beim Schreiben	Implementiert	HTTPS	
	StoragePool-Datenträger	Bereitgestellte Kapazität	Implementiert	HTTPS	
		Rohkapazität	Implementiert	HTTPS	
		Gesamtkapazität	Implementiert	HTTPS	
		Verwendete Kapazität	Implementiert	HTTPS	
		Verhältnis der Überbelegungskapazität	Implementiert	HTTPS	Als Zeitreihe gemeldet
		Verhältnis der genutzten Kapazität	Implementiert	HTTPS	

Von diesem Datensammler verwendete Verwaltungs-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschichtprotokoll	Verwendete eingehende Ports	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur schreibgeschützte Anmeldeinformationen	Unterstützt Verschlüsselung	Firewall-freundlich (statische Ports)
EMC ECS REST-API	HTTPS	HTTPS	443		true	true	true	true

Dell EMC Isilon und PowerScale Rest

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
A100 A200 A2000 A300 A3000 F200 F600 F800 F900 H400 H500 H5600 H600 H700 NL410 S210 X210 X410	9.1.0.10 9.1.0.6 9.1.0.9 9.2.1.10 9.2.1.11 9.2.1.12 9.2.1.13 9.2.1.19 9.2.1.4 9.2.1.9 9.4.0.11 9.4.0.13 9.4.0.14 9.4.0.15 9.4.0.16 9.4.0.17 9.4.0.18 9.5.0.3 9.5.0.5 9.5.0.6 9.5.0.7 9.5.0.8 9.5.1.0 9.5.1.1 9.5.1.2 9.7.1.0 9.7.1.2 9.7.1.3 9.7.1.4 9.7.1.5 v8.0.0.4 v8.0.0.6 v8.0.0.7 v8.1.0.4 v8.1.2.0 v9.0.0.0

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Stiftung					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Verhältnis von Rohmaterial zu Nutzmaterial	Implementiert	HTTPS	Verhältnis zur Umrechnung von nutzbarer
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Snapshot-zugewiesene Kapazität	Lücke	HTTPS	Zugewiesene Kapazität der Snapshots in MB
		Snapshot der genutzten Kapazität	Implementiert	HTTPS	
		Speicherpool-ID	Implementiert	HTTPS	
		Thin Provisioning wird unterstützt	Implementiert	HTTPS	Ob dieses interne Volume Thin Provisioning für die darüber liegende Volume-Schicht unterstützt
		Gesamtzugewiesene Kapazität	Implementiert	HTTPS	
		Gesamte genutzte Kapazität	Implementiert	HTTPS	Gesamtkapazität in MB
		Typ	Lücke	HTTPS	
		Virtuell	Implementiert	HTTPS	Ist dies ein Gerät zur Speichervirtualisierung?

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Leistung					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Verhältnis der genutzten Kapazität			gemeldet
Produkt	**Kategorie**	**Funktionsattribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Durchsatz lesen	Implementiert	HTTPS	
		Durchsatz gesamt	Implementiert	HTTPS	Durchschnittliche Gesamtrate der Festplatte (Lesen und Schreiben auf allen Festplatten) in MB/s
		Durchsatz beim Schreiben	Implementiert	HTTPS	

Von diesem Datensammler verwendete Verwaltungs-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschichtprotokoll	Verwendete eingehende Ports	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur schreibgeschützte Anmeldeinformationen	Unterstützt Verschlüsselung	Firewall-freundlich (statische Ports)
EMC Isilon & PowerScale REST-API	HTTPS		443		true	true	true	true

Dell EMC Isilon / PowerScale (CLI)

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
A200 H400 H500 NL400 NL410 S210 Traceback (letzter Anruf zuletzt): X200 X400 X410	9.1.0.18 9.1.0.19 9.2.1.12 9.2.1.13 9.2.1.15 9.4.0.17 9.5.0.3 9.5.0.6 9.5.0.8 9.7.1.2 9.8.0.2 v7.2.0.5 v7.2.1.3 v7.2.1.6 v8.0.0.4 v8.0.0.6 v8.0.0.7 v8.0.1.1 v8.1.2.0

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Stiftung					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

					liegende Volume-Schicht unterstützt
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Gesamtzugewiesene Kapazität	Implementiert	SSH	
		Gesamte genutzte Kapazität	Implementiert	SSH	Gesamtkapazität in MB
		Typ	Lücke	SSH	
		Virtuell	Implementiert	SSH	Ist dies ein Gerät zur Speichervirtualisierung?

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Leistung					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Durchsatz beim Schreiben	Implementiert	SSH	
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	StoragePool-Datenträger	Gesamtkapazität	Implementiert	SSH	
		Verhältnis der genutzten Kapazität	Implementiert	SSH	
		Gesamtdatenkapazität	Implementiert	SSH	
		Bereitgestellte Kapazität	Implementiert	SSH	
		Verwendete Datenkapazität	Implementiert	SSH	
		Verwendete Kapazität	Implementiert	SSH	
		Rohkapazität	Implementiert	SSH	
		Verhältnis der Überbelegungskapazität	Implementiert	SSH	Als Zeitreihe gemeldet
		Snapshot der genutzten Kapazität	Implementiert	SSH	
		Snapshot-reservierte Kapazität	Implementiert	SSH	
		Snapshot-Verhältnis der genutzten Kapazität	Implementiert	SSH	Als Zeitreihe gemeldet

Von diesem Datensammler verwendete Verwaltungs-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschichtprotokoll	Verwendete eingehende Ports	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur schreibgeschützte Anmeldeinformationen	Unterstützt Verschlüsselung	Firewall-freundlich (statische Ports)
Isilon SSH	SSH	SSH	22		true	FALSCH	true	true

EMC PowerStore REST

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
PowerStore 1000T PowerStore 1200T PowerStore 3000T PowerStore 3200T PowerStore 5000T PowerStore 5200T PowerStore 9000T PowerStore 9200T	2.1.0.1 2.1.1.0 3.2.0.1 3.2.1.0 3.2.1.1 3.5.0.1 3.5.0.2 3.6.0.0 3.6.1.0 3.6.1.1 3.6.1.2 3.6.1.3 3.6.1.4 4.0.0.1 4.0.0.2 4.0.1.0

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Stiftung					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Typ	Lücke		
		Virtuell	Implementiert		Ist dies ein Gerät zur Speichervirtualisierung?
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	Volumen	Kapazität	Implementiert		Snapshot Verwendete Kapazität in MB
		Kreuzungspfad	Implementiert		
		Name	Implementiert		
		Gesamte Rohkapazität	Implementiert		Gesamte Rohkapazität (Summe aller Festplatten im Array)
		Speicherpool-ID	Implementiert		
		Thin Provisioning	Implementiert		
		Typ	Lücke		
		UUID	Implementiert		
		Verwendete Kapazität	Implementiert		
		QoS – Richtlinie	Implementiert		
	Volumenkarte	LUN	Implementiert		Name der Backend-LUN
		Maskierung erforderlich	Implementiert		
		Protokoll-Controller	Implementiert		
		Speicherport	Implementiert		
		Typ	Lücke		
	Volumenmaske	Initiator	Implementiert		
		Protokoll-Controller	Implementiert		
		Typ	Lücke		
	WWN-Alias	Host-Aliase	Implementiert		
		Objekttyp	Implementiert		
		Quelle	Implementiert		
		WWN	Implementiert		

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Leistung					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

					allen Festplatten) in MB/s
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Durchsatz beim Schreiben	Implementiert		
	Volumen	Rohkapazität	Implementiert		
		Gesamtkapazität	Implementiert		
		Verwendete Kapazität	Implementiert		
		Verhältnis der genutzten Kapazität	Implementiert		
		IOPs gelesen	Implementiert		Anzahl der gelesenen IOPs auf der Festplatte
		IOPs gesamt	Implementiert		
		IOPs Schreiben	Implementiert		
		Schlüssel	Implementiert		
		Latenz beim Lesen	Implementiert		
		Latenz gesamt	Implementiert		
		Latenz beim Schreiben	Implementiert		
		Server-ID	Implementiert		
		Durchsatz beim Lesen	Implementiert		
		Durchsatz gesamt	Implementiert		Durchschnittliche Gesamtrate der Festplatte (Lesen und Schreiben auf allen Festplatten) in MB/s
		Durchsatz beim Schreiben	Implementiert		

Von diesem Datensammler verwendete Verwaltungs-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschichtprotokoll	Verwendete eingehende Ports	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur schreibgeschützte Anmeldeinformationen	Unterstützt Verschlüsselung	Firewall-freundlich (statische Ports)
EMC PowerStore REST-API	HTTPS	HTTPS	443		true	true	true	true

EMC RecoverPoint (HTTP)

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
Wiederherstellungspunkt	5.1.SP4.P1(h.89) 5.1.SP4.P2(h.101) 5.1.SP4.P3(h.109) 5.1.SP4.P4(h.97) 5.1.SP4.P5(h.138)

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Stiftung					

					)
		Virtuell	Implementiert	HTTPS	Ist dies ein Gerät zur Speichervirtualisierung?
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	Speicherknoten	Speichergröße	Lücke	HTTPS	Gerätespeicher in MB
		Modell	Implementiert	HTTPS	
		Name	Implementiert	HTTPS	
		Anzahl der Prozessoren	Implementiert	HTTPS	Geräte-CPU
		Seriennummer	Implementiert	HTTPS	
		Status	Implementiert	HTTPS	Freitext zur Beschreibung des Gerätezustands
		UUID	Implementiert	HTTPS	
		Version	Implementiert	HTTPS	Softwareversion
	Speichersynchronisierung	Modus	Implementiert	HTTPS	
		Modus-Enumeration	Implementiert	HTTPS	
		Quellspeicher	Implementiert	HTTPS	
		Quellvolumen	Implementiert	HTTPS	
		Status	Implementiert	HTTPS	Freitext zur Beschreibung des Gerätezustands
		Statusaufzählung	Implementiert	HTTPS	
		Zielspeicher	Implementiert	HTTPS	
		Zielvolumen	Implementiert	HTTPS	
		Technologie	Implementiert	HTTPS	Technologie, die die Speichereffizienz verändert

Von diesem Datensammler verwendete Verwaltungs-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschichtprotokoll	Verwendete eingehende Ports	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur schreibgeschützte Anmeldeinformationen	Unterstützt Verschlüsselung	Firewall-freundlich (statische Ports)
RecoverPoint REST API	HTTPS	HTTPS	443		true	true	true	true

EMC ScaleIO und PowerFlex REST

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
ScaleIO	R3_5.1201.101 R3_6.1000.134

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Stiftung					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Typ	Lücke	HTTPS	
		Virtuell	Implementiert	HTTPS	Ist dies ein Gerät zur Speichervirtualisierung?
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	Volumen	Kapazität	Implementiert	HTTPS	Snapshot Verwendete Kapazität in MB
		Kreuzungspfad	Implementiert	HTTPS	
		Name	Implementiert	HTTPS	
		Gesamte Rohkapazität	Implementiert	HTTPS	Gesamte Rohkapazität (Summe aller Festplatten im Array)
		Speicherpool-ID	Implementiert	HTTPS	
		Thin Provisioning	Implementiert	HTTPS	
		UUID	Implementiert	HTTPS	
		Host-IPs	Implementiert	HTTPS	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Leistung	Storage	Fehlgeschlagene Rohkapazität	Implementiert		
		Rohkapazität	Implementiert		
		Freie Rohkapazität	Implementiert		Rohkapazität der Ersatzfestplatten (Summe aller Ersatzfestplatten)
		Speicherpool-Kapazität	Implementiert		
		IOPs gelesen	Implementiert		Anzahl der gelesenen IOPs auf der Festplatte
		IOPs gesamt	Implementiert		
		IOPs Schreiben	Implementiert		
		Schlüssel	Implementiert		
		Server-ID	Implementiert		
		Durchsatz beim Lesen	Implementiert		
		Durchsatz gesamt	Implementiert		Durchschnittliche Gesamtrate der Festplatte (Lesen und Schreiben auf allen Festplatten) in MB/s
		Durchsatz beim Schreiben	Implementiert		

Von diesem Datensammler verwendete Verwaltungs-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschichtprotokoll	Verwendete eingehende Ports	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur schreibgeschützte Anmeldeinformationen	Unterstützt Verschlüsselung	Firewall-freundlich (statische Ports)
EMC ScaleIO und PowerFlex REST API	HTTPS	HTTPS	443		true	true	true	true

EMC Symmetrix-CLI

Von diesem Datensammler unterstützte Modelle und Versionen:

API-Versionen	Modelle	Firmware-Versionen
V10.0.0.0 V10.0.1.1 V10.1.0.0 V10.1.0.1 V10.1.0.3 V10.1.0.5 V10.2.0.0 V8.3.0.6 V8.4.0.7 V8.4.0.9 V9.1.0.5 V9.1.0.6 V9.2.1.0 V9.2.2.0 V9.2.3.0 V9.2.3.1 V9.2.3.4 V9.2.3.6 V9.2.4.1 V9.2.4.2 V9.2.4.3 V9.2.4.6 V9.2.4.7 V9.2.4.8	PMax8000 PowerMax_2000 PowerMax_8000 VMAX-1 VMAX100K VMAX10K VMAX200K VMAX250F VMAX400K VMAX40K VMAX450F VMAX850F VMAX950F	5876.286.194(16F40000) Build 115 5876.309.196(16F40000) Build 153 5876.309.196(16F40000) Build 162 5876.309.196(16F40000) Build 94 5977.1151.1151(17590000) Build 45 5977.1151.1151(17590000) Build 60 5977.1151.1151(17590000) Build 9 5978.711.711(175A0000) Build 320 5978.711.711(175A0000) Baujahr 335 5978.711.711(175A0000) Baujahr 365 5978.711.711(175A0000) Baujahr 416 5978.711.711(175A0000) Baujahr 436 5978.711.711(175A0000) Baujahr 438 5978.711.711(175A0000) Baujahr 448 5978.711.711(175A0000) Baujahr 484 5978.711.711(175A0000) Baujahr 542 5978.711.711(175A0000) Baujahr 581 5978.714.714(175A0000) Baujahr 1 5978.714.714(175A0000) Baujahr 101 5978.714.714(175A0000) Baujahr 108 5978.714.714(175A0000) Baujahr 117 5978.714.714(175A0000) Baujahr 137 5978.714.714(175A0000) Baujahr 145 5978.714.714(175A0000) Baujahr 34 5978.714.714(175A0000) Baujahr 49 5978.714.714(175A0000) Build 53 5978.714.714(175A0000) Build 79

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Stiftung					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Protokoll-Controller	Implementiert		
		Speicherport	Implementiert		

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
		Typ	Lücke		
	Volume-Mitglied	Automatisches Tiering	Implementiert		gibt an, ob dieser Speicherpool am Auto-Tiering mit anderen Pools teilnimmt
		Kapazität	Implementiert		Snapshot Verwendete Kapazität in MB
		Zylinder	Implementiert		
		Name	Implementiert		
		Rang	Implementiert		
		Gesamte Rohkapazität	Implementiert		Gesamte Rohkapazität (Summe aller Festplatten im Array)
		Redundanz	Implementiert		Redundanzstufe
		Speicherpool-ID	Implementiert		
		UUID	Implementiert		
	Volumenreferenz	Name	Implementiert		
		Speicher-IP	Implementiert		
	WWN-Alias	Host-Aliase	Implementiert		
		Objekttyp	Implementiert		
		Quelle	Implementiert		
		WWN	Implementiert		

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Leistung					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Schreiben			
		Server-ID	Implementiert		
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Durchsatz beim Lesen	Implementiert		
		Durchsatz gesamt	Implementiert		Durchschnittliche Gesamtrate der Festplatte (Lesen und Schreiben auf allen Festplatten) in MB/s
		Durchsatz beim Schreiben	Implementiert		
		Schreiben ausstehend	Implementiert		insgesamt ausstehende Schreibvorgänge

Von diesem Datensammler verwendete Verwaltungs-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschichtprotokoll	Verwendete eingehende Ports	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur schreibgeschützte Anmeldeinformationen	Unterstützt Verschlüsselung	Firewall-freundlich (statische Ports)
symcli	Befehlszeilenschnittstelle (CLI)		2707		true	true	true	true
Symmetrix SMI-S	SMI-S	HTTP/HTTPS	5988/5989		true	FALSCH	FALSCH	true

Dell Unisphere REST

Von diesem Datensammler unterstützte Modelle und Versionen:

API-Versionen	Modelle	Firmware-Versionen
V10.0.0.5 V10.0.1.5 V10.1.0.1 V10.1.0.5 V10.1.0.6 V10.1.0.8 V10.2.0.1 V10.2.0.2 V9.2.3.15 V9.2.3.20 V9.2.3.22 V9.2.3.4 V9.2.4.1 V9.2.4.10 V9.2.4.11 V9.2.4.12 V9.2.4.3 V9.2.4.6 V9.2.4.7 V9.2.4.9	PowerMax_2000 PowerMax_2500 PowerMax_8000 PowerMax_8500 VMAX200K VMAX250F VMAX400K VMAX450F VMAX950F	5977.1131.1131 Bau 615 5977.1151.1151 Bau 60 Bau 60 5978.711.711 Bau 205 5978.711.711 Bau 335 Bau 335 5978.711.711 Bau 365 5978.711.711 Bau 416 5978.711.711 Bau 436 Bau 436 5978.711.711 Bau 438 5978.711.711 Bau 448 5978.711.711 Bau 471 5978.711.711 Bau 484 5978.711.711 Bau 484 Bau 484 5978.711.711 Build 542 5978.711.711 Build 542 Build 542 5978.711.711 Build 581 5978.711.711 Build 75 5978.711.711 Build 8 Build 8 5978.714.711 Build 49 5978.714.714 Build 1 Build 1 5978.714.714 Build 101 Build 101 5978.714.714 Build 108 5978.714.714 Build 117 5978.714.714 Build 117 Build 117 5978.714.714 Build 131 Build 131 5978.714.714 Build 137 5978.714.714 Build 137 Build 137 5978.714.714 Build 145 5978.714.714 Build 149 Build 149 5978.714.714 Build 34 5978.714.714 Build 49 5978.714.714 Build 49 Build 49 5978.714.714 Build 79 5978.714.714 Build 79 Build 79 6079.175.0 Build 161 Build 161 6079.175.0 Build 259 Build 259 6079.225.0 Build 127 Build 127 6079.225.0 Build 216 Build 216 6079.225.0 Build 218 Build 218 6079.225.0 Build 291 Build 291 6079.225.0 Build 331 Build 331 6079.225.0 Build 86 Build 86 6079.275.0 Build 221 Build 221

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Stiftung					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Effektiv genutzte Kapazität in Prozent	Implementiert	HTTPS	
Produkt	**Kategorie**	**Funktion/Attribut aktiviert**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Speichergruppen	Implementiert	HTTPS	
	Volumenkarte	LUN	Implementiert	HTTPS	Name der Backend-LUN
		Protokoll-Controller	Implementiert	HTTPS	
		Speicherport	Implementiert	HTTPS	
		Typ	Lücke	HTTPS	
	Volumenmaske	Initiator	Implementiert	HTTPS	
		Protokoll-Controller	Implementiert	HTTPS	
		Speicherport	Implementiert	HTTPS	
		Typ	Lücke	HTTPS	
	WWN-Alias	Host-Aliase	Implementiert	HTTPS	
		Objekttyp	Implementiert	HTTPS	
		Quelle	Implementiert	HTTPS	
		WWN	Implementiert	HTTPS	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Leistung					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

					allen Festplatten) in MB/s
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Durchsatz beim Schreiben	Implementiert	HTTPS	
	Volumen	Schlüssel	Implementiert	HTTPS	
		Server-ID	Implementiert	HTTPS	
		Durchsatz beim Lesen	Implementiert	HTTPS	
		Durchsatz beim Schreiben	Implementiert	HTTPS	
		Durchsatz gesamt	Implementiert	HTTPS	Durchschnittliche Gesamtrate der Festplatte (Lesen und Schreiben auf allen Festplatten) in MB/s
		Latenz beim Lesen	Implementiert	HTTPS	
		Latenz beim Schreiben	Implementiert	HTTPS	
		Latenz gesamt	Implementiert	HTTPS	
		IOPs gelesen	Implementiert	HTTPS	Anzahl der gelesenen IOPs auf der Festplatte
		IOPs Schreiben	Implementiert	HTTPS	
		IOPs gesamt	Implementiert	HTTPS	
		Gesamtkapazität	Implementiert	HTTPS	
		Rohkapazität	Implementiert	HTTPS	
		Verwendete Kapazität	Implementiert	HTTPS	
		Verhältnis der genutzten Kapazität	Implementiert	HTTPS	
		Gesamteinsparungen durch Komprimierung	Implementiert	HTTPS	

Von diesem Datensammler verwendete Verwaltungs-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschichtprotokoll	Verwendete eingehende Ports	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur schreibgeschützte Anmeldeinformationen	Unterstützt Verschlüsselung	Firewall-freundlich (statische Ports)
Dell Unisphere API	HTTPS	HTTPS	443		true	true	true	true

EMC VNX (SSH)

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
VNX5300 VNX5500 VNX5700	05.32.000.5.216 05.32.000.5.221 05.32.000.5.249 7.1.76-4 7.1.80-3

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Stiftung					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Speicherport	Implementiert	SSH	
		Protokoll-Controller	Implementiert	SSH	
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Typ	Lücke	SSH	
	Volumenmaske	Speicherport	Implementiert	SSH	
		Initiator	Implementiert	SSH	
		Protokoll-Controller	Implementiert	SSH	
		Typ	Lücke	SSH	
	Volume-Mitglied	Name	Implementiert	SSH	
		Speicherpool-ID	Implementiert	SSH	
		Rang	Implementiert	SSH	
		Kapazität	Implementiert	SSH	Snapshot Verwendete Kapazität in MB
		Gesamte Rohkapazität	Implementiert	SSH	Gesamte Rohkapazität (Summe aller Festplatten im Array)
		Verwendete Kapazität	Implementiert	SSH	
		Redundanz	Implementiert	SSH	Redundanzstufe
	WWN-Alias	Quelle	Implementiert	SSH	
		Host-Aliase	Implementiert	SSH	
		WWN	Implementiert	SSH	
		Objekttyp	Implementiert	SSH	
		IP	Implementiert	SSH	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Leistung					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Bereitgestellte Kapazität	Implementiert	SSH	
		Verhältnis der	Implementiert	SSH	Als Zeitreihe
Produkt	**Kategorie**	**Funktionsname**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	Volumen	Latenz gesamt	Implementiert	SSH	
		Teilweise blockiertes Verhältnis	Implementiert	SSH	
		Latenz beim Lesen	Implementiert	SSH	
		IOPs Schreiben	Implementiert	SSH	
		Durchsatz beim Lesen	Implementiert	SSH	
		IOPs gesamt	Implementiert	SSH	
		Latenz beim Schreiben	Implementiert	SSH	
		IOPs gelesen	Implementiert	SSH	Anzahl der gelesenen IOPs auf der Festplatte
		Cache-Trefferquote beim Lesen	Implementiert	SSH	
		Cache-Trefferquote gesamt	Implementiert	SSH	
		Cache-Trefferquote beim Schreiben	Implementiert	SSH	
		Durchsatz beim Schreiben	Implementiert	SSH	
		Durchsatz gesamt	Implementiert	SSH	Durchschnittliche Gesamtrate der Festplatte (Lesen und Schreiben auf allen Festplatten) in MB/s

Von diesem Datensammler verwendete Verwaltungs-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschichtprotokoll	Verwendete eingehende Ports	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur schreibgeschützte Anmeldeinformationen	Unterstützt Verschlüsselung	Firewall-freundlich (statische Ports)
VNX SSH und CLI	SSH	SSH	22		true	FALSCH	true	true

EMC VNXe und Unity Unisphere (CLI)

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
Unity 300 Unity 300F Unity 350F Unity 380 Unity 380F Unity 400 Unity 400F Unity 450F Unity 480 Unity 480F Unity 500 Unity 550F Unity 600F Unity 650F Unity 680F Unity 880 Unity 880F UnityVSA VNXe3200	3.1.17.10229825 4.1.2.9257522 5.0.6.0.5.008 5.0.8.0.5.007 5.1.2.0.5.007 5.2.1.0.5.013 5.2.2.0.5.004 5.3.0.0.5.120 5.3.1.0.5.008 5.3.1.0.6.028 5.4.0.0.5.094 5.4.1.0.5.006

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Stiftung					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Zielvolumen	Implementiert	HTTPS	
		Technologie	Implementiert	HTTPS	Technologie, die die
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	Volumen	Kapazität	Implementiert	HTTPS	Snapshot Verwendete Kapazität in MB
		Kreuzungspfad	Implementiert	HTTPS	
		Name	Implementiert	HTTPS	
		Gesamte Rohkapazität	Implementiert	HTTPS	Gesamte Rohkapazität (Summe aller Festplatten im Array)
		Speicherpool-ID	Implementiert	HTTPS	
		Thin Provisioning	Implementiert	HTTPS	
		UUID	Implementiert	HTTPS	
		Verwendete Kapazität	Implementiert	HTTPS	
	Volumenkarte	LUN	Implementiert	HTTPS	Name der Backend-LUN
		Protokoll-Controller	Implementiert	HTTPS	
		Speicherport	Implementiert	HTTPS	
		Typ	Lücke	HTTPS	
	Volumenmaske	Initiator	Implementiert	HTTPS	
		Protokoll-Controller	Implementiert	HTTPS	
		Speicherport	Implementiert	HTTPS	
		Typ	Lücke	HTTPS	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Leistung					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

					allen Festplatten) in MB/s
Produkt	**Kategorie**	**Funktionsattribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	Volumen	Rohkapazität	Implementiert	HTTPS	
		Gesamtkapazität	Implementiert	HTTPS	
		Verwendete Kapazität	Implementiert	HTTPS	
		Verhältnis der genutzten Kapazität	Implementiert	HTTPS	
		IOPs gelesen	Implementiert	HTTPS	Anzahl der gelesenen IOPs auf der Festplatte
		IOPs gesamt	Implementiert	HTTPS	
		IOPs Schreiben	Implementiert	HTTPS	
		Latenz gesamt	Implementiert	HTTPS	
		Durchsatz beim Lesen	Implementiert	HTTPS	
		Durchsatz gesamt	Implementiert	HTTPS	Durchschnittliche Gesamtrate der Festplatte (Lesen und Schreiben auf allen Festplatten) in MB/s
		Durchsatz beim Schreiben	Implementiert	HTTPS	

Von diesem Datensammler verwendete Verwaltungs-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschichtprotokoll	Verwendete eingehende Ports	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur schreibgeschützte Anmeldeinformationen	Unterstützt Verschlüsselung	Firewall-freundlich (statische Ports)
VNXe und Unisphere CLI	HTTPS	HTTPS	443		true	true	true	true

EMC VPLEX

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
VPLEX	6.2.0.04.00.07 6.2.0.07.00.02 6.2.1.0.0.519

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Stiftung					
980					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Gesamte genutzte Kapazität	Implementiert	HTTP/S	Gesamtkapazität in MB
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Typ	Lücke	HTTP/S	
		Virtuell	Implementiert	HTTP/S	Ist dies ein Gerät zur Speichervirtualisierung?
	Volumen	Kapazität	Implementiert	HTTP/S	Snapshot Verwendete Kapazität in MB
		Name	Implementiert	HTTP/S	
		Gesamte Rohkapazität	Implementiert	HTTP/S	Gesamte Rohkapazität (Summe aller Festplatten im Array)
		Redundanz	Implementiert	HTTP/S	Redundanzstufe
		Speicherpool-ID	Implementiert	HTTP/S	
		Thin Provisioning	Implementiert	HTTP/S	
		UUID	Implementiert	HTTP/S	
		Virtuell	Implementiert	HTTP/S	Ist dies ein Gerät zur Speichervirtualisierung?
	Volumenkarte	LUN	Implementiert	HTTP/S	Name der Backend-LUN
		Protokoll-Controller	Implementiert	HTTP/S	
		Speicherport	Implementiert	HTTP/S	
		Typ	Lücke	HTTP/S	
	Volumenmaske	Initiator	Implementiert	HTTP/S	
		Protokoll-Controller	Implementiert	HTTP/S	
		Speicherport	Implementiert	HTTP/S	
		Typ	Lücke	HTTP/S	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Leistung					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

					Schreiben auf allen Festplatten) in MB/s
Produkt	**Kategorie**	**Funktionsname/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	Volumen	Rohkapazität	Implementiert	SSH	
		Gesamtkapazität	Implementiert	SSH	
		IOPs gesamt	Implementiert	SSH	
		Schlüssel	Implementiert	SSH	
		Latenz beim Lesen	Implementiert	SSH	
		Latenz gesamt	Implementiert	SSH	
		Latenz beim Schreiben	Implementiert	SSH	
		Server-ID	Implementiert	SSH	
		Durchsatz beim Lesen	Implementiert	SSH	
		Durchsatz gesamt	Implementiert	SSH	Durchschnittliche Gesamtrate der Festplatte (Lesen und Schreiben auf allen Festplatten) in MB/s
		Durchsatz beim Schreiben	Implementiert	SSH	

Von diesem Datensammler verwendete Verwaltungs-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschichtprotokoll	Verwendete eingehende Ports	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur schreibgeschützte Anmeldeinformationen	Unterstützt Verschlüsselung	Firewall-freundlich (statische Ports)
EMC VPLEX CLI	SSH	SSH	22		true	true	true	true
EMC VPLEX-API	HTTP/HTTPS	HTTP/HTTPS	80/443		true	true	true	true

EMC XtremIO (HTTP)

Von diesem Datensammler unterstützte Modelle und Versionen:

API-Versionen	Modelle	Firmware-Versionen
6.2.1 6.3.2 6.3.3 6.4.0 6.4.1 6.4.2	1 Brick & 125 TB 1 Brick & 24 TB 1 Brick & 31 TB 1 Brick & 8 TB 1 x 10 TB 1 x 20 TB 1 x 40 TB 2 Bricks & 83 TB 3 Bricks & 146 TB 3 Bricks & 251 TB 3 Bricks & 283 TB 4 Bricks & 628 TB 4 Bricks & 754 TB 4 x 20 TB 6 x 40 TB	4.0.27-1 4.0.31-11 6.3.3-8_X2 6.4.0-36_hotfix_2_X2

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Stiftung					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Zielvolumen	Implementiert	HTTPS	
		Technologie	Implementiert	HTTPS	Technologie, die die Speichereffizienz verwendet
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	Volumen	Kapazität	Implementiert	HTTPS	Snapshot Verwendete Kapazität in MB
		Festplattengröße	Implementiert	HTTPS	durch Kommas getrennte Liste der Festplattengrößen (GB)
		Festplattengeschwindigkeit	Implementiert	HTTPS	durch Kommas getrennte Liste der Festplattengeschwindigkeiten (U/min)
		Datenträgertyp	Nicht verfügbar	HTTPS	
		Name	Implementiert	HTTPS	
		Gesamte Rohkapazität	Implementiert	HTTPS	Gesamte Rohkapazität (Summe aller Festplatten im Array)
		Redundanz	Implementiert	HTTPS	Redundanzstufe
		Speicherpool-ID	Implementiert	HTTPS	
		Thin Provisioning	Implementiert	HTTPS	
		Typ	Lücke	HTTPS	
		UUID	Implementiert	HTTPS	
		Verwendete Kapazität	Implementiert	HTTPS	
		Virtuell	Implementiert	HTTPS	Ist dies ein Gerät zur Speichervirtualisierung?
	Volumenkarte	LUN	Implementiert	HTTPS	Name der Backend-LUN
		Protokoll-Controller	Implementiert	HTTPS	
		Typ	Lücke	HTTPS	
	Volumenmaske	Initiator	Implementiert	HTTPS	
		Protokoll-Controller	Implementiert	HTTPS	
		Typ	Lücke	HTTPS	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Leistung					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

					allen Festplatten) in MB/s
Produkt	**Kategorie**	**Funktionsname**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	Volumen	Durchsatz beim Schreiben	Implementiert	HTTPS	
		Rohkapazität	Implementiert	HTTPS	
		Gesamtkapazität	Implementiert	HTTPS	
		Verwendete Kapazität	Implementiert	HTTPS	
		Verhältnis der genutzten Kapazität	Implementiert	HTTPS	
		IOPs gelesen	Implementiert	HTTPS	Anzahl der gelesenen IOPs auf der Festplatte
		IOPs gesamt	Implementiert	HTTPS	
		IOPs Schreiben	Implementiert	HTTPS	
		Schlüssel	Implementiert	HTTPS	
		Latenz beim Lesen	Implementiert	HTTPS	
		Latenz gesamt	Implementiert	HTTPS	
		Latenz beim Schreiben	Implementiert	HTTPS	
		Teilweise blockiertes Verhältnis	Implementiert	HTTPS	
		Server-ID	Implementiert	HTTPS	
		Durchsatz beim Lesen	Implementiert	HTTPS	
		Durchsatz gesamt	Implementiert	HTTPS	Durchschnittliche Gesamtrate der Festplatte (Lesen und Schreiben auf allen Festplatten) in MB/s
		Durchsatz beim Schreiben	Implementiert	HTTPS	

Von diesem Datensammler verwendete Verwaltungs-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschichtprotokoll	Verwendete eingehende Ports	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur schreibgeschützte Anmeldeinformationen	Unterstützt Verschlüsselung	Firewall-freundlich (statische Ports)
EMC XtremIO REST-API	HTTPS	HTTPS	443		true	true	true	true

NetApp E-Serie

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
2660 2680 2702 2704 2800B 2804 2806 3000 4000 5486 5488 5504 5564 5600 5700 5700B 6000 7999	08.40.60.01 08.80.00.00 7.84.46.0 8.20.16.0 8.20.27.0 8.20.30.0 8.20.8.0 8.25.14.0 8.25.6.0 8.40.0.1 8.40.20.0 8.40.30.4 8.40.40.0 8.40.50.0 8.40.60.1 8.40.60.2 8.40.60.3 8.42.30.5 8.50.0.4 8.51.0.0 8.52.0.0 8.52.0.1 8.53.0.1 8.53.0.4 8.62.0.0 8.62.0.2 8.63.0.2 8.70.0.2 8.70.0.3 8.71.2.0 8.71.3.0 8.72.0.0 8.73.0.0 8.74.0.0 8.74.1.0 8.74.2.0 8.74.3.0 8.75.0.0 8.75.0.1 8.75.1.0 8.80.0.0 8.80.1.0 8.81.0.3 8.81.1.0 8.81.2.0 8.81.3.0 8.90.0.0

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Stiftung					
1002					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Typ	Lücke	RMI	
		Virtuell	Implementiert	RMI	Ist dies ein Gerät zur Speichervirtualisierung?
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	Volumen	Kapazität	Implementiert	RMI	Snapshot Verwendete Kapazität in MB
		Datenträgertyp	Nicht verfügbar	RMI	
		Name	Implementiert	RMI	
		Gesamte Rohkapazität	Implementiert	RMI	Gesamte Rohkapazität (Summe aller Festplatten im Array)
		Redundanz	Implementiert	RMI	Redundanzstufe
		Speicherpool-ID	Implementiert	RMI	
		Thin Provisioning	Implementiert	RMI	
		Typ	Lücke	RMI	
		UUID	Implementiert	RMI	
		Verwendete Kapazität	Implementiert	RMI	
		Virtuell	Implementiert	RMI	Ist dies ein Gerät zur Speichervirtualisierung?
		Schriftliche Kapazität	Implementiert	RMI	Gesamtkapazität, die von einem Host auf dieses Volume geschrieben wurde, in MB
	Volumenkarte	LUN	Implementiert	RMI	Name der Backend-LUN
		Speicherport	Implementiert	RMI	
		Typ	Lücke	RMI	
	Volumenmaske	Initiator	Implementiert	RMI	
		Speicherport	Implementiert	RMI	
		Typ	Lücke	RMI	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Leistung					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

					Festplatte (Lesen und Schreiben auf allen Festplatten)
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Durchsatz beim Schreiben	Implementiert	RMI	

Von diesem Datensammler verwendete Verwaltungs-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschichtprotokoll	Verwendete eingehende Ports	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur schreibgeschützte Anmeldeinformationen	Unterstützt Verschlüsselung	Firewall-freundlich (statische Ports)
SANtricity API	RMI	TCP			true	true	FALSCH	FALSCH

Pure Storage FlashBlade REST

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
FlashBlade FlashBlade//S200	Reinheit//FB 4.1.5 Reinheit//FB 4.3.0 Reinheit//FB 4.3.11 Reinheit//FB 4.3.6 Reinheit//FB 4.4.3

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Stiftung					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Snapshot der genutzten Kapazität	Implementiert	HTTPS	
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Speicherpool-ID	Implementiert	HTTPS	
		Thin Provisioning wird unterstützt	Implementiert	HTTPS	Ob dieses interne Volume Thin Provisioning für die darüber liegende Volume-Schicht unterstützt
		Gesamtzugewiesene Kapazität	Implementiert	HTTPS	
		Gesamte genutzte Kapazität	Implementiert	HTTPS	Gesamtkapazität in MB
		Typ	Lücke	HTTPS	
		Virtuell	Implementiert	HTTPS	Ist dies ein Gerät zur Speichervirtualisierung?

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Leistung					
1024					

		Verhältnis der genutzten Kapazität			gemeldet
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Gesamteinsparungen durch Komprimierung	Implementiert	HTTPS	
	Storage	Fehlgeschlagene Rohkapazität	Implementiert	HTTPS	
		Rohkapazität	Implementiert	HTTPS	
		Freie Rohkapazität	Implementiert	HTTPS	Rohkapazität der Ersatzfestplatten (Summe aller Ersatzfestplatten)
		Speicherpool-Kapazität	Implementiert	HTTPS	
		IOPs andere	Implementiert	HTTPS	
		IOPs gelesen	Implementiert	HTTPS	Anzahl der gelesenen IOPs auf der Festplatte
		IOPs gesamt	Implementiert	HTTPS	
		IOPs Schreiben	Implementiert	HTTPS	
		Schlüssel	Implementiert	HTTPS	
		Latenz beim Lesen	Implementiert	HTTPS	
		Latenz gesamt	Implementiert	HTTPS	
		Latenz beim Schreiben	Implementiert	HTTPS	
		Server-ID	Implementiert	HTTPS	
		Durchsatz beim Lesen	Implementiert	HTTPS	
		Durchsatz gesamt	Implementiert	HTTPS	Durchschnittliche Gesamtrate der Festplatte (Lesen und Schreiben auf allen Festplatten) in MB/s
		Durchsatz beim Schreiben	Implementiert	HTTPS	

Von diesem Datensammler verwendete Verwaltungs-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschichtprotokoll	Verwendete eingehende Ports	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur schreibgeschützte Anmeldeinformationen	Unterstützt Verschlüsselung	Firewall-freundlich (statische Ports)
Pure Storage FlashBlade-API	HTTPS	HTTPS	443		true	true	true	true

Google Cloud Compute

Von diesem Datensammler unterstützte Modelle und Versionen: API-Versionen:

- v1

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Stiftung					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Hersteller	Implementiert	HTTPS	
		Name	Implementiert	HTTPS	
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		OID	Implementiert	HTTPS	
	Info	API-Beschreibung	Implementiert	HTTPS	
		API-Name	Implementiert	HTTPS	
		API-Version	Implementiert	HTTPS	
		Datenquellenname	Implementiert	HTTPS	Info
		Datum	Implementiert	HTTPS	
		Absender-ID	Implementiert	HTTPS	
		Urheberschlüssel	Implementiert	HTTPS	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Leistung					
1030					

		Gesamt-Swapsatz			
		Wartezeit	Implementiert	HTTPS	Wartezeit auf die Platte in Millisekunden
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	VM	Gesamtkapazität	Implementiert	HTTPS	
		Verhältnis der genutzten Kapazität	Implementiert	HTTPS	
		Schlüssel	Implementiert	HTTPS	
		Server-ID	Implementiert	HTTPS	

Von diesem Datensammler verwendete Verwaltungs-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschichtprotokoll	Verwendete eingehende Ports	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur schreibgeschützte Anmeldeinformationen	Unterstützt Verschlüsselung	Firewall-freundlich (statische Ports)
Google Compute Platform REST API	HTTPS		443		true	true	true	true

Google Cloud Netapp Volumes

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Stiftung					
1032					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Zugewiesene Datenkapazität	Lücke	HTTPS	für Daten zugewiesene Kapazität
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Gesamtzugewiesene Kapazität	Implementiert	HTTPS	
		Physische Festplattenkapazität (MB)	Implementiert	HTTPS	wird als Rohkapazität für Speicherpools verwendet
		Verhältnis von Rohmaterial zu Nutzmaterial	Implementiert	HTTPS	Verhältnis zur Umrechnung von nutzbarer Kapazität in Rohkapazität
			Implementiert	HTTPS	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Leistung					
1038					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

					(Lesen und Schreiben auf allen Festplatten) in MB/s
Produkt	**Kategorie**	**Funktion/Attribut-Schlüssel**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Cluster	Implementiert	HTTPS	
	StoragePool-Datenträger	Verwendeter Objektspeicherplatz	Implementiert	HTTPS	
		Gesamtkapazität	Implementiert	HTTPS	
		IOPs Schreiben	Implementiert	HTTPS	
		Verwendete Kapazität	Implementiert	HTTPS	
		Rohkapazität	Implementiert	HTTPS	
		Durchsatz beim Lesen	Implementiert	HTTPS	
		IOPs gesamt	Implementiert	HTTPS	
		IOPs gelesen	Implementiert	HTTPS	Anzahl der gelesenen IOPs auf der Festplatte
		Verhältnis der genutzten Kapazität	Implementiert	HTTPS	
		Gesamtdatenkapazität	Implementiert	HTTPS	
		Bereitgestellte Kapazität	Implementiert	HTTPS	
		Verwendete Datenkapazität	Implementiert	HTTPS	
		Durchsatz beim Schreiben	Implementiert	HTTPS	
		Durchsatz gesamt	Implementiert	HTTPS	Durchschnittliche Gesamtrate der Festplatte (Lesen und Schreiben auf allen Festplatten) in MB/s
		Verhältnis der Überbelegungskapazität	Implementiert	HTTPS	Als Zeitreihe gemeldet

Von diesem Datensammler verwendete Verwaltungs-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschichtprotokoll	Verwendete eingehende Ports	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur schreibgeschützte Anmeldeinformationen	Unterstützt Verschlüsselung	Firewall-freundlich (statische Ports)
Google Compute Platform REST API	HTTPS		443		true	true	true	true

HDS HCP (HTTPS)

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
Hitachi Content Platform	9.6.2.37 9.6.3.33 9.7.2.27 9.7.3.14

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Stiftung					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Gesamte genutzte Kapazität	Implementiert	HTTPS	Gesamtkapazität in MB
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Typ	Lücke	HTTPS	
		Virtuell	Implementiert	HTTPS	Ist dies ein Gerät zur Speichervirtualisierung?
Leistung	Storage	Fehlgeschlagene Rohkapazität	Implementiert		
		Rohkapazität	Implementiert		
		Freie Rohkapazität	Implementiert		Rohkapazität der Ersatzfestplatten (Summe aller Ersatzfestplatten)
		Speicherpool-Kapazität	Implementiert		
		Schlüssel	Implementiert		
		Server-ID	Implementiert		
	Speicherknotendaten	Schlüssel	Implementiert		
		Server-ID	Implementiert		
		Durchsatz beim Lesen	Implementiert		
		Durchsatz gesamt	Implementiert		Durchschnittliche Gesamtrate der Festplatte (Lesen und Schreiben auf allen Festplatten) in MB/s
		Durchsatz beim Schreiben	Implementiert		
		Auslastung gesamt	Implementiert		

Von diesem Datensammler verwendete Verwaltungs-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschichtprotokoll	Verwendete eingehende Ports	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur schreibgeschützte Anmeldeinformationen	Unterstützt Verschlüsselung	Firewall-freundlich (statische Ports)
HDS HCP REST API	HTTPS	HTTPS	9090		true	true	true	true

HiCommand-Gerätemanager

Von diesem Datensammler unterstützte Modelle und Versionen:

API-Versionen	Modelle	Firmware-Versionen
7.6.1 8.0 8.7.1 8.7.3 8.7.6 8.8.3	DF850MH DF850S HM800 HM850 P9500 RAID800 VSP5000 XP24000 XP8	0983/AH 0984/BH 0985/BS 0986/AH 0988/HS DKC:60-08-22 DKC:60-08-65 DKC:70-06-43 DKC:80-06-80-00/02 DKC:80-06-91-00/00 DKC:80-06-96-00/00 DKC:83-05-46-60/00 DKC:83-05-50-60/00 DKC:83-05-53-60/00 DKC:88-08-08-60/00 DKC:88-08-10-60/00 DKC:88-08-12-60/00 DKC:88-08-13-60/00 DKC:88-08-13-60/01 DKC:90-08-81-00/00 DKC:90-09-21-00/00 DKC:90-09-23-00/00 DKC:90-09-24-00/00 DKC:90-09-24-00/01 DKC:90-09-25 SVP:60-08-21/00 SVP:60-08-54/00 SVP:70-06-30/00 SVP:80-06-76/02 SVP:80-06-86/00 SVP:80-06-91/00 SVP:83-05-50-60/00 SVP:83-05-54-60/00 SVP:83-05-57-60/00 SVP:88-08-10-60/00 SVP:88-08-12-60/00 SVP:88-08-14-60/00 SVP:88-08-15-60/00 SVP:90-08-81/00 SVP:90-09-21/00 SVP:90-09-23/00 SVP:90-09-24/00 SVP:90-09-25/00

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Stiftung					
1048					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Thin Provisioning	Implementiert	HDS XML API	
		Typ	Lücke	HDS XML API	
Produkt	**Kategorie**	**Funktionsattribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Verwendete Kapazität	Implementiert	HDS XML API	
	Volumenkarte	LUN	Implementiert	HDS XML API	Name der Backend-LUN
		Maskierung erforderlich	Implementiert	HDS XML API	
		Protokoll-Controller	Implementiert	HDS XML API	
		Speicherport	Implementiert	HDS XML API	
	Volumenmaske	Initiator	Implementiert	HDS XML API	
		Protokoll-Controller	Implementiert	HDS XML API	
		Speicherport	Implementiert	HDS XML API	
	Volume-Mitglied	Kapazität	Implementiert	HDS XML API	Snapshot Verwendete Kapazität in MB
		Zylinder	Implementiert	HDS XML API	
		Name	Implementiert	HDS XML API	
		Rang	Implementiert	HDS XML API	
		Gesamte Rohkapazität	Implementiert	HDS XML API	Gesamte Rohkapazität (Summe aller Festplatten im Array)
		Speicherpool-ID	Implementiert	HDS XML API	
		Verwendete Kapazität	Implementiert	HDS XML API	
	WWN-Alias	Host-Aliase	Implementiert	HDS XML API	
		Objekttyp	Implementiert	HDS XML API	
		Quelle	Implementiert	HDS XML API	
		WWN	Implementiert	HDS XML API	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Leistung					
1056					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Verwendete Kapazität	Implementiert	Export/CLI	
		Verhältnis der genutzten Kapazität	Implementiert	Export/CLI	
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	Volumen	Schlüssel	Implementiert	Export/CLI	
		Server-ID	Implementiert	Export/CLI	
		Gesamtkapazität	Implementiert	Export/CLI	
		Rohkapazität	Implementiert	Export/CLI	
		Verwendete Kapazität	Implementiert	Export/CLI	
		Verhältnis der genutzten Kapazität	Implementiert	Export/CLI	

Von diesem Datensammler verwendete Verwaltungs-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschichtprotokoll	Verwendete eingehende Ports	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur schreibgeschützte Anmeldeinformationen	Unterstützt Verschlüsselung	Firewall-freundlich (statische Ports)
Export-Dienstprogramm (USPV) / SNM CLI (AMS)	Export/CLI				FALSCH	FALSCH	FALSCH	FALSCH
HiCommand Device Manager XML API	HDS XML API	HTTP/HTTPS	2001		true	true	true	true

Hitachi Ops Center

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
VSP 5100 VSP 5500 VSP 5600 VSP 5600H VSP E1090 VSP E590 VSP E790 VSP E790H VSP F1500 VSP F400 VSP F900 VSP G1000 VSP G1500 VSP G600 VSP G800 VSP G900 XP8	80-06-91-00/00:01-71-03/02 80-06-94-00/00:01-70-03/04 80-06-96-00/00:01-71-03/02 80-06-96-00/00:01-76-03/03 83-05-49-40/01:01-69-03/02 83-05-49-60/01:01-65-03/05 83-05-49-60/01:01-69-03/02 83-05-51-40/00:01-70-03/04 83-05-51-40/00:01-71-03/02 83-05-51-40/00:01-76-03/03 88-08-08-60/00:01-65-03/05 88-08-08-60/00:01-70-03/04 88-08-11-60/00:01-65-03/05 88-08-11-60/00:01-70-03/04 88-08-13-60/00:01-65-03/05 88-08-13-60/01:01-65-03/05 88-08-13-60/01:01-70-03/04 88-08-13-60/01:01-71-03/02 88-08-13-60/01:01-76-03/03 90-08-82-00/00:01-65-03/05 90-08-82:01.70.04 90-09-01-00/01:01-65-03/05 90-09-22-00/00:01-65-03/05 90-09-22-00/00:01-70-03/04 90-09-22-00/00:01-71-03/02 90-09-24-00/01:01-65-03/05 90-09-24-00/01:01-71-03/02 90-09-24-00/01:01-76-03/03 90-09-24:01.65.05 90-09-25-00/00:01-76-03/03 90-09-25:01.70.04 90-09-26-00/00:01-65-03/05 90-09-26-00/00:01-71-03/02 90-09-26-00/00:01-76-03/03 93-07-01-80/00:01-70-03/04 93-07-22-40/00:01-65-03/05 93-07-22-40/00:01-69-03/02 93-07-22-80/00:01-70-03/04 93-07-22-80/00:01-71-03/02 93-07-23-80/00:01-71-03/02 93-07-23-80/01:01-71-03/02 93-07-24-40/00:01-76-03/03 93-07-24-80/00:01-70-03/04 null:null

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Stiftung					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Zielvolumen	Implementiert		
		Technologie	Implementiert		Technologie, die die
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	Volumen	Kapazität	Implementiert		Snapshot Verwendete Kapazität in MB
		Kreuzungspfad	Implementiert		
		Name	Implementiert		
		Schutzart	Implementiert		
		Gesamte Rohkapazität	Implementiert		Gesamte Rohkapazität (Summe aller Festplatten im Array)
		Speicherpool-ID	Implementiert		
		Thin Provisioning	Implementiert		
		Typ	Lücke		
		Verwendete Kapazität	Implementiert		
		Komprimierung aktiviert	Implementiert		
	Volumenkarte	LUN	Implementiert		Name der Backend-LUN
		Maskierung erforderlich	Implementiert		
		Protokoll-Controller	Implementiert		
		Speicherport	Implementiert		
		Typ	Lücke		
	Volumenmaske	Initiator	Implementiert		
		Protokoll-Controller	Implementiert		
		Speicherport	Implementiert		
		Typ	Lücke		

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Leistung					
1070					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

					Festplatte (Lesen und Schreiben auf allen Festplatten) in MB/s
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	Volumen	Cache-Trefferquote beim Lesen	Implementiert		
		Cache-Trefferquote gesamt	Implementiert		
		IOPs gelesen	Implementiert		Anzahl der gelesenen IOPs auf der Festplatte
		IOPs gesamt	Implementiert		
		IOPs Schreiben	Implementiert		
		Schlüssel	Implementiert		
		Latenz beim Lesen	Implementiert		
		Latenz gesamt	Implementiert		
		Latenz beim Schreiben	Implementiert		
		Server-ID	Implementiert		
		Durchsatz beim Lesen	Implementiert		
		Durchsatz gesamt	Implementiert		Durchschnittliche Gesamtrate der Festplatte (Lesen und Schreiben auf allen Festplatten) in MB/s
		Durchsatz beim Schreiben	Implementiert		

Von diesem Datensammler verwendete Verwaltungs-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschichtprotokoll	Verwendete eingehende Ports	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur schreibgeschützte Anmeldeinformationen	Unterstützt Verschlüsselung	Firewall-freundlich (statische Ports)
Hitachi Ops Center REST-API	HTTPS	HTTPS	443		true	true	true	true

HDS HNAS (CLI)

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
Datei 34 G600 G800 HNAS 4060 HNAS 4080 HNAS 4100 N800	14.6.7520.04 14.7.7623.07 14.9.7916.07 15.1.8030.03 15.1.8030.05 15.2.8128.05 15.2.8128.07 15.2.8128.09 15.3.8224.02

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Stiftung					
1078					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

					des Gerätezustands
		UUID	Implementiert	SSH	
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Version	Implementiert	SSH	Softwareversion
	Speicherpool	Verwendete Datenkapazität	Implementiert	SSH	
		Deduplizierung aktiviert	Implementiert	SSH	Ist die Deduplizierung im Speicherpool aktiviert?
		In DWH-Kapazität einschließen	Implementiert	SSH	Eine Möglichkeit von ACQ, zu steuern, welche Speicherpools in der DWH-Kapazität interessant sind
		Name	Implementiert	SSH	
		Raid-Gruppe	Implementiert	SSH	gibt an, ob dieser Speicherpool eine RAID-Gruppe ist
		Verhältnis von Rohmaterial zu Nutzmaterial	Implementiert	SSH	Verhältnis zur Umrechnung von nutzbarer Kapazität in Rohkapazität
		Snapshot der genutzten Kapazität	Implementiert	SSH	
		Speicherpool-ID	Implementiert	SSH	
		Thin Provisioning wird unterstützt	Implementiert	SSH	Ob dieses interne Volume Thin Provisioning für die darüber liegende Volume-Schicht unterstützt
		Gesamtzugewiesene Kapazität	Implementiert	SSH	
		Gesamte genutzte Kapazität	Implementiert	SSH	Gesamtkapazität in MB
		Typ	Lücke	SSH	
		Virtuell	Implementiert	SSH	Ist dies ein Gerät zur Speichervirtualisierung?

Von diesem Datensammler verwendete Verwaltungs-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschichtprotokoll	Verwendete eingehende Ports	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur schreibgeschützte Anmeldeinformationen	Unterstützt Verschlüsselung	Firewall-freundlich (statische Ports)
HDS HNAS CLI	SSH	SSH	22		true	true	true	true

HPE Nimble / Alletra 6000 Storage

Von diesem Datensammler unterstützte Modelle und Versionen:

API-Versionen	Modelle	Firmware-Versionen
v1	5050 6070 AF1000 AF20Q AF40 AF60 AF80 CS1000 CS300 CS3000 CS500 HF20 HF20C HF20H HF40 HF60	5.0.8.0-677726-opt 5.2.1.1100-1027043-opt 5.2.1.400-796142-opt 5.2.1.700-882343-opt 5.2.1.800-930936-opt 6.0.0.400-991061-opt 6.0.0.500-1005932-opt 6.1.1.200-1020304-opt 6.1.1.300-1028597-opt 6.1.2.300-1042680-opt 6.1.2.400-1048557-opt 6.1.2.500-1053701-opt 6.1.2.502-1057650-opt 6.1.2.600-1064273-opt

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Stiftung					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

					erung?
		Komprimierung aktiviert	Implementiert	HTTPS	
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Verschlüsselt	Implementiert	HTTPS	
	Volumenkarte	LUN	Implementiert	HTTPS	Name der Backend-LUN
		Maskierung erforderlich	Implementiert	HTTPS	
		Protokoll-Controller	Implementiert	HTTPS	
		Speicherport	Implementiert	HTTPS	
		Typ	Lücke	HTTPS	
	Volumenmaske	Initiator	Implementiert	HTTPS	
		Protokoll-Controller	Implementiert	HTTPS	
		Speicherport	Implementiert	HTTPS	
		Typ	Lücke	HTTPS	
	WWN-Alias	Host-Aliase	Implementiert	HTTPS	
		Objekttyp	Implementiert	HTTPS	
		Quelle	Implementiert	HTTPS	
		WWN	Implementiert	HTTPS	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Leistung					
1094					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

					allen Festplatten) in MB/s
Produkt	**Kategorie**	**Funktionsattribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	Volumen	Durchsatz beim Schreiben	Implementiert	HTTPS	
		Rohkapazität	Implementiert	HTTPS	
		Gesamtkapazität	Implementiert	HTTPS	
		Verwendete Kapazität	Implementiert	HTTPS	
		Verhältnis der genutzten Kapazität	Implementiert	HTTPS	
		Gesamteinsparungen durch Komprimierung	Implementiert	HTTPS	
		Komprimierung spart Platz	Implementiert	HTTPS	
		IOPs gelesen	Implementiert	HTTPS	Anzahl der gelesenen IOPs auf der Festplatte
		IOPs gesamt	Implementiert	HTTPS	
		IOPs Schreiben	Implementiert	HTTPS	
		Latenz beim Lesen	Implementiert	HTTPS	
		Latenz gesamt	Implementiert	HTTPS	
		Latenz beim Schreiben	Implementiert	HTTPS	
		Durchsatz beim Lesen	Implementiert	HTTPS	
		Durchsatz gesamt	Implementiert	HTTPS	Durchschnittliche Gesamtrate der Festplatte (Lesen und Schreiben auf allen Festplatten) in MB/s
		Durchsatz beim Schreiben	Implementiert	HTTPS	

Von diesem Datensammler verwendete Verwaltungs-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschichtprotokoll	Verwendete eingehende Ports	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur schreibgeschützte Anmeldeinformationen	Unterstützt Verschlüsselung	Firewall-freundlich (statische Ports)
HP Nimble REST API	HTTPS	HTTPS	5392		true	FALSCH	true	true

Huawei OceanStor (REST/HTTPS)

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
18800 V5 2600 V3 5310 V5 5500 V3 5500 V5 5800 V3 6800 V3 Dorado 18000 V6 NVMe Dorado 3000 V6 Dorado 5000 V3 Dorado 6000 V3 Dorado 6000 V6 NVMe	V300R001C01 V300R002C10 V300R006C10 V300R006C20 V300R006C50 V500R007C10 V500R007C30 V500R007C60 Kunpeng V500R007C61 V500R007C71 Kunpeng V600R003C00 V600R005C11 V600R005C26 V600R005C27

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Stiftung					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Typ	Lücke	HTTPS	
		Virtuell	Implementiert	HTTPS	Ist dies ein Gerät zur Speichervirtualisierung?
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	Volumen	Kapazität	Implementiert	HTTPS	Snapshot Verwendete Kapazität in MB
		Kreuzungspfad	Implementiert	HTTPS	
		Name	Implementiert	HTTPS	
		Gesamte Rohkapazität	Implementiert	HTTPS	Gesamte Rohkapazität (Summe aller Festplatten im Array)
		Redundanz	Implementiert	HTTPS	Redundanzstufe
		Speicherpool-ID	Implementiert	HTTPS	
		Thin Provisioning	Implementiert	HTTPS	
		UUID	Implementiert	HTTPS	
		Verwendete Kapazität	Implementiert	HTTPS	
		Virtuell	Implementiert	HTTPS	Ist dies ein Gerät zur Speichervirtualisierung?
	Volumenkarte	LUN	Implementiert	HTTPS	Name der Backend-LUN
		Protokoll-Controller	Implementiert	HTTPS	
		Speicherport	Implementiert	HTTPS	
		Typ	Lücke	HTTPS	
	Volumenmaske	Initiator	Implementiert	HTTPS	
		Protokoll-Controller	Implementiert	HTTPS	
		Speicherport	Implementiert	HTTPS	
		Typ	Lücke	HTTPS	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Leistung					
1108					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

					allen Festplatten) in MB/s
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	Volumen	Cache-Trefferquote beim Schreiben	Implementiert	HTTPS	
		Cache-Trefferquote beim Lesen	Implementiert	HTTPS	
		Cache-Trefferquote gesamt	Implementiert	HTTPS	
		Cache-Trefferquote beim Schreiben	Implementiert	HTTPS	
		Rohkapazität	Implementiert	HTTPS	
		Gesamtkapazität	Implementiert	HTTPS	
		Verwendete Kapazität	Implementiert	HTTPS	
		Verhältnis der genutzten Kapazität	Implementiert	HTTPS	
		IOPs gelesen	Implementiert	HTTPS	Anzahl der gelesenen IOPs auf der Festplatte
		IOPs gesamt	Implementiert	HTTPS	
		IOPs Schreiben	Implementiert	HTTPS	
		Schlüssel	Implementiert	HTTPS	
		Latenz beim Lesen	Implementiert	HTTPS	
		Latenz gesamt	Implementiert	HTTPS	
		Latenz beim Schreiben	Implementiert	HTTPS	
		Server-ID	Implementiert	HTTPS	
		Durchsatz beim Lesen	Implementiert	HTTPS	
		Durchsatz gesamt	Implementiert	HTTPS	Durchschnittliche Gesamtrate der Festplatte (Lesen und Schreiben auf allen Festplatten) in MB/s
		Durchsatz beim Schreiben	Implementiert	HTTPS	

Von diesem Datensammler verwendete Verwaltungs-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschichtprotokoll	Verwendete eingehende Ports	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur schreibgeschützte Anmeldeinformationen	Unterstützt Verschlüsselung	Firewall-freundlich (statische Ports)
Huawei OceanStor REST API	HTTPS	HTTPS	8088		true	true	true	true
Huawei OceanStor Performance REST API	HTTPS	HTTPS	8088		true	FALSCH	true	true

IBM Cleversafe

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Stiftung					
1118					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		UUID	Implementiert	HTTPS	
		Version	Implementiert	HTTPS	Softwareversion
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Management-IP-Adressen	Implementiert	HTTPS	
	Speicherpool	In DWH-Kapazität einschließen	Implementiert	HTTPS	Eine Möglichkeit von ACQ, zu steuern, welche Speicherpools in der DWH-Kapazität interessant sind
		Name	Implementiert	HTTPS	
		Physische Festplattenkapazität (MB)	Implementiert	HTTPS	wird als Rohkapazität für Speicherpools verwendet
		Raid-Gruppe	Implementiert	HTTPS	gibt an, ob dieser Speicherpool eine RAID-Gruppe ist
		Verhältnis von Rohmaterial zu Nutzmaterial	Implementiert	HTTPS	Verhältnis zur Umrechnung von nutzbarer Kapazität in Rohkapazität
		Speicherpool-ID	Implementiert	HTTPS	
		Thin Provisioning wird unterstützt	Implementiert	HTTPS	Ob dieses interne Volume Thin Provisioning für die darüber liegende Volume-Schicht unterstützt
		Gesamtzugewiesene Kapazität	Implementiert	HTTPS	
		Gesamte genutzte Kapazität	Implementiert	HTTPS	Gesamtkapazität in MB
		Typ	Lücke	HTTPS	
		Virtuell	Implementiert	HTTPS	Ist dies ein Gerät zur Speichervirtualisierung?

Von diesem Datensammler verwendete Verwaltungs-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschichtprotokoll	Verwendete eingehende Ports	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur schreibgeschützte Anmeldeinformationen	Unterstützt Verschlüsselung	Firewall-freundlich (statische Ports)
IBM Cleversafe REST-API	HTTPS	HTTPS	443		true	true	true	true

IBM DS 8K (DSCLI)

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
2107-951 2107-961 2107-993 2107-994 2107-996 2107-A05	- 7.10.1.8 7.6.31.4250 7.7.51.1400 7.9.32.101 7.9.33.132 7.9.33.95 7.9.40.251 7.9.41.65

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Stiftung					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

	Volumenmaske	Initiator	Implementiert	DSNI	
		Protokoll-Controller	Implementiert	DSNI	
		Speicherport	Implementiert	DSNI	
	WWN-Alias	Host-Aliase	Implementiert	DSNI	
		Host-Betriebssystem	Implementiert	DSNI	
		Objekttyp	Implementiert	DSNI	
		Quelle	Implementiert	DSNI	
		WWN	Implementiert	DSNI	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Leistung					
1128					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Verwendete Kapazität	Implementiert	DSNI	
		Verhältnis der genutzten Kapazität	Implementiert	DSNI	
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	Volumen	Cache-Trefferquote beim Lesen	Implementiert	DSNI	
		Cache-Trefferquote gesamt	Implementiert	DSNI	
		Cache-Trefferquote beim Schreiben	Implementiert	DSNI	
		Rohkapazität	Implementiert	DSNI	
		Gesamtkapazität	Implementiert	DSNI	
		Verwendete Kapazität	Implementiert	DSNI	
		Verhältnis der genutzten Kapazität	Implementiert	DSNI	
		IOPs gelesen	Implementiert	DSNI	Anzahl der gelesenen IOPs auf der Festplatte
		IOPs gesamt	Implementiert	DSNI	
		IOPs Schreiben	Implementiert	DSNI	
		Schlüssel	Implementiert	DSNI	
		Latenz beim Lesen	Implementiert	DSNI	
		Latenz gesamt	Implementiert	DSNI	
		Latenz beim Schreiben	Implementiert	DSNI	
		Server-ID	Implementiert	DSNI	
		Durchsatz beim Lesen	Implementiert	DSNI	
		Durchsatz gesamt	Implementiert	DSNI	Durchschnittliche Gesamtrate der Festplatte (Lesen und Schreiben auf allen Festplatten) in MB/s
		Durchsatz beim Schreiben	Implementiert	DSNI	

Von diesem Datensammler verwendete Verwaltungs-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschichtprotokoll	Verwendete eingehende Ports	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur schreibgeschützte Anmeldeinformationen	Unterstützt Verschlüsselung	Firewall-freundlich (statische Ports)
Konfiguration des Datenquellenassistenten	Manuelle Eingabe				true	true	true	true
IBM DS CLI	DSNI	DSNI			true	true	true	true

IBM PowerVM (SSH)

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Stiftung					
1136					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

	VirtualMachine-Festplatte	OID	Implementiert	SSH	
		VirtualDisk-OID	Implementiert	SSH	
Produkt	**Kategorie**	**Funktionsname/Attribut OID**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	Gastgeber	Host-CPU-Anzahl	Implementiert	SSH	
		Vom Host installierter Speicher	Implementiert	SSH	
		Hostmodell	Implementiert	SSH	
		NIC-Anzahl	Implementiert	SSH	
		IP-Adressen	Implementiert	SSH	
		Hersteller	Implementiert	SSH	
		Name	Implementiert	SSH	
		OID	Implementiert	SSH	
		Plattformtyp	Implementiert	SSH	
	Info	Datenquellenname	Implementiert	SSH	Info
		Datum	Implementiert	SSH	
		Absender-ID	Implementiert	SSH	

Von diesem Datensammler verwendete Verwaltungs-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschichtprotokoll	Verwendete eingehende Ports	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur schreibgeschützte Anmeldeinformationen	Unterstützt Verschlüsselung	Firewall-freundlich (statische Ports)
SSH-Zugriff auf die IBM Hardware Management Console	SSH	SSH	22		true	FALSCH	true	true

IBM SVC (CLI)

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
2072-12F 2072-12G 2072-224 2072-24C 2072-24E 2072-24F 2072-24G 2072-2N4 2072-324 2072-3H4 2072-3N2 2072-3N4 2072-92F 2072-92G 2076-124 2076-12F 2076-224 2076-24F 2076-24G 2076-524 2076-624 2076-724 2076-824 2076-AF6 2076- AFF 2077-24F 2077-24G 2077-424 2077-4H4 2078-12F 2078-12G 2078-224 2078-24C 2078-24F 2078-24G 2078-324 2078-424 2078-4H4 2078-92G 2078-AF3 4657-24G 4657-924 4662-12G 4662-24G 4662-6H2 4666-AH8 4666-UH8 4680-24H 4680-2P4 4680-3P4 4680-92H 4983-AH8 9843-AE2 9843-AE3 9846-AG8 9848-AF7 9848-AF8 9848-AG8 9848-UG8 SVC	1.5.2.7 1.6.1.2 1.6.1.4 1.6.1.5 7.7.1.8 7.8.1.11 7.8.1.12 7.8.1.13 7.8.1.14 7.8.1.16 7.8.1.5 7.8.1.6 7.8.1.7 7.8.1.8 8.2.1.10 8.2.1.8 8.2.1.9 8.3.1.10 8.3.1.2 8.3.1.5 8.3.1.6 8.3.1.7 8.3.1.8 8.3.1.9 8.4.0.10 8.4.0.11 8.4.0.13 8.4.0.15 8.4.0.2 8.4.0.5 8.4.0.6 8.4.0.9 8.4.2.0 8.5.0.10 8.5.0.11 8.5.0.12 8.5.0.13 8.5.0.14 8.5.0.5 8.5.0.6 8.5.0.7 8.5.0.8 8.5.0.9 8.6.0.0 8.6.0.2 8.6.0.3 8.6.0.4 8.6.0.5 8.7.0.0 8.7.0.1 8.7.0.2 8.7.0.3

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Stiftung					
1140					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Kapazität			, die von einem Host auf dieses Volume
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Komprimierung aktiviert	Implementiert	SSH	
		Verschlüsselt	Implementiert	SSH	
	Volumenkarte	LUN	Implementiert	SSH	Name der Backend-LUN
		Protokoll-Controller	Implementiert	SSH	
		Speicherport	Implementiert	SSH	
	Volumenmaske	Initiator	Implementiert	SSH	
		Protokoll-Controller	Implementiert	SSH	
		Speicherport	Implementiert	SSH	
		Typ	Lücke	SSH	
	WWN-Alias	Host-Aliase	Implementiert	SSH	
		Objekttyp	Implementiert	SSH	
		Quelle	Implementiert	SSH	
		WWN	Implementiert	SSH	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Leistung					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

					Festplatte (Lesen und Schreiben auf allen Festplatten)
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Durchsatz beim Schreiben	Implementiert	SSH	

Von diesem Datensammler verwendete Verwaltungs-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschichtprotokoll	Verwendete eingehende Ports	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur schreibgeschützte Anmeldeinformationen	Unterstützt Verschlüsselung	Firewall-freundlich (statische Ports)
IBM SVC-CLI	SSH	SSH	22		true	FALSCH	true	true

IBM XIV und A9000 (XIVCLI)

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
A14	10.2.4.e

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Stiftung					
1156					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Kapazität			
		Redundanz	Implementiert	XIV CLI	Redundanzstufe
Produkt	**Kategorie**	**Konfiguration/Attribut aktiviert**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	Volumenkarte	LUN	Implementiert	XIV CLI	Name der Backend-LUN
		Protokoll-Controller	Implementiert	XIV CLI	
	Volumenmaske	Initiator	Implementiert	XIV CLI	
		Protokoll-Controller	Implementiert	XIV CLI	
	WWN-Alias	Quelle	Implementiert	XIV CLI	
		Host-Aliase	Implementiert	XIV CLI	
		WWN	Implementiert	XIV CLI	
		Objekttyp	Implementiert	XIV CLI	
		Host-Betriebssystem	Implementiert	XIV CLI	

Von diesem Datensammler verwendete Verwaltungs-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschichtprotokoll	Verwendete eingehende Ports	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur schreibgeschützte Anmeldeinformationen	Unterstützt Verschlüsselung	Firewall-freundlich (statische Ports)
IBM DS CLI	DSNI	DSNI			true	true	true	true
IBM XIV CLI	XIV CLI	TCP	7778		true	FALSCH	true	FALSCH

Infinidat Infinibox (HTTP)

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
F4303 F6230 F6240	6.0.20.40 6.0.31.0 7.1.14.0 7.1.15.0 7.3.20.90 8.1.0.280

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Stiftung					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Protokoll-Controller	Implementiert	HTTPS	
		Speicherport	Implementiert	HTTPS	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
		Typ	Lücke	HTTPS	
	WWN-Alias	Host-Aliase	Implementiert	HTTPS	
		Objekttyp	Implementiert	HTTPS	
		Quelle	Implementiert	HTTPS	
		WWN	Implementiert	HTTPS	

Von diesem Datensammler verwendete Verwaltungs-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschichtprotokoll	Verwendete eingehende Ports	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur schreibgeschützte Anmeldeinformationen	Unterstützt Verschlüsselung	Firewall-freundlich (statische Ports)
Infinidat REST API	HTTPS	HTTPS	443		true	true	true	true

Microsoft Azure Compute

Von diesem Datensammler unterstützte Modelle und Versionen: API-Versionen:

- 01.06.2018

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Stiftung					
1170					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Hersteller	Implementiert	HTTPS	
		Name	Implementiert	HTTPS	
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		UID	Implementiert	HTTPS	
	Info	API-Beschreibung	Implementiert	HTTPS	
		API-Name	Implementiert	HTTPS	
		API-Version	Implementiert	HTTPS	
		Datenquellenname	Implementiert	HTTPS	Info
		Datum	Implementiert	HTTPS	
		Absender-ID	Implementiert	HTTPS	
		Urheberschlüssel	Implementiert	HTTPS	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Leistung					

					allen Festplatten) in MB/s
Produkt	**Kategorie**	**Funktionsname**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	vm	Gesamtkapazität	Implementiert	HTTPS	
		Gesamte CPU-Auslastung	Implementiert	HTTPS	
		IOPs gelesen	Implementiert	HTTPS	Anzahl der gelesenen IOPs auf der Festplatte
		diskIops.total	Implementiert	HTTPS	
		Festplatten-IOPs beim Schreiben	Implementiert	HTTPS	
		Festplattendurchsatz beim Lesen	Implementiert	HTTPS	
		Durchsatz beim Lesen	Implementiert	HTTPS	Gesamtdurchsatz der Festplatte beim Lesen
		Festplattendurchsatz beim Schreiben	Implementiert	HTTPS	
		IP-Durchsatz beim Lesen	Implementiert	HTTPS	
		Durchsatz gesamt	Implementiert	HTTPS	IP-Durchsatz gesamt
		ipThroughput.write	Implementiert	HTTPS	
	VM	Gesamtkapazität	Implementiert	HTTPS	
		Schlüssel	Implementiert	HTTPS	
		Server-ID	Implementiert	HTTPS	

Von diesem Datensammler verwendete Verwaltungs-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschichtprotokoll	Verwendete eingehende Ports	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur schreibgeschützte Anmeldeinformationen	Unterstützt Verschlüsselung	Firewall-freundlich (statische Ports)
Microsoft Azure Compute REST-API	HTTPS	HTTPS	443		true	true	true	true

Microsoft Hyper-V

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Stiftung					
1176					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

	VirtualMachine-Festplatte	OID	Implementiert	WMI	
		VirtualDisk-OID	Implementiert	WMI	
Produkt	**Kategorie**	**Funktionsattribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		VirtualMachine-OID	Implementiert	WMI	
	Gastgeber	Host-CPU-Anzahl	Implementiert	WMI	
		Host-CPU-Geschwindigkeit	Implementiert	WMI	
		Hostdomäne	Implementiert	WMI	
		Vom Host installierter Speicher	Implementiert	WMI	
		Hostmodell	Implementiert	WMI	
		NIC-Anzahl	Implementiert	WMI	
		NIC-Geschwindigkeit	Implementiert	WMI	
		IP-Adressen	Implementiert	WMI	
		Hersteller	Implementiert	WMI	
		Name	Implementiert	WMI	
		OID	Implementiert	WMI	
		Plattformtyp	Implementiert	WMI	
	ISCSI-Knoten	Host-Aliase	Implementiert	WMI	
		Knotenname	Implementiert	WMI	
		OID	Implementiert	WMI	
		Typ	Lücke	WMI	
	Info	Datenquellenname	Implementiert	WMI	Info
		Datum	Implementiert	WMI	
		Absender-ID	Implementiert	WMI	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Leistung					
1180					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Durchsatz gesamt	Implementiert	WS-Management	IP-Durchsatz gesamt
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	VM	Gesamtkapazität	Implementiert	WS-Management	
		Verwendete Kapazität	Implementiert	WS-Management	
		Verhältnis der genutzten Kapazität	Implementiert	WS-Management	
		Schlüssel	Implementiert	WS-Management	
		Server-ID	Implementiert	WS-Management	

Von diesem Datensammler verwendete Verwaltungs-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschichtprotokoll	Verwendete eingehende Ports	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur schreibgeschützte Anmeldeinformationen	Unterstützt Verschlüsselung	Firewall-freundlich (statische Ports)
PowerShell	WS-Management	HTTP	5985		true	FALSCH	FALSCH	true
WMI	WMI	WMI	135		true	FALSCH	true	true

NetApp 7-Modus

Von diesem Datensammler unterstützte Modelle und Versionen:

API-Versionen	Modelle	Firmware-Versionen
1,12 1,17 1,19 1,20 1,21	FAS2040 FAS2220 FAS2240-4 FAS2520 FAS2552 FAS2554 FAS3140 FAS3160 FAS3250 FAS3270 FAS6240 FAS6250 FAS8020 FAS8040 FAS8060 N6070 N6240 N6270	8.1.1 7-Modus 8.1.4P9D18 7-Modus 8.2.2 7-Modus 8.2.3 7-Modus 8.2.3P2 7-Modus 8.2.3P3 7-Modus 8.2.4 7-Modus 8.2.4P4 7-Modus 8.2.4P5 7-Modus 8.2.4P6 7-Modus 8.2.5 7-Modus 8.2.5P3 7-Modus 8.2.5P4 7-Modus 8.2.5P5 7-Modus 8.2P3 7-Modus 8.2P4 7-Modus Data ONTAP Version 7.3.3 Data ONTAP -Version 8.2.5 7-Modus Data ONTAP Version 8.2.5P1 7-Modus

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Stiftung					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

					Backend-LUN
		Protokoll-Controller	Implementiert		
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Typ	Lücke		
	Volumenmaske	Initiator	Implementiert		
		Protokoll-Controller	Implementiert		
		Speicherport	Implementiert		
		Typ	Lücke		

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Leistung					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Auslastung gesamt	Implementiert		
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Auslastung Schreiben	Implementiert		
	Volumen	Rohkapazität	Implementiert		
		Gesamtkapazität	Implementiert		
		Verwendete Kapazität	Implementiert		
		Verhältnis der genutzten Kapazität	Implementiert		
		IO-Dichte lesen	Implementiert		
		IO-Dichte gesamt	Implementiert		
		Schreib-E/A-Dichte	Implementiert		
		IOPs gelesen	Implementiert		Anzahl der gelesenen IOPs auf der Festplatte
		IOPs gesamt	Implementiert		
		IOPs Schreiben	Implementiert		
		Latenz beim Lesen	Implementiert		
		Latenz gesamt	Implementiert		
		Latenz beim Schreiben	Implementiert		
		Teilweise blockiertes Verhältnis	Implementiert		
		Durchsatz beim Lesen	Implementiert		
		Durchsatz gesamt	Implementiert		Durchschnittliche Gesamtrate der Festplatte (Lesen und Schreiben auf allen Festplatten) in MB/s
		Durchsatz beim Schreiben	Implementiert		
		Schreiben ausstehend	Implementiert		insgesamt ausstehende Schreibvorgänge

Von diesem Datensammler verwendete Verwaltungs-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschichtprotokoll	Verwendete eingehende Ports	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur schreibgeschützte Anmeldeinformationen	Unterstützt Verschlüsselung	Firewall-freundlich (statische Ports)
NetApp 7-Modus ZAPI	ZAPI	ZAPI			true	true	true	true

NetApp E-Serie REST

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
2800B 2806 5700	08.71.03.00 08.73.00.00 08.74.02.00 08.75.00.00 08.75.00.01 08.80.00.00 08.81.00.03 08.81.02.00 08.81.03.00 08.90.00.00

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Stiftung					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Virtuell	Implementiert	HTTPS	Ist dies ein Gerät zur Speichervirtualisierung?
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Verschlüsselt	Implementiert	HTTPS	
	Volumenkarte	LUN	Implementiert	HTTPS	Name der Backend-LUN
		Speicherport	Implementiert	HTTPS	
		Typ	Lücke	HTTPS	
	Volumenmaske	Initiator	Implementiert	HTTPS	
		Speicherport	Implementiert	HTTPS	
		Typ	Lücke	HTTPS	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Leistung					

		Schreiben			
		Server-ID	Implementiert	HTTPS	
Produkt	**Kategorie**	**Funktion/Attribut lesen**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Durchsatz gesamt	Implementiert	HTTPS	Durchschnittliche Gesamtrate der Festplatte (Lesen und Schreiben auf allen Festplatten) in MB/s
		Durchsatz beim Schreiben	Implementiert	HTTPS	

Von diesem Datensammler verwendete Verwaltungs-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschichtprotokoll	Verwendete eingehende Ports	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur schreibgeschützte Anmeldeinformationen	Unterstützt Verschlüsselung	Firewall-freundlich (statische Ports)
NetApp E-Serie REST API	HTTPS	HTTPS	443		true	true	true	true

Amazon FSx for NetApp ONTAP

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
FSx für ONTAP	Data ONTAP

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Stiftung					
1222					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

	Volumes der virtuellen Maschine				
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	Kategorie Maschine StoragePool lRef	Eigenschaft	Implementiert	HTTPS	
	VirtualMachine-Volume-Referenz	Datenträgername	Implementiert	HTTPS	
	Volumen	Kapazität	Implementiert	HTTPS	Snapshot Verwendete Kapazität in MB
		Datenträgergruppe	Implementiert	HTTPS	Datenträgergruppentyp
		Kreuzungspfad	Implementiert	HTTPS	
		Letzter bekannter Zugriffszeitpunkt	Implementiert	HTTPS	Letzter bekannter Zugriff auf das Volume
		Name	Implementiert	HTTPS	
		Qtree-ID	Implementiert	HTTPS	eindeutige ID des Qtree
		Gesamte Rohkapazität	Implementiert	HTTPS	Gesamte Rohkapazität (Summe aller Festplatten im Array)
		Speicherpool-ID	Implementiert	HTTPS	
		Thin Provisioning	Implementiert	HTTPS	
		Typ	Lücke	HTTPS	
		UUID	Implementiert	HTTPS	
		Verwendete Kapazität	Implementiert	HTTPS	
		Verschlüsselt	Implementiert	HTTPS	
	Volumenkarte	LUN	Implementiert	HTTPS	Name der Backend-LUN
		Protokoll-Controller	Implementiert	HTTPS	
		Speicherport	Implementiert	HTTPS	
		Typ	Lücke	HTTPS	
	Volumenmaske	Initiator	Implementiert	HTTPS	
		Protokoll-Controller	Implementiert	HTTPS	
		Speicherport	Implementiert	HTTPS	
		Typ	Lücke	HTTPS	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Leistung					
1238					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

					in MB/s
		Verhältnis der	Implementiert	HTTPS	Als Zeitreihe
Produkt	**Kategorie**	**Funktionsname**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Snapshot der genutzten Kapazität	Implementiert	HTTPS	
		Snapshot-reservierte Kapazität	Implementiert	HTTPS	
	Virtuelle Maschine	Gesamtkapazität	Implementiert	HTTPS	
		Verwendete Kapazität	Implementiert	HTTPS	
		Schlüssel	Implementiert	HTTPS	
		Server-ID	Implementiert	HTTPS	

Von diesem Datensammler verwendete Verwaltungs-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschichtprotokoll	Verwendete eingehende Ports	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur schreibgeschützte Anmeldeinformationen	Unterstützt Verschlüsselung	Firewall-freundlich (statische Ports)
NetApp ONTAP API	HTTP/HTTPS	HTTP/HTTPS	80/443		true	true	true	true

NetApp Clustered Data ONTAP 8.1.1+

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
AFF-A150 AFF-A1K AFF-A20 AFF-A200 AFF-A220 AFF -A250 AFF-A300 AFF-A320 AFF-A400 AFF-A70 AFF-A700 AFF-A700s AFF-A800 AFF-A90 AFF-A900 AFF-C190 AFF-C250 AFF-C400 AFF-C60 AFF-C80 AFF-C800 AFF AFF8040 AFF8060 AFF8080 ASA-A250 ASA-A400 ASA-A800 ASA-A900 ASA-C250 ASA-C400 ASA-C800 CDvM100 CDvM200 DM5000H DM7100F FAS2240-2 FAS2520 FAS2552 FAS2554 FAS2620 FAS2650 FAS2720 FAS2750 FAS2820 FAS3220 FAS3250 FAS3270 FAS500f FAS6210 FAS8020 FAS8040 FAS8060 FAS8080 FAS8200 FAS8200 FAS8300 FAS8700 FAS9000 FAS9500 FASDvM300 SIMBOX	• 8.2.3P4 • 8.2.3P5 • 8.3.1P2 • 8.3.2 • 8.3.2P12 • 8.3.2P5 • 9.0.0 • 9.1.0 • 9.1.0P1 • 9.1.0P11 • 9.1.0P15 • 9.1.0P17 • 9.1.0P19 • 9.1.0P2 • 9.1.0P20 • 9.1.0P3 • 9.1.0P6 • 9.1.0P7 • 9.1.0P8 • 9.1.0P9 • 9.10.0 • 9.10.1 • 9.10.1P1 • 9.10.1P10 • 9.10.1P11 • 9.10.1P12 • 9.10.1P13 • 9.10.1P14 • 9.10.1P15 • 9.10.1P16 • 9.10.1P17 • 9.10.1P18 • 9.10.1P19 • 9.10.1P2 • 9.10.1P20 • 9.10.1P3 9.10.1P4 9.10.1P5

Von diesem Datensammler unterstützte Produkte:

-
- 9.10.1P6
- 9.10.1P7
- 9.10.1P8
- 9.10.1P9
- 9.11.0P1
- 9.11.1
- 9.11.1P1
- 9.11.1P10
- 9.11.1P11
- 9.11.1P12
- 9.11.1P13
- 9.11.1P14
- 9.11.1P15
- 9.11.1P16
- 9.11.1P17
- 9.11.1P18
- 9.11.1P2
- 9.11.1P3
- 9.11.1P4
- 9.11.1P5
- 9.11.1P6
- 9.11.1P7
- 9.11.1P8
- 9.11.1P9
- 9.12.1
- 9.12.1P1
- 9.12.1P10
- 9.12.1P11
- 9.12.1P12
- 9.12.1P13
- 9.12.1P14
- 9.12.1P15
- 9.12.1P16
- 9.12.1P17
- 9.12.1P2
- 9.12.1P3

9.12.1P4

9.12.1P5

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Stiftung			• 9.12.1P7 • 9.12.1P8 • 9.12.1P9 • 9.13.0 • 9.13.0P1 • 9.13.0P3 • 9.13.1 • 9.13.1D1 • 9.13.1P1 • 9.13.1P10 • 9.13.1P11 • 9.13.1P12 • 9.13.1P13 • 9.13.1P14 • 9.13.1P2 • 9.13.1P3 • 9.13.1P4 • 9.13.1P5 • 9.13.1P6 • 9.13.1P7 • 9.13.1P8 • 9.13.1P9 • 9.14.0 • 9.14.0P1 • 9.14.0P2 • 9.14.1 • 9.14.1P1 • 9.14.1P10 • 9.14.1P11 • 9.14.1P2 • 9.14.1P4 • 9.14.1P5 • 9.14.1P6 • 9.14.1P7 • 9.14.1P8 9.14.1P8D5 9.14.1P9		

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
			• 9.15.0P2 • 9.15.1 • 9.15.1P1 • 9.15.1P2 • 9.15.1P2D2 • 9.15.1P3 • 9.15.1P4 • 9.15.1P5 • 9.15.1P6 • 9.15.1P7 • 9.15.1P7D4 • 9.15.1P8 • 9.16.1 • 9.16.1P1 • 9.17.1 • 9.2.0P3 • 9.2.0P4 • 9.3.0P15 • 9.3.0P18 • 9.3.0P20 • 9.3.0P21 • 9.3.0P6 • 9.3.0P7 • 9.3.0P8 • 9.4.0 • 9.4.0P2 • 9.4.0P5 • 9.5.0 • 9.5.0P1 • 9.5.0P10 • 9.5.0P14 • 9.5.0P16 • 9.5.0P17 • 9.5.0P18 • 9.5.0P19 9.5.0P2 9.5.0P3		

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
			• 9.5.0P7 • 9.5.0P9 • 9.6.0 • 9.6.0P11 • 9.6.0P18 • 9.6.0P2 • 9.6.0P3 • 9.6.0P5 • 9.7.0 • 9.7.0P10 • 9.7.0P11 • 9.7.0P12 • 9.7.0P13 • 9.7.0P14 • 9.7.0P15 • 9.7.0P16 • 9.7.0P17 • 9.7.0P18 • 9.7.0P19 • 9.7.0P20 • 9.7.0P21 • 9.7.0P22 • 9.7.0P23 • 9.7.0P4 • 9.7.0P5 • 9.7.0P6 • 9.7.0P7 • 9.7.0P8 • 9.7.0P9 • 9.8.0 • 9.8.0P1 • 9.8.0P10 • 9.8.0P11 • 9.8.0P12 • 9.8.0P13 9.8.0P14 9.8.0P15		

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
			• 9.8.0P17 • 9.8.0P18 • 9.8.0P19 • 9.8.0P2 • 9.8.0P20 • 9.8.0P21 • 9.8.0P3 • 9.8.0P4 • 9.8.0P6 • 9.8.0P7 • 9.8.0P8 • 9.8.0P9 • 9,0 • 9,1 • 9.9.1P10 • 9.9.1P11 • 9.9.1P12 • 9.9.1P13 • 9.9.1P14 • 9.9.1P15 • 9.9.1P16 • 9.9.1P17 • 9.9.1P18 • 9.9.1P19 • 9.9.1P2 • 9.9.1P20 • 9.9.1P3 • 9.9.1P6 • 9.9.1P7 • 9.9.1P9		

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

					Speichervirtualisierung?
		Verschlüsselt	Implementiert	HTTPS	
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		QoS-Limit IOPS	Implementiert	HTTPS	
		QoS-Limit MBPS	Implementiert	HTTPS	
		QoS-Limit Raw	Implementiert	HTTPS	
		QoS – Richtlinie	Implementiert	HTTPS	
	Volumenkarte	LUN	Implementiert	HTTPS	Name der Backend-LUN
		Protokoll-Controller	Implementiert	HTTPS	
		Speicherport	Implementiert	HTTPS	
		Typ	Lücke	HTTPS	
	Volumenmaske	Initiator	Implementiert	HTTPS	
		Protokoll-Controller	Implementiert	HTTPS	
		Speicherport	Implementiert	HTTPS	
		Typ	Lücke	HTTPS	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Leistung					
1268					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
	Maschine	Verwendete Kapazität	Implementiert	HTTPS	
		Schlüssel	Implementiert	HTTPS	
		Server-ID	Implementiert	HTTPS	
	Volumen	Rohkapazität	Implementiert	HTTPS	
		Gesamtkapazität	Implementiert	HTTPS	
		Verwendete Kapazität	Implementiert	HTTPS	
		Verhältnis der genutzten Kapazität	Implementiert	HTTPS	
		IO-Dichte lesen	Implementiert	HTTPS	
		IO-Dichte gesamt	Implementiert	HTTPS	
		Schreib-E/A-Dichte	Implementiert	HTTPS	
		IOPs gelesen	Implementiert	HTTPS	Anzahl der gelesenen IOPs auf der Festplatte
		IOPs gesamt	Implementiert	HTTPS	
		IOPs Schreiben	Implementiert	HTTPS	
		Latenz beim Lesen	Implementiert	HTTPS	
		Latenz gesamt	Implementiert	HTTPS	
		Latenz beim Schreiben	Implementiert	HTTPS	
		Teilweise blockiertes Verhältnis	Implementiert	HTTPS	
		Durchsatz beim Lesen	Implementiert	HTTPS	
		Durchsatz gesamt	Implementiert	HTTPS	Durchschnittliche Gesamtrate der Festplatte (Lesen und Schreiben auf allen Festplatten) in MB/s
		Durchsatz beim Schreiben	Implementiert	HTTPS	

Von diesem Datensammler verwendete Verwaltungs-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschichtprotokoll	Verwendete eingehende Ports	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur schreibgeschützte Anmeldeinformationen	Unterstützt Verschlüsselung	Firewall-freundlich (statische Ports)
NetApp ONTAP API	HTTP/HTTPS	HTTP/HTTPS	80/443		true	true	true	true

ASA

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
ASA-A1K ASA-A20 ASA-A90	NetApp Release 9.16.1: Sa., 18. Januar 2025, 19:31:15 UTC. NetApp Release 9.16.1RC1: Mo., 4. November 2024, 10:39:46 UTC.

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Stiftung					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Protokoll-Controller	Implementiert	HTTPS	
		Speicherport	Implementiert	HTTPS	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
		Typ	Lücke	HTTPS	
	Volumenmaske	Initiator	Implementiert	HTTPS	
		Protokoll-Controller	Implementiert	HTTPS	
		Speicherport	Implementiert	HTTPS	
		Typ	Lücke	HTTPS	
Leistung	Scheibe	IOPs gelesen	Implementiert	HTTPS	Anzahl der gelesenen IOPs auf der Festplatte
		IOPs gesamt	Implementiert	HTTPS	
		IOPs Schreiben	Implementiert	HTTPS	
		Schlüssel	Implementiert	HTTPS	
		Server-ID	Implementiert	HTTPS	
		Durchsatz beim Lesen	Implementiert	HTTPS	
		Durchsatz gesamt	Implementiert	HTTPS	Durchschnittliche Gesamtrate der Festplatte (Lesen und Schreiben auf allen Festplatten) in MB/s
		Durchsatz beim Schreiben	Implementiert	HTTPS	
		Leseauslastung	Implementiert	HTTPS	
		Auslastung gesamt	Implementiert	HTTPS	
		Auslastung Schreiben	Implementiert	HTTPS	

Von diesem Datensammler verwendete Verwaltungs-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschichtprotokoll	Verwendete eingehende Ports	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur schreibgeschützte Anmeldeinformationen	Unterstützt Verschlüsselung	Firewall-freundlich (statische Ports)
NetApp ASA API	HTTPS	HTTPS	443		true	true	true	true

NetApp ONTAP REST

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
AFF-A150 AFF-A220 AFF-A250 AFF-A300 AFF -A400 AFF-A70 AFF-A700 AFF-A700s AFF-A800 AFF-A90 AFF-A900 AFF-C190 AFF-C250 AFF-C400 AFF-C800 AFF-A250 ASA-A400 ASA-A800 ASA-C250 ASA-C800 ASA FAS2720 FAS2750 FAS2820 FAS8200 FAS8300 FAS8700 FAS9000 FAS9500 FASDvM300 SIMBOX	• NetApp Release 9.14.1P10: Do., 28. Nov. 2024, 12:32:16 UTC • NetApp Release 9.14.1P11: Mi., 22. Januar 2025, 11:55:28 UTC • NetApp Release 9.14.1P1: Do., 15. Feb. 2024, 00:45:21 UTC • NetApp Release 9.14.1P4: Do., 18. April 2024, 15:59:10 UTC • NetApp Release 9.14.1P5: Sa., 18. Mai 2024, 19:42:16 UTC • NetApp Release 9.14.1P6: Di., 18. Juni 2024, 16:11:44 UTC • NetApp Release 9.14.1P7: Do., 1. Aug. 2024, 03:07:44 UTC • NetApp Release 9.14.1P8: Fr., 13. September 2024, 07:12:27 UTC • NetApp Release 9.14.1P9: Montag, 21. Oktober 2024, 18:04:05 UTC • NetApp Release 9.15.1: Do Jul 04 12:21:07 UTC 2024 • NetApp Release 9.15.1P1: Di., 30. Juli 2024, 05:15:49 UTC • NetApp Release 9.15.1P2: Di., 27. Aug. 2024, 16:35:16 UTC • NetApp Release 9.15.1P3: Mi., 25. September 2024, 22:33:44 UTC • NetApp Release 9.15.1P4: So., 27. Okt. 2024, 20:15:53 UTC • NetApp Release 9.15.1P5: So., 24. Nov. 2024, 16:31:37 UTC • NetApp Release 9.15.1P6: Mi., 4. Dez. 2024, 01:42:39 UTC • NetApp Release 9.15.1P7: Sa., 18. Januar 2025, 21:34:02 UTC • NetApp Release 9.15.1RC2: Montag, 24. Juni 2024, 04:49:55 UTC • NetApp Release 9.16.1: Sa., 18. Januar 2025, 19:31:15 UTC • NetApp -Version 9.16.1P1: Fr., 14. Feb., 03:53:50 UTC 2025 • NetApp Release 9.16.1RC1: Montag, 4. November 2024, 10:39:46 UTC • NetApp Release Clawhammer__9.14.1: Sa., 18. Mai 2024, 09:23:49 UTC • NetApp -Release Cloudstream__9.16.1: Montag, 4. November 2024, 05:51:46 UTC

Von diesem Datensammler unterstützte Produkte:

-
- NetApp Release Cloudstream__9.16.1: Do., 13. März 2025, 20:55:54 UTC
- NetApp Release Electricjellyfish__9.17.1: Montag, 3. März 2025, 05:57:49 UTC
- NetApp Release Electricjellyfish__9.17.1: So., 9. März 2025, 05:56:14 UTC
- NetApp Release Electricjellyfish__9.17.1: So., 16. März 2025, 04:54:53 UTC
- NetApp -Release Electricjellyfish__9.17.1: Di., 28. Januar 2025, 11:48:14 UTC
- NetApp -Release Electricjellyfish__9.17.1: Di., 18. März 2025, 04:59:54 UTC
- NetApp -Release Electricjellyfish__9.17.1: Mi., 12. März 2025, 04:42:03 UTC
- NetApp -Release Mightysquirrel__9.15.1: Fr., 24. Mai 05:03:10 UTC 2024
- NetApp -Release Mightysquirrel__9.15.1: Sa., 18. Januar 2025, 11:39:42 UTC
- NetApp -Release Tropicallightning__9.18.0: Fr., 21. Feb., 14:02:58 UTC 2025
- NetApp -Version Tropicallightning__9.18.0: Montag, 17. Februar, 08:18:14 UTC 2025
- NetApp -Version Tropicallightning__9.18.0: Do., 20. Feb. 08:11:55 UTC 2025
- NetApp -Version Tropicallightning__9.18.0: Do., 27. Feb. 04:15:40 UTC 2025
- NetApp -Version Tropicallightning__9.18.0: Di., 18. Feb. 14:00:54 UTC 2025
- NetApp -Version Tropicallightning__9.18.0: Mi., 26. Feb. 08:19:21 UTC 2025
- NetApp -Version Tropicallightning__9.18.0: Mi., 29. Januar 2025, 08:34:06 UTC

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Stiftung					
1302					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Virtuell	Implementiert	HTTPS	Ist dies ein Gerät zur Speichervirtualisierung?
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Verschlüsselt	Implementiert	HTTPS	
	Volumenkarte	LUN	Implementiert	HTTPS	Name der Backend-LUN
		Protokoll-Controller	Implementiert	HTTPS	
		Speicherport	Implementiert	HTTPS	
		Typ	Lücke	HTTPS	
	Volumenmaske	Initiator	Implementiert	HTTPS	
		Protokoll-Controller	Implementiert	HTTPS	
		Speicherport	Implementiert	HTTPS	
		Typ	Lücke	HTTPS	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Leistung					
1318					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Server-ID	Implementiert	HTTPS	
		Snapshot-Kapazität	Implementiert	HTTPS	
Produkt	**Kategorie**	**Feature/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Snapshot der genutzten Kapazität	Implementiert	HTTPS	
		Snapshot-Verhältnis der genutzten Kapazität	Implementiert	HTTPS	Als Zeitreihe gemeldet

Von diesem Datensammler verwendete Verwaltungs-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschichtprotokoll	Verwendete eingehende Ports	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur schreibgeschützte Anmeldeinformationen	Unterstützt Verschlüsselung	Firewall-freundlich (statische Ports)
NetApp ONTAP REST API	HTTPS	HTTPS	443		true	true	true	true

NetApp SolidFire 8.1+

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
H410S-2 H610S-2 H610S-4 SF19210 SF2405 SF4805 SF9605 SF9608 H410S-0 H410S-1 H410S-2 H500S H610S-1 H610S-2 H610S-4 SF19210 SF38410 SF4805 SF9605 SF9608	11.1.0.72 11.7.0.76 12.0.0.333 12.2.0.777 12.3.0.958 12.3.1.103 12.3.1.165 12.3.2.3 12.5.0.897 12.7.0.380

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Stiftung					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		QoS-Limit IOPS	Implementiert	HTTPS	
		gos Min. IOPS	Implementiert	HTTPS	
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		QoS – Richtlinie	Implementiert	HTTPS	
	Volumenkarte	LUN	Implementiert	HTTPS	Name der Backend-LUN
		Maskierung erforderlich	Implementiert	HTTPS	
		Protokoll-Controller	Implementiert	HTTPS	
		Speicherport	Implementiert	HTTPS	
		Typ	Lücke	HTTPS	
	Volumenmaske	Initiator	Implementiert	HTTPS	
		Protokoll-Controller	Implementiert	HTTPS	
		Speicherport	Implementiert	HTTPS	
		Typ	Lücke	HTTPS	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Leistung					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Durchsatz beim Schreiben	Implementiert	HTTPS	
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	Volumen	Auslastung gesamt	Implementiert	HTTPS	
		Rohkapazität	Implementiert	HTTPS	
		Gesamtkapazität	Implementiert	HTTPS	
		Verwendete Kapazität	Implementiert	HTTPS	
		Verhältnis der genutzten Kapazität	Implementiert	HTTPS	
		Gesamteinsparungen durch Komprimierung	Implementiert	HTTPS	
		IOPs gelesen	Implementiert	HTTPS	Anzahl der gelesenen IOPs auf der Festplatte
		IOPs gesamt	Implementiert	HTTPS	
		IOPs Schreiben	Implementiert	HTTPS	
		Schlüssel	Implementiert	HTTPS	
		Latenz beim Lesen	Implementiert	HTTPS	
		Latenz gesamt	Implementiert	HTTPS	
		Latenz beim Schreiben	Implementiert	HTTPS	
		Teilweise blockiertes Verhältnis	Implementiert	HTTPS	
		Server-ID	Implementiert	HTTPS	
		Durchsatz beim Lesen	Implementiert	HTTPS	
		Durchsatz gesamt	Implementiert	HTTPS	Durchschnittliche Gesamtrate der Festplatte (Lesen und Schreiben auf allen Festplatten) in MB/s
		Durchsatz beim Schreiben	Implementiert	HTTPS	
		Auslastung gesamt	Implementiert	HTTPS	

Von diesem Datensammler verwendete Verwaltungs-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschichtprotokoll	Verwendete eingehende Ports	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur schreibgeschützte Anmeldeinformationen	Unterstützt Verschlüsselung	Firewall-freundlich (statische Ports)
SolidFire REST API	HTTPS	HTTPS	443		true	true	true	true

NetApp StorageGRID (HTTPS)

Von diesem Datensammler unterstützte Modelle und Versionen:

API-Versionen	Modelle	Firmware-Versionen
3,2 3,3 3,4 3,5 4,0 4,1	Webscale	11.4.0 11.5.0.11 11.5.0.6 11.5.0.7 11.5.0.9 11.6.0 11.6.0.10 11.6.0.11 11.6.0.12 11.6.0.13 11.6.0.14 11.6.0.15 11.6.0.16 11.6.0.4 11.6.0.5 11.6.0.7 11.6.0.8 11.6.0.9 11.7.0 11.7.0.11 11.7.0.12 11.7.0.13 11.7.0.3 11.7.0.4 11.7.0.5 11.7.0.6 11.7.0.8 11.7.0.9 11.8.0 11.8.0.1 11.8.0.2 11.8.0.3 11.8.0.5 11.8.0.6 11.8.0.7 11.8.0.8 11.8.0.9 11.9.0 11.9.0.1 11.9.0.2 11.9.0.3 11.9.0.4

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Stiftung					
1338					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Metadaten zur Knotenkapazitätsauslastung in MB	Implementiert	HTTPS	
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Sitename	Implementiert	HTTPS	
	Speicherpool	In DWH-Kapazität einschließen	Implementiert	HTTPS	Eine Möglichkeit von ACQ, zu steuern, welche Speicherpools in der DWH-Kapazität interessant sind
		Name	Implementiert	HTTPS	
		Physische Festplattenkapazität (MB)	Implementiert	HTTPS	wird als Rohkapazität für Speicherpools verwendet
		Raid-Gruppe	Implementiert	HTTPS	gibt an, ob dieser Speicherpool eine RAID-Gruppe ist
		Verhältnis von Rohmaterial zu Nutzmaterial	Implementiert	HTTPS	Verhältnis zur Umrechnung von nutzbarer Kapazität in Rohkapazität
		Speicherpool-ID	Implementiert	HTTPS	
		Thin Provisioning wird unterstützt	Implementiert	HTTPS	Ob dieses interne Volume Thin Provisioning für die darüber liegende Volume-Schicht unterstützt
		Gesamtzugewiesene Kapazität	Implementiert	HTTPS	
		Gesamte genutzte Kapazität	Implementiert	HTTPS	Gesamtkapazität in MB
		Typ	Lücke	HTTPS	
		Virtuell	Implementiert	HTTPS	Ist dies ein Gerät zur Speichervirtualisierung?

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Leistung					
1344					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

					allen Festplatten) in MB/s
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Durchsatz beim Schreiben	Implementiert		
	Speicherknotendaten	Schlüssel	Implementiert		
		Zulässige Metadaten zur Knotenkapazitätsauslastung	Implementiert		
		Knotenkapazitätsauslastung gesamt	Implementiert		
		Knotenkapazitätsauslastung Nutzbar	Implementiert		
		Verwendete Knotenkapazitätsauslastung	Implementiert		
		Verwendete Metadaten zur Knotenkapazitätsauslastung	Implementiert		
		Server-ID	Implementiert		
		Durchsatz beim Lesen	Implementiert		
		Durchsatz gesamt	Implementiert		Durchschnittliche Gesamtrate der Festplatte (Lesen und Schreiben auf allen Festplatten) in MB/s
		Durchsatz beim Schreiben	Implementiert		
	StoragePool-Datenträger	Bereitgestellte Kapazität	Implementiert		
		Rohkapazität	Implementiert		
		Gesamtkapazität	Implementiert		
		Verwendete Kapazität	Implementiert		
		Verhältnis der Überbelegungskapazität	Implementiert		Als Zeitreihe gemeldet
		Verhältnis der genutzten Kapazität	Implementiert		

Von diesem Datensammler verwendete Verwaltungs-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschichtprotokoll	Verwendete eingehende Ports	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur schreibgeschützte Anmeldeinformationen	Unterstützt Verschlüsselung	Firewall-freundlich (statische Ports)
StorageGrid REST-API	HTTPS	HTTPS	443		true	FALSCH	true	true

Nutanix-Speicher (REST)

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
NX-3170-G7 NX-8155-G7 HPE DX380 12LFF G11 HPE DX380-24 G10 HPE DX385-12 Gen10 Plus NX-3060-G6 NX-3060-G7 NX-3060-G8 NX-3155G-G7 NX-3155G-G8 NX-3170-G6 NX-8035-G8 NX-8150-G7 NX-8150-G8 NX-8155-G8 XF3070 XF8050-Core	5.20.1.1 6.10 6.10.1 6.5.3.7 6.5.4 6.5.5.1 6.5.5.7 6.5.6 6.5.6.5 6.5.6.6 6.5.6.7 6.7.1.6 7.0

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Stiftung					
1348					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Gesamtzugewiesene Kapazität	Implementiert	HTTPS	
		Gesamte Kapazität	Implementiert	HTTPS	Gesamtkapazität in MB
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Typ	Lücke	HTTPS	
		Virtuell	Implementiert	HTTPS	Ist dies ein Gerät zur Speichervirtualisierung?
	Volumen	Kapazität	Implementiert	HTTPS	Snapshot Verwendete Kapazität in MB
		Kreuzungspfad	Implementiert	HTTPS	
		Name	Implementiert	HTTPS	
		Qtree-ID	Implementiert	HTTPS	eindeutige ID des Qtree
		Gesamte Rohkapazität	Implementiert	HTTPS	Gesamte Rohkapazität (Summe aller Festplatten im Array)
		Redundanz	Implementiert	HTTPS	Redundanzstufe
		Speicherpool-ID	Implementiert	HTTPS	
		Thin Provisioning	Implementiert	HTTPS	
		UUID	Implementiert	HTTPS	
	Volumenkarte	LUN	Implementiert	HTTPS	Name der Backend-LUN
		Protokoll-Controller	Implementiert	HTTPS	
		Speicherport	Implementiert	HTTPS	
		Typ	Lücke	HTTPS	
	Volumenmaske	Initiator	Implementiert	HTTPS	
		Protokoll-Controller	Implementiert	HTTPS	
		Speicherport	Implementiert	HTTPS	
		Typ	Lücke	HTTPS	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Leistung					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

					allen Festplatten) in MB/s
Produkt	**Kategorie**	**Funktionsattribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Durchsatz beim Schreiben	Implementiert	HTTPS	
	StoragePool-Datenträger	IOPs gelesen	Implementiert	HTTPS	Anzahl der gelesenen IOPs auf der Festplatte
		IOPs gesamt	Implementiert	HTTPS	
		IOPs Schreiben	Implementiert	HTTPS	
		Durchsatz beim Lesen	Implementiert	HTTPS	
		Durchsatz gesamt	Implementiert	HTTPS	Durchschnittliche Gesamtrate der Festplatte (Lesen und Schreiben auf allen Festplatten) in MB/s
		Durchsatz beim Schreiben	Implementiert	HTTPS	
	Volumen	Latenz gesamt	Implementiert	HTTPS	
		IOPs gelesen	Implementiert	HTTPS	Anzahl der gelesenen IOPs auf der Festplatte
		Latenz beim Lesen	Implementiert	HTTPS	
		IOPs Schreiben	Implementiert	HTTPS	
		Durchsatz beim Lesen	Implementiert	HTTPS	
		Durchsatz beim Schreiben	Implementiert	HTTPS	
		Durchsatz gesamt	Implementiert	HTTPS	Durchschnittliche Gesamtrate der Festplatte (Lesen und Schreiben auf allen Festplatten) in MB/s
		IOPs gesamt	Implementiert	HTTPS	
		Latenz beim Schreiben	Implementiert	HTTPS	

Von diesem Datensammler verwendete Verwaltungs-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschichtprotokoll	Verwendete eingehende Ports	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur schreibgeschützte Anmeldeinformationen	Unterstützt Verschlüsselung	Firewall-freundlich (statische Ports)
Nutanix REST API	HTTPS	HTTPS	443		true	true	true	true

OpenStack (REST-API / SSH)

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Stiftung					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Knotenname	Implementiert	HTTPS	
		OID	Implementiert	HTTPS	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
		Typ	Lücke	HTTPS	
	Info	Datenquellenname	Implementiert	HTTPS	Info
		Datum	Implementiert	HTTPS	
		Absender-ID	Implementiert	HTTPS	
		Urheberschlüssel	Implementiert	HTTPS	
Leistung	Gastgeber	Gesamte CPU-Auslastung	Implementiert		
		Schlüssel	Implementiert		
		Gesamtspeicherauslastung	Implementiert		
		Server-ID	Implementiert		

Von diesem Datensammler verwendete Verwaltungs-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschichtprotokoll	Verwendete eingehende Ports	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur schreibgeschützte Anmeldeinformationen	Unterstützt Verschlüsselung	Firewall-freundlich (statische Ports)
OpenStack REST API	HTTPS	HTTPS	443		true	FALSCH	true	true
OpenStack SSH	SSH	SSH	22		true	FALSCH	true	true

Oracle ZFS (HTTPS)

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
Sun ZFS-Speicher 7120 Sun ZFS-Speicher 7320 Sun ZFS-Speicher 7330 Sun ZFS-Speicher 7335 Sun ZFS-Speicher 7350 Sun ZFS-Speicher 7370 Sun ZFS-Speicher 7390 Sun ZFS-Speicher 7420	1-1.1 1-1.2 1-1.3 1-1.34 1-1.4 2013.06.05.6.12 2013.06.05.6.15 2013.06.05.7.21 2013.06.05.7.24 2013.06.05.7.25 2013.06.05.7.26 2013.06.05.7.29 2013.06.05.8.0 2013.06.05.8.26 2013.06.05.8.29 2013.06.05.8.37 2013.06.05.8.44 2013.06.05.8.50 2013.06.05.8.53 2013.06.05.8.56 2013.06.05.8.6 2013.06.05.8.61 2013.06.05.8.65 2013.06.05.8.7 2013.06.05.8.72 2013.06.05.8.74 2013.06.05.8.76

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Stiftung					
1366					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Kapazität			
		Virtuell	Implementiert	HTTP/S	Ist dies ein Gerät zur Speichervirtualisierung?
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	Volumenkarte	LUN	Implementiert	HTTP/S	Name der Backend-LUN
		Maskierung erforderlich	Implementiert	HTTP/S	
		Protokoll-Controller	Implementiert	HTTP/S	
		Speicherport	Implementiert	HTTP/S	
		Typ	Lücke	HTTP/S	
	Volumenmaske	Initiator	Implementiert	HTTP/S	
		Protokoll-Controller	Implementiert	HTTP/S	
		Speicherport	Implementiert	HTTP/S	
		Typ	Lücke	HTTP/S	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Leistung					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Durchsatz beim Schreiben	Implementiert		
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	Speicherknotendaten	Cache-Trefferquote gesamt	Implementiert		
		IOPs gelesen	Implementiert		Anzahl der gelesenen IOPs auf der Festplatte
		IOPs gesamt	Implementiert		
		IOPs Schreiben	Implementiert		
		Schlüssel	Implementiert		
		Server-ID	Implementiert		
		Durchsatz beim Lesen	Implementiert		
		Durchsatz gesamt	Implementiert		Durchschnittliche Gesamtrate der Festplatte (Lesen und Schreiben auf allen Festplatten) in MB/s
		Durchsatz beim Schreiben	Implementiert		
		Auslastung gesamt	Implementiert		
	StoragePool-Datenträger	IOPs gesamt	Implementiert		

Von diesem Datensammler verwendete Verwaltungs-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschichtprotokoll	Verwendete eingehende Ports	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur schreibgeschützte Anmeldeinformationen	Unterstützt Verschlüsselung	Firewall-freundlich (statische Ports)
Oracle ZFS REST-API	HTTP/HTTPS	HTTP/HTTPS	215		true	true	true	true

Pure Storage FlashArray (HTTP)

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
DFSC1 FA-450 FA-C40R3 FA-C50R4 FA-C60 FA-C60R3 FA-C70R4 FA-C90R4 FA-X10R2 FA-X10R3 FA-X20R2 FA-X20R3 FA-X20R4 FA-X50R2 FA-X50R3 FA-X50R4 FA-X70R2 FA-X70R3 FA-X70R4 FA-X90R2 FA-X90R3 FA-X90R4 FA-XL130 FA-XL170 FA-m20 FA-m20r2 FA-m50 FA-m70 FA-m70r2 SAUERSTOFF	5.3.14 5.3.20 6.1.10 6.1.14 6.1.18 6.1.19 6.1.21 6.1.22 6.1.23 6.2.10 6.3.10 6.3.11 6.3.12 6.3.13 6.3.14 6.3.15 6.3.16 6.3.17 6.3.18 6.3.3 6.3.6 6.3.7 6.3.9 6.4.10 6.4.2 6.4.3 6.4.7 6.4.8 6.4.9 6.5.0 6.5.1 6.5.2 6.5.3 6.5.4 6.5.5 6.5.6 6.5.7 6.5.8 6.5.9 6.6.10 6.6.11 6.6.5 6.6.6 6.6.7 6.7.0 6.7.1 6.8.1 6.8.2 6.8.3

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Stiftung					
1380					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

					Volume geschrieben wurde, in MB
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Funktion/Attribut aktiviert	Implementiert	HTTP/S	
	Volumenkarte	LUN	Implementiert	HTTP/S	Name der Backend-LUN
		Protokoll-Controller	Implementiert	HTTP/S	
		Speicherport	Implementiert	HTTP/S	
		Typ	Lücke	HTTP/S	
	Volumenmaske	Initiator	Implementiert	HTTP/S	
		Protokoll-Controller	Implementiert	HTTP/S	
		Speicherport	Implementiert	HTTP/S	
		Typ	Lücke	HTTP/S	
	WWN-Alias	Host-Aliase	Implementiert	HTTP/S	
		Objekttyp	Implementiert	HTTP/S	
		Quelle	Implementiert	HTTP/S	
		WWN	Implementiert	HTTP/S	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Leistung					
1388					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Kapazität			
		Snapshot-Verhältnis der genutzten Kapazität	Implementiert		Als Zeitreihe gemeldet
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	Volumen	Rohkapazität	Implementiert		
		Gesamtkapazität	Implementiert		
		Verwendete Kapazität	Implementiert		
		Verhältnis der genutzten Kapazität	Implementiert		
		IOPs gelesen	Implementiert		Anzahl der gelesenen IOPs auf der Festplatte
		IOPs gesamt	Implementiert		
		IOPs Schreiben	Implementiert		
		Latenz beim Lesen	Implementiert		
		Latenz gesamt	Implementiert		
		Latenz beim Schreiben	Implementiert		
		Durchsatz beim Lesen	Implementiert		
		Durchsatz gesamt	Implementiert		Durchschnittliche Gesamtrate der Festplatte (Lesen und Schreiben auf allen Festplatten) in MB/s
		Durchsatz beim Schreiben	Implementiert		

Von diesem Datensammler verwendete Verwaltungs-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschichtprotokoll	Verwendete eingehende Ports	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur schreibgeschützte Anmeldeinformationen	Unterstützt Verschlüsselung	Firewall-freundlich (statische Ports)
Pure Storage REST-API	HTTP/HTTPS	HTTP/HTTPS	80/443		true	true	true	true

Red Hat RHV (REST)

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Stiftung					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Name	Implementiert	HTTP/S	
		OID	Implementiert	HTTP/S	
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Plattformtyp	Implementiert	HTTP/S	
	ISCSI-Knoten	Knotenname	Implementiert	HTTP/S	
		OID	Implementiert	HTTP/S	
		Typ	Lücke	HTTP/S	
	Info	Datenquellenname	Implementiert	HTTP/S	Info
		Datum	Implementiert	HTTP/S	
		Absender-ID	Implementiert	HTTP/S	

Von diesem Datensammler verwendete Verwaltungs-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschichtprotokoll	Verwendete eingehende Ports	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur schreibgeschützte Anmeldeinformationen	Unterstützt Verschlüsselung	Firewall-freundlich (statische Ports)
Red Hat RHEV REST API	HTTPS	HTTPS	443		true	true	true	true

Rubrik Storage

Von diesem Datensammler unterstützte Modelle und Versionen: Firmware-Versionen:

- 8.1.3-p12-25506
- 8.1.3-p13-25544
- 8.1.3-p2-24912
- 9.0.3-p10-25744
- 9.0.3-p5-25595
- 9.0.3-p6-25611
- 9.1.1-27527
- 9.1.2-27824
- 9.1.2-p1-27870
- 9.1.2-p1-27870_HP1473894
- 9.1.3-p1-28075
- 9.1.3-p8-28434
- 9.2.2-p1-29213
- 9.2.3-29313
- 9.2.3-p1-29368

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Stiftung					
1398					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Gesamte genutzte Kapazität	Implementiert	HTTPS	Gesamtkapazität in MB
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Typ	Lücke	HTTPS	
		Virtuell	Implementiert	HTTPS	Ist dies ein Gerät zur Speichervirtualisierung?
		Effektiv genutzte Kapazität in Prozent	Implementiert	HTTPS	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Leistung					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Durchsatz beim Schreiben	Implementiert	HTTPS	
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	StoragePool-Datenträger	IOPs gelesen	Implementiert	HTTPS	Anzahl der gelesenen IOPs auf der Festplatte
		IOPs Schreiben	Implementiert	HTTPS	
		Durchsatz beim Lesen	Implementiert	HTTPS	
		Durchsatz beim Schreiben	Implementiert	HTTPS	
		Durchsatz gesamt	Implementiert	HTTPS	Durchschnittliche Gesamtrate der Festplatte (Lesen und Schreiben auf allen Festplatten) in MB/s
		IOPs gesamt	Implementiert	HTTPS	
		Gesamtkapazität	Implementiert	HTTPS	
		Verwendete Kapazität	Implementiert	HTTPS	
		Andere genutzte Kapazität	Implementiert	HTTPS	
		Rohkapazität	Implementiert	HTTPS	
		Verhältnis der genutzten Kapazität	Implementiert	HTTPS	
		Verwendete Datenkapazität	Implementiert	HTTPS	
		Snapshot der genutzten Kapazität	Implementiert	HTTPS	

Von diesem Datensammler verwendete Verwaltungs-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschichtprotokoll	Verwendete eingehende Ports	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur schreibgeschützte Anmeldeinformationen	Unterstützt Verschlüsselung	Firewall-freundlich (statische Ports)
Rubrik Storage REST API	HTTPS	HTTPS	443		true	true	true	true

VAST DataStore

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
VA2437096 VAST-Daten	Build-Version: Release-5.0.0-sp24-1389206 Build-Version: Release-5.0.0-sp24-1389206 Build-Version: Release-5.0.0-sp70-1532643 Build-Version: Release-5.1.0-sp50-1578267 Build-Version: Release-5.1.0-sp51-hf3-1643358 Build-Version: Release-5.1.0-sp56-1630237 Build-Version: Release-5.1.0-sp56-hf10-1682647 Build-Version: Release-5.1.0-sp56-hf14-1700467 Systemversion: 5.0.0.94 Systemversion: 5.0.0.133 Systemversion: 5.0.0.94 Systemversion: 5.1.0.210 Systemversion: 5.1.0.231

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Stiftung					
1408					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Snapshot der genutzten Kapazität	Implementiert	HTTPS	
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Speicherpool-ID	Implementiert	HTTPS	
		Thin Provisioning wird unterstützt	Implementiert	HTTPS	Ob dieses interne Volume Thin Provisioning für die darüber liegende Volume-Schicht unterstützt
		Gesamtzugewiesene Kapazität	Implementiert	HTTPS	
		Gesamte genutzte Kapazität	Implementiert	HTTPS	Gesamtkapazität in MB
		Typ	Lücke	HTTPS	
		Virtuell	Implementiert	HTTPS	Ist dies ein Gerät zur Speichervirtualisierung?
		Verschlüsselt	Implementiert	HTTPS	
	Speicher-VirtualMachine	Zugewiesene Kapazität (MB)	Implementiert	HTTPS	Zugewiesene Kapazität der Snapshots
		Kommentar	Implementiert	HTTPS	
		Guid-Schlüssel	Implementiert	HTTPS	Global eindeutiger Schlüssel der virtuellen Speichermaschine
		Name	Implementiert	HTTPS	
		Typ	Lücke	HTTPS	
		UUID	Implementiert	HTTPS	
		Verwendete Kapazität	Implementiert	HTTPS	
	Referenz des internen Volumes der virtuellen Maschine	Interne Volume-ID	Implementiert	HTTPS	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Leistung	Storage	Fehlgeschlagene Rohkapazität	Implementiert	HTTPS	
		Rohkapazität	Implementiert	HTTPS	
		Freie Rohkapazität	Implementiert	HTTPS	Rohkapazität der Ersatzfestplatten (Summe aller Ersatzfestplatten)
		Speicherpool-Kapazität	Implementiert	HTTPS	
		IO-Dichte lesen	Implementiert	HTTPS	
		IO-Dichte gesamt	Implementiert	HTTPS	
		Schreib-E/A-Dichte	Implementiert	HTTPS	
		IOPs andere	Implementiert	HTTPS	
		IOPs gelesen	Implementiert	HTTPS	Anzahl der gelesenen IOPs auf der Festplatte
		IOPs gesamt	Implementiert	HTTPS	
		IOPs Schreiben	Implementiert	HTTPS	
		Schlüssel	Implementiert	HTTPS	
		Latenz beim Lesen	Implementiert	HTTPS	
		Latenz gesamt	Implementiert	HTTPS	
		Latenz beim Schreiben	Implementiert	HTTPS	
		Server-ID	Implementiert	HTTPS	
		Durchsatz beim Lesen	Implementiert	HTTPS	
		Durchsatz gesamt	Implementiert	HTTPS	Durchschnittliche Gesamtrate der Festplatte (Lesen und Schreiben auf allen Festplatten) in MB/s
		Durchsatz beim Schreiben	Implementiert	HTTPS	

Von diesem Datensammler verwendete Verwaltungs-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschichtprotokoll	Verwendete eingehende Ports	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur schreibgeschützte Anmeldeinformationen	Unterstützt Verschlüsselung	Firewall-freundlich (statische Ports)
VAST DataStore API	HTTPS	HTTPS	443		true	true	true	true

NetApp HCI Virtual Center

Von diesem Datensammler unterstützte Modelle und Versionen: API-Versionen:

- VMware vCenter Server 6.7.0 Build-10244857
- VMware vCenter Server 7.0.3 Build-20395099

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Stiftung					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

	VirtualMachine-Festplatte	OID	Implementiert	Webdienste	
		VirtualMachine-OID	Implementiert	Webdienste	
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		VirtualDisk-OID	Implementiert	Webdienste	
	Gastgeber	Host-CPU-Anzahl	Implementiert	Webdienste	
		Host-CPU-Geschwindigkeit	Implementiert	Webdienste	
		Hostdomäne	Implementiert	Webdienste	
		Vom Host installierter Speicher	Implementiert	Webdienste	
		Hostmodell	Implementiert	Webdienste	
		NIC-Anzahl	Implementiert	Webdienste	
		NIC-Geschwindigkeit	Implementiert	Webdienste	
		IP-Adressen	Implementiert	Webdienste	
		Hersteller	Implementiert	Webdienste	
		Name	Implementiert	Webdienste	
		OID	Implementiert	Webdienste	
		Plattformtyp	Implementiert	Webdienste	
	ISCSI-Knoten	Host-Aliase	Implementiert	Webdienste	
		Knotenname	Implementiert	Webdienste	
		OID	Implementiert	Webdienste	
		Typ	Lücke	Webdienste	
	Info	API-Beschreibung	Implementiert	Webdienste	
		API-Name	Implementiert	Webdienste	
		API-Version	Implementiert	Webdienste	
		Client-API-Name	Implementiert	Webdienste	
		Client-API-Version	Implementiert	Webdienste	
		Datenquellenname	Implementiert	Webdienste	Info
		Datum	Implementiert	Webdienste	
		Absender-ID	Implementiert	Webdienste	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Leistung					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Festplattendurchsatz beim Schreiben	Implementiert	Webdienste	
Produkt	**Kategorie**	**Leistungsmerkmale**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Festplatten-Auslastung	Implementiert	Webdienste	
		Wartezeit einplanen	Implementiert	Webdienste	Wartezeit auf die Planung in Prozent
		diskIops.total	Implementiert	Webdienste	
		Gesamt-Swapsatz	Implementiert	Webdienste	
		Durchsatz beim Lesen	Implementiert	Webdienste	Gesamtdurchsatz der Festplatte beim Lesen

Von diesem Datensammler verwendete Verwaltungs-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschichtprotokoll	Verwendete eingehende Ports	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur schreibgeschützte Anmeldeinformationen	Unterstützt Verschlüsselung	Firewall-freundlich (statische Ports)
VMware REST API	Webdienste	HTTP/HTTPS	80/443		true	true	true	true

VMware Cloud auf AWS

Von diesem Datensammler unterstützte Modelle und Versionen: API-Versionen:

- VMware vCenter Server 7.0.3 Build-21477706
- VMware vCenter Server 7.0.3 Build-24322018
- VMware vCenter Server 8.0.0 Build-22877852
- VMware vCenter Server 8.0.1 Build-22161730
- VMware vCenter Server 8.0.1 Build-23525738
- VMware vCenter Server 8.0.3 Build-24322831

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Stiftung					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

	VirtualMachine-Festplatte	OID	Implementiert	Webdienste	
		VirtualDisk-OID	Implementiert	Webdienste	
Produkt	**Kategorie**	**Funktionsattribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		VirtualMachine-OID	Implementiert	Webdienste	
	Gastgeber	Host-CPU-Anzahl	Implementiert	Webdienste	
		Host-CPU-Geschwindigkeit	Implementiert	Webdienste	
		Hostdomäne	Implementiert	Webdienste	
		Vom Host installierter Speicher	Implementiert	Webdienste	
		Hostmodell	Implementiert	Webdienste	
		NIC-Anzahl	Implementiert	Webdienste	
		NIC-Geschwindigkeit	Implementiert	Webdienste	
		IP-Adressen	Implementiert	Webdienste	
		Hersteller	Implementiert	Webdienste	
		Name	Implementiert	Webdienste	
		OID	Implementiert	Webdienste	
		Plattformtyp	Implementiert	Webdienste	
	Info	API-Beschreibung	Implementiert	Webdienste	
		API-Name	Implementiert	Webdienste	
		API-Version	Implementiert	Webdienste	
		Client-API-Name	Implementiert	Webdienste	
		Client-API-Version	Implementiert	Webdienste	
		Datenquellenname	Implementiert	Webdienste	Info
		Datum	Implementiert	Webdienste	
		Absender-ID	Implementiert	Webdienste	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Leistung	Gastgeber	Gesamte CPU-Auslastung	Implementiert	Webdienste	
		IOPs gelesen	Implementiert	Webdienste	Anzahl der gelesenen IOPs auf der Festplatte
		diskIops.total	Implementiert	Webdienste	
		Festplatten-IOPs beim Schreiben	Implementiert	Webdienste	
		Latenz beim Lesen	Implementiert	Webdienste	
		Latenz gesamt	Implementiert	Webdienste	
		Latenz beim Schreiben	Implementiert	Webdienste	
		Festplattendurchsatz beim Lesen	Implementiert	Webdienste	
		Durchsatz beim Lesen	Implementiert	Webdienste	Gesamtdurchsatz der Festplatte beim Lesen
		Festplattendurchsatz beim Schreiben	Implementiert	Webdienste	
		IP-Durchsatz beim Lesen	Implementiert	Webdienste	
		Durchsatz gesamt	Implementiert	Webdienste	IP-Durchsatz gesamt
		ipThroughput.write	Implementiert	Webdienste	
		Schlüssel	Implementiert	Webdienste	
		Gesamtspeicherauslastung	Implementiert	Webdienste	
		Server-ID	Implementiert	Webdienste	
		swapRate.inRate	Implementiert	Webdienste	
		Swapsatz	Implementiert	Webdienste	
		Gesamt-Swapsatz	Implementiert	Webdienste	

Von diesem Datensammler verwendete Verwaltungs-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschichtprotokoll	Verwendete eingehende Ports	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur schreibgeschützte Anmeldeinformationen	Unterstützt Verschlüsselung	Firewall-freundlich (statische Ports)
VMware REST API	Webdienste	HTTP/HTTPS	80/443		true	true	true	true

VMware vSphere (Webdienste)

Von diesem Datensammler unterstützte Modelle und Versionen: API-Versionen:

- VMware ESXi 6.0.0 Build-10474991
- VMware ESXi 6.0.0 Build-10719132
- VMware ESXi 6.0.0 Build-13635687
- VMware ESXi 6.0.0 Build-2494585
- VMware ESXi 6.0.0 Build-3620759
- VMware ESXi 6.0.0 Build-5050593
- VMware ESXi 6.0.0 Build-5224934
- VMware ESXi 6.0.0 Build-9239799
- VMware ESXi 6.5.0 Build-5310538
- VMware ESXi 7.0.3 Build-20036589
- VMware ESXi 7.0.3 Build-20328353
- VMware ESXi 8.0.0 Build-21203435
- VMware ESXi 8.0.1 Build-21495797
- VMware vCenter Server 5.0.0 Build-623373
- VMware vCenter Server 5.5.0 Build-1750787
- VMware vCenter Server 5.5.0 Build-2442329
- VMware vCenter Server 5.5.0 Build-3252642
- VMware vCenter Server 5.5.0 Build-6516310
- VMware vCenter Server 5.5.0 Build-9911218
- VMware vCenter Server 6.0.0 Build-13638472
- VMware vCenter Server 6.0.0 Build-14510545
- VMware vCenter Server 6.0.0 Build-2776511
- VMware vCenter Server 6.0.0 Build-3634793
- VMware vCenter Server 6.0.0 Build-5183551
- VMware vCenter Server 6.0.0 Build-9313458
- VMware vCenter Server 6.5.0 Build-10964411

- VMware vCenter Server 6.5.0 Build-12863991
- VMware vCenter Server 6.5.0 Build-15259038
- VMware vCenter Server 6.5.0 Build-17994927
- VMware vCenter Server 6.5.0 Build-18499837
- VMware vCenter Server 6.5.0 Build-18711281
- VMware vCenter Server 6.5.0 Build-20510539
- VMware vCenter Server 6.5.0 Build-22499743
- VMware vCenter Server 6.5.0 Build-5973321
- VMware vCenter Server 6.7.0 Build-10244857
- VMware vCenter Server 6.7.0 Build-11727113
- VMware vCenter Server 6.7.0 Build-14070654
- VMware vCenter Server 6.7.0 Build-14792544
- VMware vCenter Server 6.7.0 Build-15679289
- VMware vCenter Server 6.7.0 Build-17137232
- VMware vCenter Server 6.7.0 Build-17137327
- VMware vCenter Server 6.7.0 Build-18010560
- VMware vCenter Server 6.7.0 Build-18010599
- VMware vCenter Server 6.7.0 Build-18485185
- VMware vCenter Server 6.7.0 Build-18831049
- VMware vCenter Server 6.7.0 Build-19299595
- VMware vCenter Server 6.7.0 Build-19832280
- VMware vCenter Server 6.7.0 Build-20504301
- VMware vCenter Server 6.7.0 Build-20504362
- VMware vCenter Server 6.7.0 Build-22509751
- VMware vCenter Server 6.7.0 Build-24323669
- VMware vCenter Server 6.7.0 Build-8170161
- VMware vCenter Server 7.0.2 Build-17958471
- VMware vCenter Server 7.0.2 Build-18356314
- VMware vCenter Server 7.0.2 Build-18455184
- VMware vCenter Server 7.0.2 Build-22781136
- VMware vCenter Server 7.0.3 Build-18778458
- VMware vCenter Server 7.0.3 Build-19234570
- VMware vCenter Server 7.0.3 Build-19480866
- VMware vCenter Server 7.0.3 Build-19717403
- VMware vCenter Server 7.0.3 Build-20150588
- VMware vCenter Server 7.0.3 Build-20395099
- VMware vCenter Server 7.0.3 Build-20845200

- VMware vCenter Server 7.0.3 Build-20990077
- VMware vCenter Server 7.0.3 Build-21290409
- VMware vCenter Server 7.0.3 Build-21477706
- VMware vCenter Server 7.0.3 Build-21784236
- VMware vCenter Server 7.0.3 Build-21958406
- VMware vCenter Server 7.0.3 Build-22357613
- VMware vCenter Server 7.0.3 Build-22837322
- VMware vCenter Server 7.0.3 Build-23085514
- VMware vCenter Server 7.0.3 Build-23788036
- VMware vCenter Server 7.0.3 Build-24026615
- VMware vCenter Server 7.0.3 Build-24201990
- VMware vCenter Server 7.0.3 Build-24322018
- VMware vCenter Server 8.0.0 Build-20519528
- VMware vCenter Server 8.0.0 Build-20920323
- VMware vCenter Server 8.0.0 Build-21216066
- VMware vCenter Server 8.0.0 Build-21457384
- VMware vCenter Server 8.0.1 Build-21560480
- VMware vCenter Server 8.0.1 Build-21815093
- VMware vCenter Server 8.0.1 Build-21860503
- VMware vCenter Server 8.0.1 Build-22088981
- VMware vCenter Server 8.0.1 Build-22368047
- VMware vCenter Server 8.0.1 Build-24005165
- VMware vCenter Server 8.0.2 Build-22385739
- VMware vCenter Server 8.0.2 Build-22617221
- VMware vCenter Server 8.0.2 Build-23319993
- VMware vCenter Server 8.0.2 Build-23504390
- VMware vCenter Server 8.0.2 Build-23929136
- VMware vCenter Server 8.0.2 Build-24321653
- VMware vCenter Server 8.0.3 Build-24022515
- VMware vCenter Server 8.0.3 Build-24091160
- VMware vCenter Server 8.0.3 Build-24262322
- VMware vCenter Server 8.0.3 Build-24305161
- VMware vCenter Server 8.0.3 Build-24322831

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Stiftung					
1438					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
		Kapazität			
		Verwendete Kapazität	Implementiert	Webdienste	
		UUID	Implementiert	Webdienste	
	VirtualMachine-Festplatte	OID	Implementiert	Webdienste	
		VirtualDisk-OID	Implementiert	Webdienste	
		VirtualMachine-OID	Implementiert	Webdienste	
	Gastgeber	Host-CPU-Anzahl	Implementiert	Webdienste	
		Host-CPU-Geschwindigkeit	Implementiert	Webdienste	
		Hostdomäne	Implementiert	Webdienste	
		Vom Host installierter Speicher	Implementiert	Webdienste	
		Hostmodell	Implementiert	Webdienste	
		NIC-Anzahl	Implementiert	Webdienste	
		NIC-Geschwindigkeit	Implementiert	Webdienste	
		IP-Adressen	Implementiert	Webdienste	
		Hersteller	Implementiert	Webdienste	
		Name	Implementiert	Webdienste	
		OID	Implementiert	Webdienste	
		Plattformtyp	Implementiert	Webdienste	
	ISCSI-Knoten	Host-Aliase	Implementiert	Webdienste	
		Knotenname	Implementiert	Webdienste	
		OID	Implementiert	Webdienste	
		Typ	Lücke	Webdienste	
	Info	API-Beschreibung	Implementiert	Webdienste	
		API-Name	Implementiert	Webdienste	
		API-Version	Implementiert	Webdienste	
		Client-API-Name	Implementiert	Webdienste	
		Client-API-Version	Implementiert	Webdienste	
		Datenquellenname	Implementiert	Webdienste	Info
		Datum	Implementiert	Webdienste	
		Absender-ID	Implementiert	Webdienste	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Leistung					
1442					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Festplattendurchsatz beim Schreiben	Implementiert	Webdienste	
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Durchsatz beim Lesen	Implementiert	Webdienste	
		Durchsatz gesamt	Implementiert	Webdienste	IP-Durchsatz gesamt
		ipThroughput.write	Implementiert	Webdienste	
		Gesamtspeicherauslastung	Implementiert	Webdienste	
		swapRate.inRate	Implementiert	Webdienste	
		Swapsatz	Implementiert	Webdienste	
		Gesamt-Swapsatz	Implementiert	Webdienste	
		Wartezeit einplanen	Implementiert	Webdienste	Wartezeit auf die Planung in Prozent

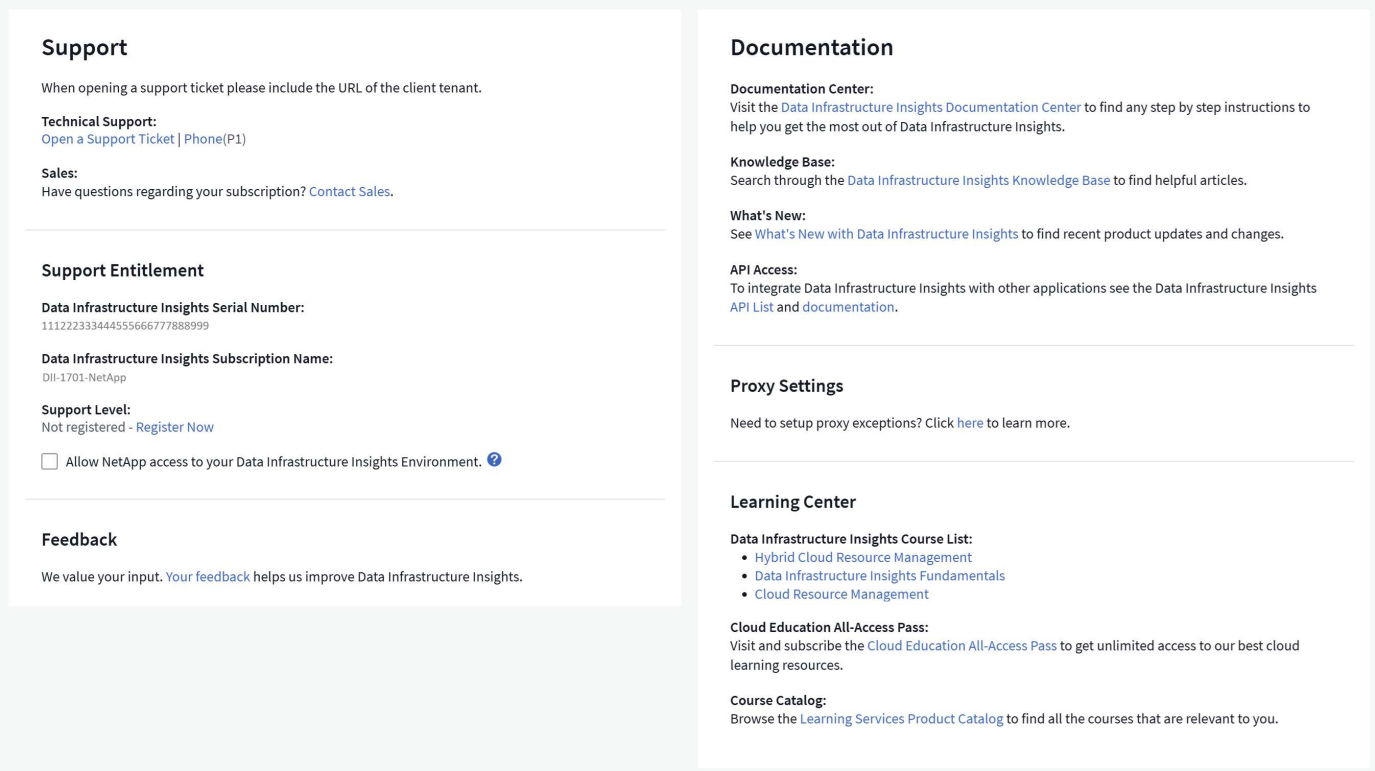
Von diesem Datensammler verwendete Verwaltungs-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschichtprotokoll	Verwendete eingehende Ports	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur schreibgeschützte Anmeldeinformationen	Unterstützt Verschlüsselung	Firewall-freundlich (statische Ports)
VMware REST API	Webdienste	HTTP/HTTPS	80/443		true	true	true	true

Referenz & Support

Support anfordern

Sie können auf die verfügbaren Supportoptionen in Data Infrastructure Insights zugreifen, indem Sie **Hilfe > Support** auswählen.



Supportanspruch aktivieren

Data Infrastructure Insights bietet im Testmodus Self-Service- und E-Mail-Support. Sobald Sie den Dienst abonniert haben, wird dringend empfohlen, den Supportanspruch zu aktivieren. Durch die Aktivierung der Supportberechtigung erhalten Sie Zugriff auf den technischen Support über das Web-Ticketsystem und per Telefon. Der Standard-Supportmodus ist Selbstbedienung, bis die Registrierung abgeschlossen ist. SehenDetails unten.

Während des ersten Abonnementvorgangs generiert Ihre Data Infrastructure Insights -Instanz eine 20-stellige NetApp -Seriennummer, die mit „950“ beginnt. Diese NetApp Seriennummer stellt das mit Ihrem Konto verknüpfte Data Infrastructure Insights -Abonnement dar. Sie müssen die NetApp Seriennummer registrieren, um den Supportanspruch zu aktivieren. Wir bieten zwei Möglichkeiten zur Support-Registrierung:

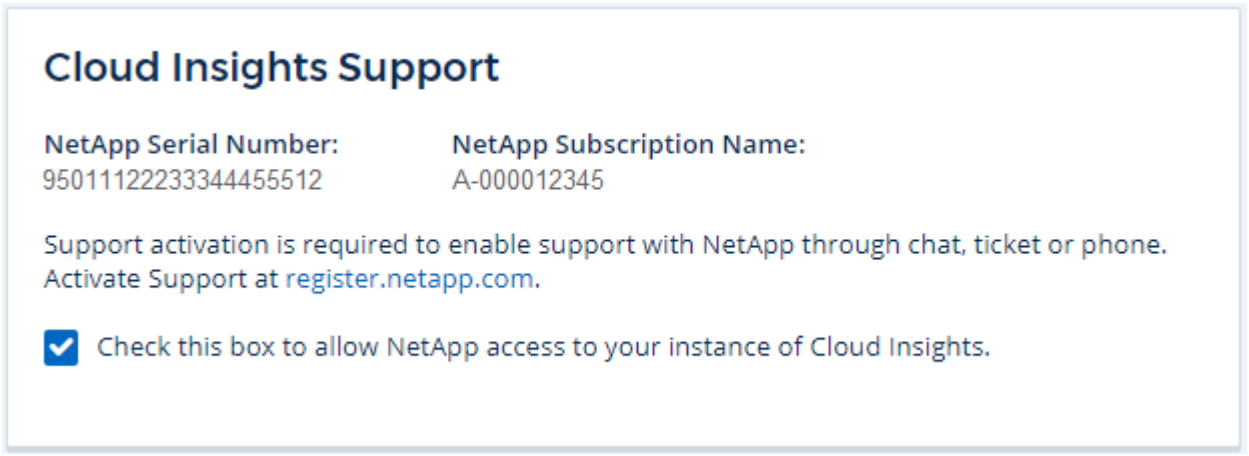
1. Benutzer mit bereits vorhandenem NetApp Support Site (NSS) SSO-Konto (z. B. aktueller NetApp Kunde)
2. Neuer NetApp Kunde ohne bereits vorhandenes SSO-Konto für die NetApp Support Site (NSS)

Option 1: Schritte für einen Benutzer mit einem bereits vorhandenen NetApp Support Site (NSS) SSO-Konto

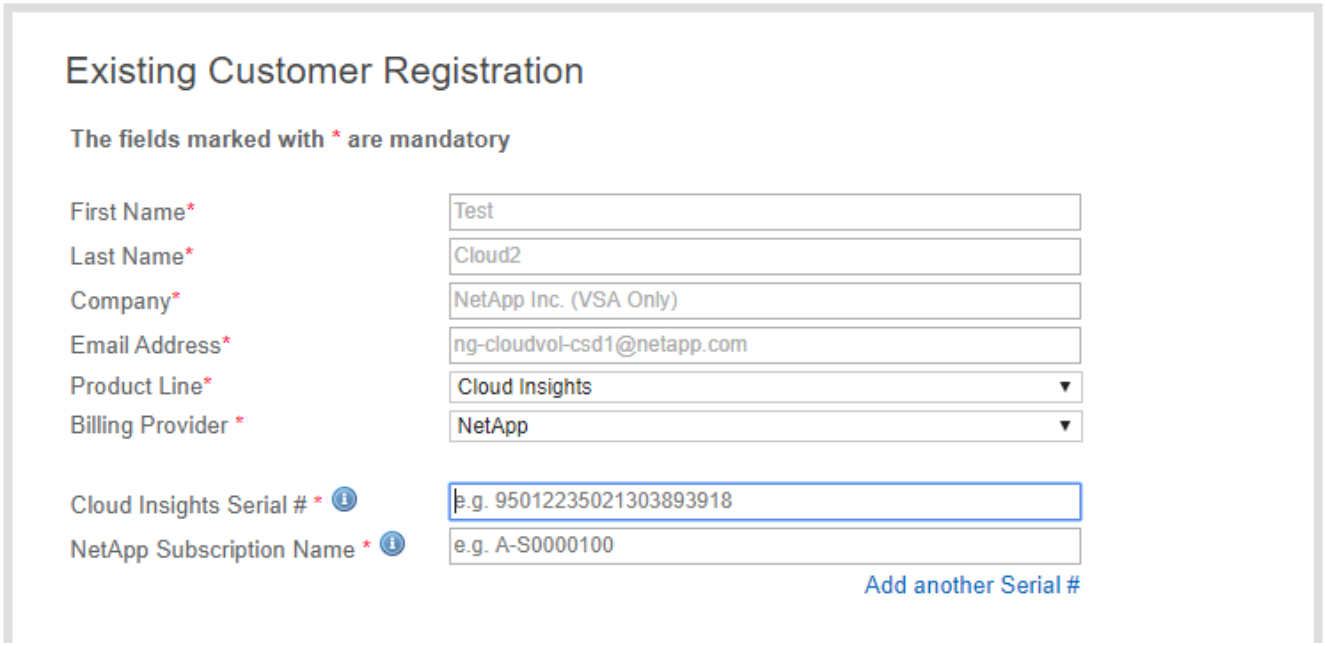
Schritte

1. Navigieren Sie zur NetApp -Registrierungswebsite https://register.netapp.com

2. Wählen Sie „Ich bin bereits als NetApp -Kunde registriert“ und wählen Sie *Data Infrastructure Insights* als Produktlinie. Wählen Sie Ihren Abrechnungsanbieter (NetApp oder AWS) aus und geben Sie Ihre Seriennummer und Ihren NetApp Abonnementnamen oder Ihre AWS-Kunden-ID ein, indem Sie auf das Menü „Hilfe > Support“ in der Benutzeroberfläche von Data Infrastructure Insights verweisen:



3. Füllen Sie das Registrierungsformular für Bestandskunden aus und klicken Sie auf **Senden**.



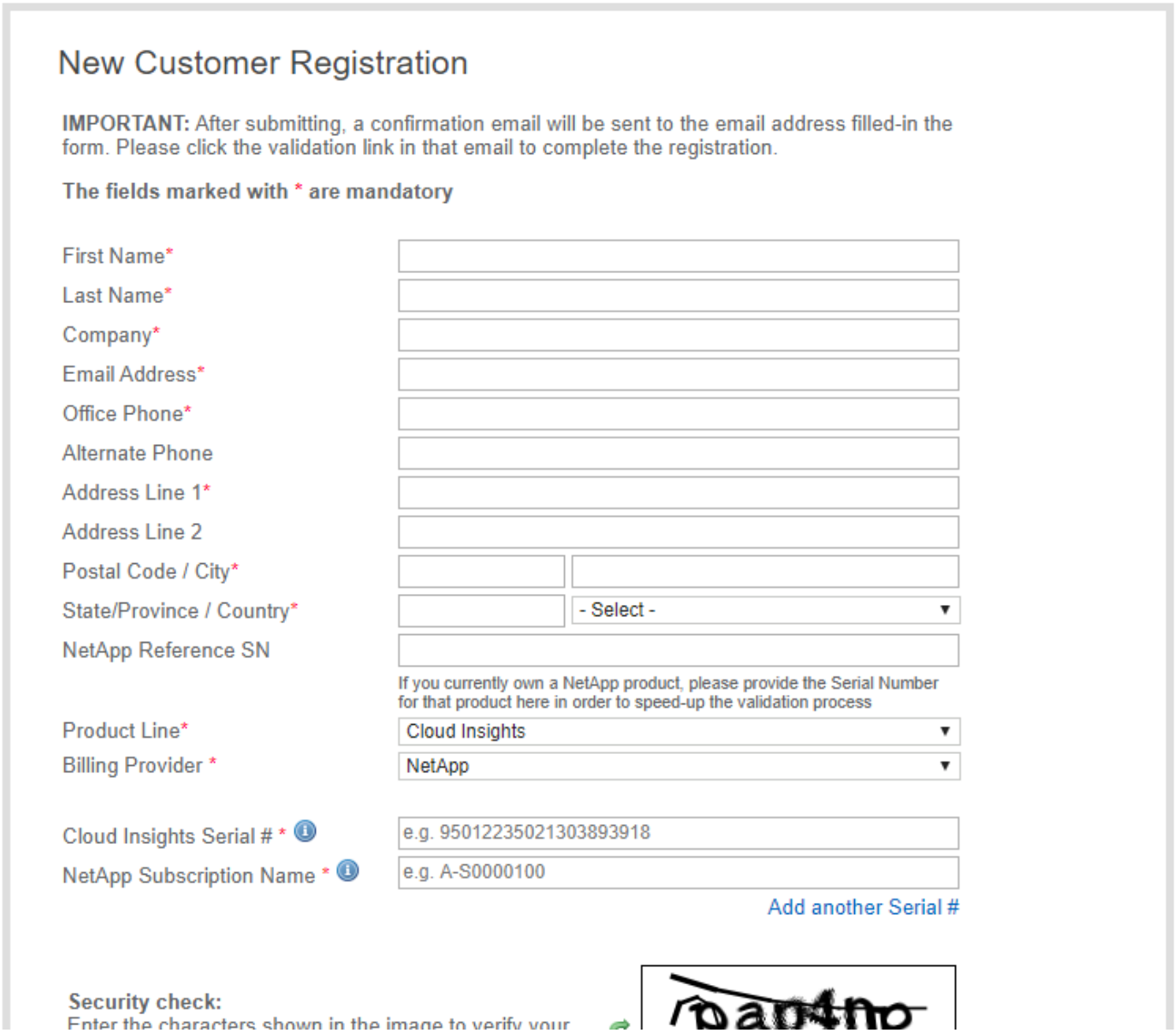
4. Wenn keine Fehler auftreten, wird der Benutzer auf die Seite „Registrierung erfolgreich übermittelt“ weitergeleitet. An die E-Mail-Adresse, die mit dem für die Registrierung verwendeten NSS SSO-Benutzernamen verknüpft ist, wird innerhalb weniger Minuten eine E-Mail mit der Meldung „Für Ihr Produkt besteht jetzt Anspruch auf Support“ gesendet.
5. Dies ist eine einmalige Registrierung für die Data Infrastructure Insights NetApp -Seriennummer.

Option 2: Schritte für einen neuen NetApp Kunden ohne bereits vorhandenes NetApp Support Site (NSS) SSO-Konto

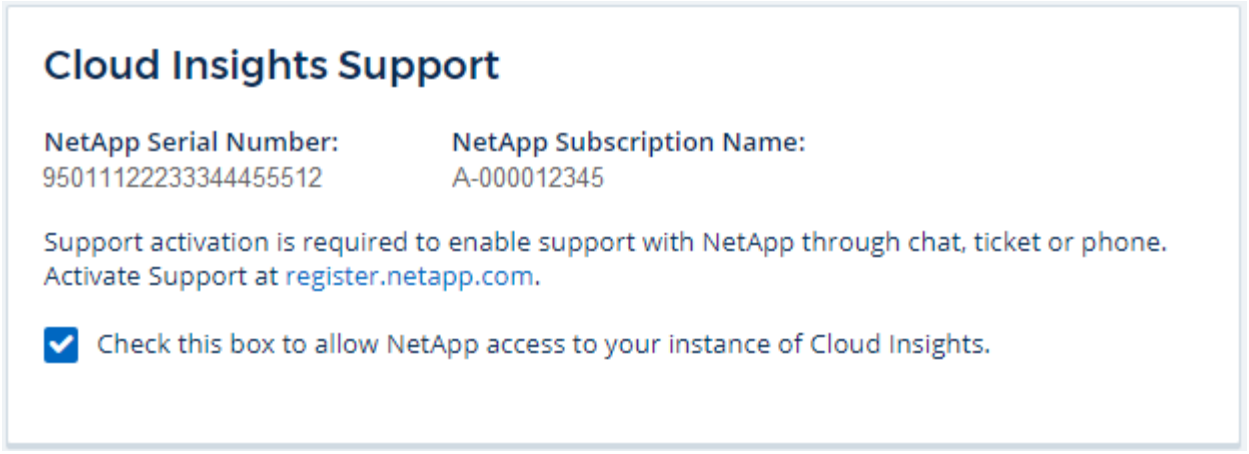
Schritte

1. Navigieren Sie zur NetApp -Registrierungswebsite https://register.netapp.com
2. Wählen Sie „Ich bin kein registrierter NetApp -Kunde“ und geben Sie die erforderlichen Informationen im

folgenden Beispielformular ein:



1. Wählen Sie *Data Infrastructure Insights* als Produktlinie aus. Wählen Sie Ihren Abrechnungsanbieter (NetApp oder AWS) aus und geben Sie Ihre Seriennummer und Ihren NetApp Abonnementnamen oder Ihre AWS-Kunden-ID ein, indem Sie auf das Menü „Hilfe > Support“ in der Benutzeroberfläche von Data Infrastructure Insights verweisen:



2. Wenn keine Fehler auftreten, wird der Benutzer auf die Seite „Registrierung erfolgreich übermittelt“ weitergeleitet. An die E-Mail-Adresse, die mit dem für die Registrierung verwendeten NSS SSO-Benutzernamen verknüpft ist, wird innerhalb weniger Stunden eine E-Mail mit der Meldung „Für Ihr Produkt besteht jetzt Anspruch auf Support“ gesendet.
3. Als neuer NetApp Kunde müssen Sie außerdem ein Benutzerkonto für die NetApp Support Site (NSS) für zukünftige Registrierungen und den Zugriff auf das Support-Portal für technischen Support und Web-Ticketing erstellen. Dieser Link befindet sich unter https://mysupport.netapp.com/eservice/public/now.do . Sie können Ihre neu registrierte Data Infrastructure Insights -Seriennummer angeben, um den Vorgang zu beschleunigen.
4. Dies ist eine einmalige Registrierung für die Data Infrastructure Insights NetApp Seriennummer.

Supportinformationen erhalten

NetApp bietet auf vielfältige Weise Unterstützung für Data Infrastructure Insights . Umfangreiche kostenlose Self-Support-Optionen stehen rund um die Uhr zur Verfügung, beispielsweise Knowledgebase-Artikel (KB) oder die NetApp Community. Für Benutzer, die Data Infrastructure Insights abonniert haben, steht technischer Support per Telefon oder Webticket zur Verfügung. Für Webtickets und das Fallmanagement ist ein SSO-Konto der NetApp Support Site (NSS) erforderlich.

Self-Service-Support:

Diese Supportoptionen sind im Testmodus verfügbar und stehen rund um die Uhr kostenlos zur Verfügung:

- **Wissensdatenbank**

  Wenn Sie auf die Links in diesem Abschnitt klicken, gelangen Sie zur NetApp Knowledgebase, wo Sie relevante Artikel, Anleitungen und mehr durchsuchen können.

- *"Dokumentation" *

  Wenn Sie auf den Link „Dokumentation“ klicken, gelangen Sie zu diesem Dokumentationscenter.

- *"Gemeinschaft" *

  Wenn Sie auf den Community-Link klicken, gelangen Sie zur NetApp Data Infrastructure Insights -Community, wo Sie sich mit Kollegen und Experten vernetzen können.

Es gibt auch einen Link zum Angeben**"Rückmeldung"** um uns bei der Verbesserung von Data Infrastructure Insights zu unterstützen.

Abonnement-Support

Wenn Sie über ein Data Infrastructure Insights Abonnement oder kostenpflichtigen Support für überwachte NetApp -Produkte oder -Services verfügen, können Sie zusätzlich zu den oben genannten Optionen zur Selbstunterstützung mit einem NetApp Supporttechniker zusammenarbeiten, um Ihr Problem zu lösen.

Sie müssen sich registrieren, umSupport aktivieren für NetApp Cloud-Produkte. Um sich zu registrieren, gehen Sie zu NetApp's"Registrierung für den Support von Cloud Data Services" .

Es wird dringend empfohlen, das Kontrollkästchen zu aktivieren, um einem NetApp -Supporttechniker während Ihrer Supportsitzung Zugriff auf Ihren Data Infrastructure Insights Mandanten zu gewähren. Dadurch kann der Techniker das Problem beheben und Ihnen helfen, es schnell zu lösen. Wenn Ihr Problem gelöst oder Ihre Support-Sitzung beendet ist, können Sie das Kontrollkästchen deaktivieren.

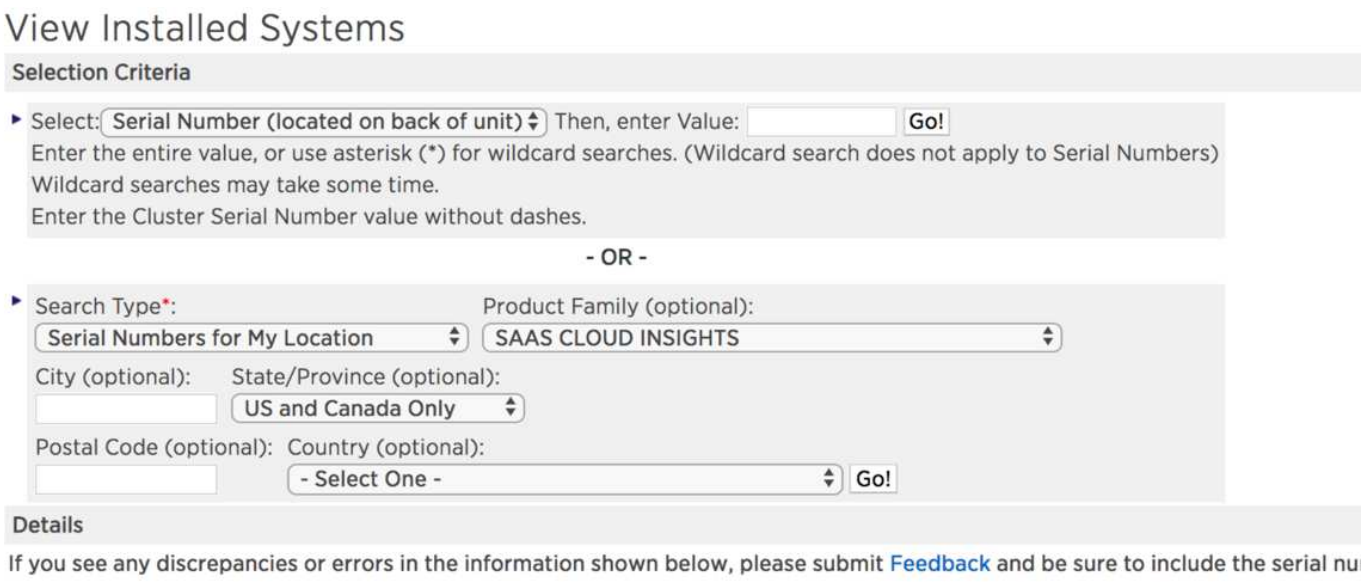
Sie können mit einer der folgenden Methoden Support anfordern. Sie müssen über ein aktives Data Infrastructure Insights -Abonnement verfügen, um diese Supportoptionen nutzen zu können:

- **"Telefon"**
- **"Support-Ticket"**

Sie können auch Vertriebsunterstützung anfordern, indem Sie auf den Link **Vertrieb kontaktieren** klicken.

Ihre Data Infrastructure Insights Seriennummer ist innerhalb des Dienstes im Menü **Hilfe > Support** sichtbar. Wenn Sie Probleme beim Zugriff auf den Dienst haben und zuvor eine Seriennummer bei NetApp registriert haben, können Sie Ihre Liste der Data Infrastructure Insights Seriennummern auch wie folgt auf der NetApp Support-Site anzeigen:

- Melden Sie sich bei mysupport.netapp.com an
- Verwenden Sie auf der Menüregisterkarte „Produkte“ > „Meine Produkte“ die Produktfamilie „SaaS Data Infrastructure Insights“, um alle Ihre registrierten Seriennummern zu finden:



Data Infrastructure Insights Datensammler-Supportmatrix

Informationen und Details zu unterstützten Datensammlern können Sie im* Data Infrastructure Insights Datensammler-Supportmatrix*, role= .

Lernzentrum

Unabhängig von Ihrem Abonnement finden Sie unter **Hilfe > Support** Links zu mehreren Kursangeboten der NetApp University, die Ihnen dabei helfen, Data Infrastructure Insights optimal zu nutzen. Schauen Sie sie sich an!

Datensammlerreferenz – Infrastruktur

Anbieterspezifische Referenz

Die Themen in diesem Abschnitt bieten anbieterspezifische Referenzinformationen. In den meisten Fällen ist die Konfiguration eines Datensammlers unkompliziert. In einigen Fällen benötigen Sie möglicherweise zusätzliche Informationen oder Befehle, um den Datensammler richtig zu konfigurieren.

Klicken Sie im Menü links auf einen **Anbieter**, um Informationen zu dessen Datensammlern anzuzeigen.

Konfigurieren des Amazon EC2-Datensammlers

Data Infrastructure Insights verwendet den Amazon EC2-Datensammler, um Bestands- und Leistungsdaten von EC2-Instances zu erfassen.

Anforderungen

Um Daten von Amazon EC2-Geräten zu erfassen, benötigen Sie die folgenden Informationen:

- Sie müssen über eines der folgenden Elemente verfügen:
  - Die **IAM-Rolle** für Ihr Amazon EC2-Cloud-Konto, wenn Sie die IAM-Rollenauthentifizierung verwenden. Die IAM-Rolle gilt nur, wenn Ihre Erfassungseinheit auf einer AWS-Instanz installiert ist.
  - Die **IAM-Zugriffsschlüssel**-ID und der geheime Zugriffsschlüssel für Ihr Amazon EC2-Cloud-Konto, wenn Sie die IAM-Zugriffsschlüssel-Authentifizierung verwenden.
- Sie müssen über die Berechtigung „Organisation auflisten“ verfügen
- Port 443 HTTPS
- EC2-Instanzen können als virtuelle Maschine oder (weniger natürlich) als Host gemeldet werden. EBS-Volumes können sowohl als von der VM verwendete VirtualDisk als auch als DataStore gemeldet werden, der die Kapazität für die VirtualDisk bereitstellt.

Zugriffsschlüssel bestehen aus einer Zugriffsschlüssel-ID (z. B. AKIAIOSFODNN7EXAMPLE) und einem geheimen Zugriffsschlüssel (z. B. wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY). Sie verwenden Zugriffsschlüssel, um programmgesteuerte Anfragen zu signieren, die Sie an EC2 stellen, wenn Sie die Amazon EC2 SDKs, REST oder Query-API-Operationen verwenden. Diese Schlüssel werden Ihnen mit Ihrem Vertrag von Amazon zur Verfügung gestellt.

Konfiguration

Geben Sie die Daten in die Felder des Datensammlers gemäß der folgenden Tabelle ein:

Feld	Beschreibung
AWS-Region	AWS-Region auswählen

Feld	Beschreibung
IAM-Rolle	Nur zur Verwendung, wenn es auf einer AU in AWS erworben wurde. Weitere Informationen finden Sie weiter untenIAM-Rolle .
AWS IAM-Zugriffsschlüssel-ID	Geben Sie die AWS IAM-Zugriffsschlüssel-ID ein. Erforderlich, wenn Sie keine IAM-Rolle verwenden.
Geheimer AWS IAM-Zugriffsschlüssel	Geben Sie den geheimen AWS IAM-Zugriffsschlüssel ein. Erforderlich, wenn Sie keine IAM-Rolle verwenden.
Mir ist bekannt, dass AWS mir API-Anfragen in Rechnung stellt.	Aktivieren Sie dies, um zu bestätigen, dass Sie verstanden haben, dass AWS Ihnen die API-Anfragen in Rechnung stellt, die durch Data Infrastructure Insights -Polling gestellt werden.

Erweiterte Konfiguration

Feld	Beschreibung
Zusätzliche Regionen einschließen	Geben Sie zusätzliche Regionen an, die in die Abfrage einbezogen werden sollen.
Cross-Account-Rolle	Rolle für den Zugriff auf Ressourcen in verschiedenen AWS-Konten.
Inventarabfrageintervall (min)	Der Standardwert ist 60
Wählen Sie „Ausschließen“ oder „Einschließen“, um VMs nach Tags zu filtern	Geben Sie an, ob VMs beim Sammeln von Daten anhand von Tags ein- oder ausgeschlossen werden sollen. Wenn „Einschließen“ ausgewählt ist, darf das Feld „Tag-Schlüssel“ nicht leer sein.
Tag-Schlüssel und -Werte zum Filtern von VMs	Klicken Sie auf **+ Tag filtern**, um auszuwählen, welche VMs (und zugehörigen Datenträger) ein-/ausgeschlossen werden sollen, indem Sie nach Schlüsseln und Werten filtern, die mit den Schlüsseln und Werten der Tags auf der VM übereinstimmen. Tag-Schlüssel ist erforderlich, Tag-Wert ist optional. Wenn der Tag-Wert leer ist, wird die VM gefiltert, solange sie mit dem Tag-Schlüssel übereinstimmt.
Leistungsabfrageintervall (Sek.)	Der Standardwert ist 1800
Namespace für CloudWatch-Agent-Metriken	Namespace in EC2/EBS, aus dem Daten gesammelt werden sollen. Beachten Sie, dass Data Infrastructure Insights diese umbenannten Daten möglicherweise nicht erfassen kann, wenn die Namen der Standardmetriken in diesem Namespace geändert werden. Es wird empfohlen, die Standardmetriknamen beizubehalten.

IAM-Zugriffsschlüssel

Zugriffsschlüssel sind langfristige Anmeldeinformationen für einen IAM-Benutzer oder den Stammbenutzer des AWS-Kontos. Zugriffsschlüssel werden verwendet, um programmgesteuerte Anfragen an die AWS CLI oder

AWS API zu signieren (direkt oder mithilfe des AWS SDK).

Zugriffsschlüssel bestehen aus zwei Teilen: einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel. Wenn Sie die Authentifizierung mit *IAM-Zugriffsschlüssel* verwenden (im Gegensatz zur Authentifizierung mit *IAM-Rolle*), müssen Sie zur Authentifizierung von Anfragen sowohl die Zugriffsschlüssel-ID als auch den geheimen Zugriffsschlüssel zusammen verwenden. Weitere Informationen finden Sie in der Amazon-Dokumentation unter"Zugriffsschlüssel" .

IAM-Rolle

Wenn Sie die Authentifizierung mit *IAM-Rolle* verwenden (im Gegensatz zur Authentifizierung mit IAM-Zugriffsschlüssel), müssen Sie sicherstellen, dass die von Ihnen erstellte oder angegebene Rolle über die entsprechenden Berechtigungen für den Zugriff auf Ihre Ressourcen verfügt.

Wenn Sie beispielsweise eine IAM-Rolle mit dem Namen *InstanceEc2ReadOnly* erstellen, müssen Sie die Richtlinie so einrichten, dass EC2 für diese IAM-Rolle die schreibgeschützte Listenzugriffsberechtigung für alle EC2-Ressourcen erhält. Zusätzlich müssen Sie STS (Security Token Service)-Zugriff gewähren, damit diese Rolle kontoübergreifend Rollen übernehmen darf.

Nachdem Sie eine IAM-Rolle erstellt haben, können Sie sie anhängen, wenn Sie eine neue EC2-Instanz oder eine vorhandene EC2-Instanz erstellen.

Nachdem Sie die IAM-Rolle *InstanceEc2ReadOnly* an eine EC2-Instanz angehängt haben, können Sie die temporären Anmeldeinformationen über die Instanzmetadaten anhand des IAM-Rollennamens abrufen und sie verwenden, um mit jeder auf dieser EC2-Instanz ausgeführten Anwendung auf AWS-Ressourcen zuzugreifen.

Weitere Informationen finden Sie in der Amazon-Dokumentation unter"IAM-Rollen" .

Hinweis: Die IAM-Rolle kann nur verwendet werden, wenn die Acquisition Unit in einer AWS-Instanz ausgeführt wird.

Zuordnen von Amazon-Tags zu Data Infrastructure Insights -Anmerkungen

Der Amazon EC2-Datensammler enthält eine Option, mit der Sie Data Infrastructure Insights -Anmerkungen mit auf EC2 konfigurierten Tags füllen können. Die Anmerkungen müssen genau wie die EC2-Tags benannt sein. Data Infrastructure Insights füllt immer gleichnamige Textanmerkungen aus und unternimmt den bestmöglichen Versuch, Anmerkungen anderer Typen (Zahl, Boolescher Wert usw.) auszufüllen. Wenn Ihre Anmerkung einen anderen Typ hat und der Datensammler sie nicht ausfüllen kann, kann es erforderlich sein, die Anmerkung zu entfernen und als Texttyp neu zu erstellen.

Beachten Sie, dass bei AWS die Groß- und Kleinschreibung beachtet wird, während bei Data Infrastructure Insights die Groß- und Kleinschreibung nicht beachtet wird. Wenn Sie also in Data Infrastructure Insights eine Annotation mit dem Namen „OWNER“ und in EC2 Tags mit den Namen „OWNER“, „Owner“ und „owner“ erstellen, werden alle EC2-Varianten von „owner“ der Annotation „OWNER“ von Cloud Insight zugeordnet.

Zusätzliche Regionen einschließen

Im Abschnitt **Erweiterte Konfiguration** des AWS Data Collector können Sie das Feld **Zusätzliche Regionen einschließen** so festlegen, dass zusätzliche Regionen eingeschlossen werden, getrennt durch Komma oder Semikolon. Standardmäßig ist dieses Feld auf ***us-.**** eingestellt, wodurch alle US-amerikanischen AWS-Regionen erfasst werden. Um in *allen* Regionen zu sammeln, setzen Sie dieses Feld auf ***.**. Wenn das Feld **Zusätzliche Regionen einschließen** leer ist, sammelt der Datensammler Daten für die im Feld **AWS-Region** angegebenen Assets, wie im Abschnitt **Konfiguration** angegeben.

Sammeln von AWS-Unterkonten

Data Infrastructure Insights unterstützt die Erfassung untergeordneter Konten für AWS innerhalb eines einzelnen AWS-Datensammlers. Die Konfiguration für diese Sammlung wird in der AWS-Umgebung durchgeführt:

- Sie müssen jedes untergeordnete Konto so konfigurieren, dass es über eine AWS-Rolle verfügt, die der Hauptkonto-ID den Zugriff auf EC2-Details des untergeordneten Kontos ermöglicht.
- Für jedes untergeordnete Konto muss der Rollenname als dieselbe Zeichenfolge konfiguriert sein.
- Geben Sie diese Rollennamenzeichenfolge in den Abschnitt **Erweiterte Konfiguration** des Data Infrastructure Insights AWS Data Collector im Feld **Kontoübergreifende Rolle** ein.
- Das Konto, unter dem der Collector installiert ist, muss über die Berechtigung „Delegierter Zugriffsadministrator“ verfügen. Siehe die"AWS-Dokumentation" für weitere Informationen.

Best Practice: Es wird dringend empfohlen, dem EC2-Hauptkonto die von AWS vordefinierte Richtlinie *AmazonEC2ReadOnlyAccess* zuzuweisen. Außerdem sollte dem in der Datenquelle konfigurierten Benutzer mindestens die vordefinierte Richtlinie *AWSOrganizationsReadOnlyAccess* zugewiesen sein, um AWS abfragen zu können.

Im Folgenden finden Sie Informationen zum Konfigurieren Ihrer Umgebung, damit Data Infrastructure Insights Daten von untergeordneten AWS-Konten erfassen kann:

"Tutorial: Zugriff über AWS-Konten hinweg mithilfe von IAM-Rollen delegieren"

"AWS-Setup: Bereitstellen des Zugriffs für einen IAM-Benutzer in einem anderen AWS-Konto, das Ihnen gehört"

"Erstellen einer Rolle zum Delegieren von Berechtigungen an einen IAM-Benutzer"

Fehlerbehebung

Weitere Informationen zu diesem Datensammler finden Sie im"Support" Seite oder in der"Datensammler-Supportmatrix" .

Amazon FSx for NetApp ONTAP Datenkollektor

Dieser Datensammler erfasst Bestands- und Leistungsdaten von Amazon FSx for NetApp ONTAP. Dieser Datensammler wird schrittweise in allen Serviceregionen von Data Infrastructure Insights verfügbar gemacht. Wenden Sie sich an Ihren Vertriebsmitarbeiter, wenn Sie das Symbol für diesen Collector in Ihrer Data Infrastructure Insights -Umgebung nicht sehen.

Dieser Data Infrastructure Insights Collector erfordert einen ONTAP Benutzer mit einer *Filesystem-Scoped*-Rolle. Bitte überprüfen Sie die AWS"Rollen und Regeln" Informationen zu verfügbaren Optionen finden Sie in der Dokumentation. Derzeit unterstützt AWS nur eine Art von Benutzerrolle mit Dateisystembereich, nämlich *fsxadmin*. Dies ist die geeignete Rolle für den Data Infrastructure Insights -Collector. Dem Benutzer sollten außerdem alle drei dieser Anwendungen zugewiesen sein: http, ontapi, ssh.

Terminologie

Data Infrastructure Insights erfasst Bestands- und Leistungsdaten vom FSx- NetApp Datenkollektor. Für jeden erworbenen Vermögenswerttyp wird die am häufigsten verwendete Terminologie für den Vermögenswert angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Cluster	Storage
LUN	Volumen
Volumen	Internes Volumen

FSx- NetApp -Terminologie

Die folgenden Bedingungen gelten für Objekte oder Referenzen, die Sie möglicherweise auf den Zielseiten der FSx- NetApp Speicherressourcen finden. Viele dieser Begriffe gelten auch für andere Datensammler.

Storage

- Modell – Eine durch Kommas getrennte Liste der eindeutigen, diskreten Modellnamen innerhalb dieses Clusters.
- Anbieter – AWS
- Seriennummer – Die Seriennummer des Arrays.
- IP – im Allgemeinen handelt es sich dabei um die in der Datenquelle konfigurierten IPs oder Hostnamen.
- Rohkapazität – Basis-2-Summe des gesamten dem FSx-Dateisystem zugewiesenen SSD-Speichers.
- Latenz – eine Darstellung der Arbeitslasten, die der Host sowohl beim Lesen als auch beim Schreiben erfährt. Im Idealfall bezieht Data Infrastructure Insights diesen Wert direkt, dies ist jedoch häufig nicht der Fall. Anstelle des Arrays, das dies anbietet, führt Data Infrastructure Insights im Allgemeinen eine IOP-gewichtete Berechnung durch, die aus den Statistiken der einzelnen internen Volumes abgeleitet wird.
- Durchsatz – aggregiert aus internen Volumes. Verwaltung – dies kann einen Hyperlink zur Verwaltungsschnittstelle des Geräts enthalten. Programmgesteuert von der Data Infrastructure Insights Datenquelle als Teil der Bestandsberichterstattung erstellt.

Speicherpool

- Speicher – auf welchem Speicher-Array dieser Pool lebt. Obligatorisch.
- Typ – ein beschreibender Wert aus einer Liste mit aufgezählten Möglichkeiten. Am häufigsten wird „Aggregat“ oder „RAID-Gruppe“ verwendet.
- Kapazität – die Werte hier sind die logisch genutzte, nutzbare Kapazität und die logische Gesamtkapazität sowie der davon genutzte Prozentsatz.
- IOPS – die Summe der IOPs aller diesem Speicherpool zugewiesenen Volumes.
- Durchsatz – der Gesamtdurchsatz aller diesem Speicherpool zugewiesenen Volumes.

Anforderungen

Für die Konfiguration und Verwendung dieses Datensammlers gelten die folgenden Voraussetzungen:

- Sie müssen Zugriff auf ein Konto mit der Rolle „fsxadmin“ haben, dem drei Anwendungen zugewiesen sind

– ssh, ontapi, http

- Zu den Kontodetails gehören Benutzername und Passwort.
- Portanforderungen: 443

Konfiguration

Feld	Beschreibung
NetApp Management IP	IP-Adresse oder vollqualifizierter Domänenname des NetApp -Clusters
Benutzername	Benutzername für NetApp Cluster
Passwort	Passwort für NetApp -Cluster

Erweiterte Metriken

Dieser Datensammler sammelt die folgenden erweiterten Metriken aus dem FSx für NetApp ONTAP -Speicher:

- fpolicy
- nfsv3
- nfsv3:Knoten
- nfsv4
- nfsv4_1
- nfsv4_1:Knoten
- nfsv4:Knoten
- Richtliniengruppe
- qtree
- Volumen
- Arbeitslastvolumen

Beachten Sie, dass FSx CLI- und API-Befehle einige Kapazitätswerte abrufen, die Data Infrastructure Insights ZAPI nicht erfasst. Daher können bestimmte Kapazitätswerte (z. B. für Speicherpools) in Data Infrastructure Insights anders sein als auf dem FSx selbst.

Fehlerbehebung

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Inventar

Problem:	Versuchen Sie Folgendes:
Erhalten Sie die HTTP-Antwort 401 oder den ZAPI-Fehlercode 13003 und ZAPI gibt „Unzureichende Berechtigungen“ oder „Nicht für diesen Befehl autorisiert“ zurück.	Überprüfen Sie Benutzernamen und Passwort sowie Benutzerrechte/Berechtigungen.

Problem:	Versuchen Sie Folgendes:
ZAPI gibt „Clusterrolle ist nicht cluster_mgmt LIF“ zurück.	AU muss mit der Cluster-Management-IP kommunizieren. Überprüfen Sie die IP und wechseln Sie gegebenenfalls zu einer anderen IP
ZAPI-Befehl schlägt nach erneutem Versuch fehl	AU hat ein Kommunikationsproblem mit dem Cluster. Überprüfen Sie Netzwerk, Portnummer und IP-Adresse. Der Benutzer sollte auch versuchen, einen Befehl über die Befehlszeile der AU-Maschine auszuführen.
AU konnte keine Verbindung zu ZAPI über HTTP herstellen	Überprüfen Sie, ob der ZAPI-Port Klartext akzeptiert. Wenn AU versucht, Klartext an einen SSL-Socket zu senden, schlägt die Kommunikation fehl.
Die Kommunikation schlägt mit SSLException fehl	AU versucht, SSL an einen Klartext-Port auf einem Filer zu senden. Überprüfen Sie, ob der ZAPI-Port SSL akzeptiert, oder verwenden Sie einen anderen Port.
Weitere Verbindungsfehler: Die ZAPI-Antwort hat den Fehlercode 13001, „Datenbank ist nicht geöffnet“. Der ZAPI-Fehlercode ist 60 und die Antwort enthält „API wurde nicht rechtzeitig beendet“. Die ZAPI-Antwort enthält „initialize_session() hat eine NULL-Umgebung zurückgegeben“. Der ZAPI-Fehlercode ist 14007 und die Antwort enthält „Knoten ist nicht fehlerfrei“.	Überprüfen Sie Netzwerk, Portnummer und IP-Adresse. Der Benutzer sollte auch versuchen, einen Befehl über die Befehlszeile der AU-Maschine auszuführen.

Weitere Informationen finden Sie in der"Support" Seite oder in der"Datensammler-Supportmatrix" .

Konfigurieren des Azure-Compute-Datensammlers

Data Infrastructure Insights verwendet den Azure Compute-Datensammler, um Bestands- und Leistungsdaten von Azure Compute-Instanzen zu erfassen.

Anforderungen

Zur Konfiguration dieses Datensammlers benötigen Sie folgende Informationen.

- Portanforderung: 443 HTTPS
- Azure OAuth 2.0-Umleitungs-URI (login.microsoftonline.com)
- Azure Management Rest-IP (management.azure.com)
- Azure Resource Manager-IP (management.core.windows.net)
- Azure Service Principal Application (Client) ID (Leserrolle erforderlich)
- Azure-Dienstprinzipal-Authentifizierungsschlüssel (Benutzerkennwort)
- Sie müssen für die Data Infrastructure Insights Erkennung ein Azure-Konto einrichten.

  Sobald das Konto ordnungsgemäß konfiguriert ist und Sie die Anwendung in Azure registrieren, verfügen Sie über die erforderlichen Anmeldeinformationen, um die Azure-Instanz mit Data Infrastructure Insights zu ermitteln. Unter dem folgenden Link wird beschrieben, wie Sie das Konto für die Erkennung einrichten.https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal[]

Konfiguration

Geben Sie die Daten in die Felder des Datensammlers gemäß der folgenden Tabelle ein:

Feld	Beschreibung
Azure Service Principal Application (Client) ID (Leserrolle erforderlich)	Anmelde-ID für Azure. Erfordert Zugriff mit der Rolle „Leser“.
Azure-Mandanten-ID	Microsoft-Mandanten-ID
Azure-Dienstprinzipalauthentifizierungsschlüssel	Login-Authentifizierungsschlüssel
Mir ist bekannt, dass Microsoft mir API-Anfragen in Rechnung stellt.	Aktivieren Sie dies, um zu bestätigen, dass Sie verstanden haben, dass Microsoft Ihnen für API-Anfragen, die durch Insight-Polling gestellt werden, eine Rechnung stellt.

Erweiterte Konfiguration

Feld	Beschreibung
Inventarabfrageintervall (min)	Der Standardwert ist 60
Wählen Sie „Ausschließen“ oder „Einschließen“, um VMs nach Tags zu filtern	Geben Sie an, ob VMs beim Sammeln von Daten anhand von Tags ein- oder ausgeschlossen werden sollen. Wenn „Einschließen“ ausgewählt ist, darf das Feld „Tag-Schlüssel“ nicht leer sein.
Tag-Schlüssel und -Werte zum Filtern von VMs	Klicken Sie auf **+ Tag filtern**, um auszuwählen, welche VMs (und zugehörigen Datenträger) ein-/ausgeschlossen werden sollen, indem Sie nach Schlüsseln und Werten filtern, die mit den Schlüsseln und Werten der Tags auf der VM übereinstimmen. Tag-Schlüssel ist erforderlich, Tag-Wert ist optional. Wenn der Tag-Wert leer ist, wird die VM gefiltert, solange sie mit dem Tag-Schlüssel übereinstimmt.
Leistungsabfrageintervall (Sek.)	Der Standardwert ist 300

Fehlerbehebung

Weitere Informationen zu diesem Datensammler finden Sie im"Support" Seite oder in der"Datensammler-Supportmatrix" .

Broadcom

Brocade Network Advisor-Datensammler

Data Infrastructure Insights verwendet den Brocade Network Advisor-Datensammler, um Bestands- und Leistungsdaten von Brocade -Switches zu erfassen.

Terminologie

Data Infrastructure Insights erhält die folgenden Bestandsinformationen vom Brocade Network Advisor-Datensammler. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten

verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Schalten	Schalten
Hafen	Hafen
Virtuelles Gewebe, physisches Gewebe	Stoff
Logischer Switch	Logischer Switch

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Anforderungen

Zur Konfiguration dieses Datensammlers sind folgende Voraussetzungen erforderlich:

- Die Data Infrastructure Insights Acquisition Unit initiiert Verbindungen zum TCP-Port 443 auf dem BNA-Server. Auf dem BNA-Server muss Version 14.2.1 oder höher ausgeführt werden.
- IP-Adresse des Brocade Network Advisor-Servers
- Benutzername und Kennwort für ein Administratorkonto
- Portanforderung: HTTP/HTTPS 443

Konfiguration

Feld	Beschreibung
Brocade Network Advisor-Server-IP	IP-Adresse des Network Advisor-Servers
Benutzername	Benutzername für den Switch
Benutzername	Administrator-Benutzername
Passwort	Administratorkennwort

Erweiterte Konfiguration

Feld	Beschreibung
Verbindungstyp	HTTPS (Standardport 443) oder HTTP (Standardport 80)
Verbindungsport überschreiben	Wenn das Feld „Verbindungstyp“ leer ist, verwenden Sie den Standardport. Andernfalls geben Sie den zu verwendenden Verbindungsport ein.
Passwort	Passwort für den Switch
Inventarabfrageintervall (min)	Der Standardwert ist 40
Bericht Access Gateway	Aktivieren Sie dieses Kontrollkästchen, um Geräte in den Access Gateway-Modus einzuschließen
Leistungsabfrageintervall (Sek.)	Der Standardwert ist 1800

Fehlerbehebung

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Inventar

Problem:	Versuchen Sie Folgendes:
Sie erhalten eine Meldung, dass mehr als ein Knoten am Access Gateway-Port angemeldet ist oder dass der Datensammler das Access Gateway-Gerät nicht erkennen kann.	Überprüfen Sie, ob das NPV-Gerät ordnungsgemäß funktioniert und ob alle angeschlossenen WWNs den Erwartungen entsprechen. Erwerben Sie das NPV-Gerät nicht direkt. Stattdessen werden die NPV-Gerätedaten durch die Erfassung des Core Fabric Switch erfasst.

Weitere Informationen finden Sie in der"Support" Seite oder in der"Datensammler-Supportmatrix" .

Brocade FC Switch-Datenkollektor

Data Infrastructure Insights verwendet die Datenquelle Brocade FC Switch (SSH), um den Bestand für Brocade oder umbenannte Switch-Geräte zu ermitteln, auf denen die Factored Operating System (FOS)-Firmware 4.2 und höher ausgeführt wird. Es werden Geräte sowohl im FC-Switch- als auch im Access Gateway-Modus unterstützt.

Terminologie

Data Infrastructure Insights erhält die folgenden Bestandsinformationen vom Brocade FC Switch-Datensammler. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Schalten	Schalten
Hafen	Hafen
Virtuelles Gewebe, physisches Gewebe	Stoff
Zone	Zone
Logischer Switch	Logischer Switch
Virtuelles Volume	Volumen
LSAN-Zone	IVR-Zone

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Anforderungen

- Die Data Infrastructure Insights Acquisition Unit (AU) initiiert Verbindungen zum TCP-Port 22 auf Brocade -Switches, um Inventardaten zu erfassen. Die AU initiiert außerdem Verbindungen zum UDP-Port 161, um Leistungsdaten zu erfassen.
- Es muss eine IP-Konnektivität zu allen Switches im Fabric bestehen. Wenn Sie das Kontrollkästchen „Alle

Switches im Fabric erkennen“ aktivieren, identifiziert Data Infrastructure Insights alle Switches im Fabric. Allerdings ist für die Erkennung dieser zusätzlichen Switches eine IP-Verbindung erforderlich.

- Für alle Switches im Fabric ist global dasselbe Konto erforderlich. Sie können PuTTY (Open Source-Terminalemulator) verwenden, um den Zugriff zu bestätigen.
- Die Ports 161 und 162 müssen für alle Switches im Fabric für die SNMP-Leistungsabfrage geöffnet sein.
- SNMP-Nur-Lese-Community-String

Konfiguration

Feld	Beschreibung
IP wechseln	IP-Adresse oder vollqualifizierter Domänenname des EFC-Servers
Benutzername	Benutzername für den Switch
Passwort	Passwort für den Switch
SNMP	SNMP-Version
SNMP-Community-String	SNMP-schreibgeschützte Community-Zeichenfolge für den Zugriff auf den Switch
SNMP-Benutzername	SNMP-Benutzername
SNMP-Passwort	SNMP-Passwort

Erweiterte Konfiguration

Feld	Beschreibung
Stoffname	Vom Datensammler zu meldender Stoffname. Lassen Sie das Feld leer, um den Fabric-Namen als WWN zu melden.
Inventarabfrageintervall (min)	Intervall zwischen den Bestandsabfragen. Der Standardwert ist 15.
Ausgeschlossene Geräte	Durch Kommas getrennte Liste von Geräte-IDs, die von der Abfrage ausgeschlossen werden sollen
Aktive Admin-Domänen	Wählen Sie aus, ob Sie Admin-Domänen verwenden
MPR-Daten abrufen	Wählen Sie diese Option aus, um Routingdaten von Ihrem Multiprotokoll-Router abzurufen.
Überfüllung aktivieren	Wählen Sie diese Option, um die Erfassung beim Empfang eines SNMP-Traps vom Gerät zu aktivieren. Wenn Sie „Trapping aktivieren“ auswählen, müssen Sie auch SNMP aktivieren.
Mindestzeit zwischen Traps (Sek.)	Mindestzeit zwischen durch Traps ausgelösten Erfassungsversuchen. Der Standardwert ist 10.
Entdecken Sie alle Switches im Fabric	Wählen Sie diese Option aus, um alle Switches im Fabric zu erkennen
Wählen Sie HBA gegenüber Zonenaliasen	Wählen Sie, ob HBA- oder Zonenaliase bevorzugt werden sollen

Feld	Beschreibung
Leistungsabfrageintervall (Sek.)	Intervall zwischen Leistungsabfragen. Der Standardwert ist 300.
SNMP-Authentifizierungsprotokoll	SNMP-Authentifizierungsprotokoll (nur SNMP v3)
SNMP-Datenschutzkennwort	SNMP-Datenschutzkennwort (nur SNMP v3)
SNMP-Wiederholungen	Anzahl der SNMP-Wiederholungsversuche

Fehlerbehebung

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Inventar

Problem:	Versuchen Sie Folgendes:
Die Inventarerfassung der Brocade -Datenquelle schlägt mit folgendem Fehler fehl: <Datum> <Uhrzeit> FEHLER [com.onaro.sanscreen.acquisition.framework.datasource.BaseDataSource] Fehler 2 von 2: <Datenquellenname> [Interner Fehler] – Das Modell für Gerät <IP> konnte nicht generiert werden. Fehler beim Erkennen der Eingabeaufforderung ([Gerätename <Name>]: Das Modell für Gerät <IP> konnte nicht generiert werden. Fehler bei der Eingabeaufforderung)	Das Problem kann dadurch verursacht werden, dass der Brocade -Switch zu lange braucht, um mit einer Eingabeaufforderung zurückzukehren, und das Standard-Timeout von 5 Sekunden überschreitet. Versuchen Sie, in den erweiterten Konfigurationseinstellungen des Datensammlers in Data Infrastructure Insights den Wert *SSH-Banner-Wartezeitüberschreitung (Sek.)* auf einen höheren Wert zu erhöhen.
Fehler: „Data Infrastructure Insights hat eine ungültige Chassis-Rolle erhalten“	Überprüfen Sie, ob dem in dieser Datenquelle konfigurierten Benutzer die Berechtigung für die Chassis-Rolle erteilt wurde.
Fehler: „Nicht übereinstimmende Gehäuse-IP-Adresse“	DII unterstützt grundsätzlich KEINE Netzwerkadressübersetzung oder Portadressübersetzung zwischen der Erfassungseinheit und Geräten. DII erkennt möglicherweise, dass der Hostname/die IP-Adresse in der Collector-Konfiguration NICHT mit einer der Adressen übereinstimmt, die das Gerät zu haben glaubt.
Erhalten Sie eine Meldung, dass mehr als ein Knoten am Access Gateway-Port angemeldet ist	Überprüfen Sie, ob das NPV-Gerät ordnungsgemäß funktioniert und ob alle angeschlossenen WWNs den Erwartungen entsprechen. Erwerben Sie das NPV-Gerät nicht direkt. Stattdessen werden die NPV-Gerätedaten durch die Erfassung des Core Fabric Switch erfasst.

Problem:	Versuchen Sie Folgendes:
Fehler: ….Maximale Remote-Sitzungen für die Anmeldung…	FOS hat unterschiedliche Beschränkungen für die Anzahl unterstützter gleichzeitiger SSH-Sitzungen pro Benutzerrolle. Die SSH-Sitzung von DII zu diesem Gerät wird bei der Anmeldung wegen Verletzung dieser Grenzwerte abgelehnt. Dies kann ein Zeichen dafür sein, dass Sie doppelte Sammler haben, die denselben Vermögenswert entdecken, was vermieden werden sollte

Performance

Problem:	Versuchen Sie Folgendes:
Die Leistungserfassung schlägt mit der Meldung „Zeitüberschreitung beim Senden der SNMP-Anforderung“ fehl.	Abhängig von Abfragevariablen und Switch-Konfiguration können einige Abfragen das Standard-Timeout überschreiten. "Weitere Informationen" .
Die Leistungserfassung schlägt fehl mit … Zeilenduplikate in der SNMP-Tabelle gefunden …	DII hat fehlerhafte SNMP-Antworten erkannt. Sie verwenden wahrscheinlich FOS 8.2.3e. Aktualisieren Sie auf 8.2.3e2 oder höher.
Leistungserfassungen schlagen mit …Unbekanntem Benutzernamen… fehl	Sie haben Ihren DII-Collector mit einem „SNMP-Benutzernamen“-Wert konfiguriert, der nicht in einen der SNMPv3-Benutzersteckplätze passt. Durch das einfache Erstellen eines Benutzers auf Brocade FOS wird dieser NICHT unbedingt als SNMPv3-Benutzer aktiviert – Sie müssen ihn in einem der v3-Benutzerslots platzieren.
Leistungserfassungen schlagen mit …Nicht unterstützte Sicherheitsstufe… fehl.	Sie haben Ihren DII-Collector für die Verwendung von SNMPv3 konfiguriert, jedoch mit Verschlüsselungs- (auch Datenschutz-) und/oder Autorisierungseinstellungen, die auf dem betreffenden Gerät nicht aktiviert sind.
Die Leistungserfassung schlägt fehl mit … Leeres Datenschutzkennwort ist nur für das Datenschutzprotokoll NONE zulässig	Sie haben Ihren DII-Collector für die Verwendung von SNMPv3 mit einem Verschlüsselungs- bzw. Datenschutzprotokoll (AES usw.) konfiguriert, aber Sie haben einen leeren Wert für „SNMP-Datenschutzkennwort“, sodass DII keine verschlüsselten SNMPv3-Datenflüsse mit diesem Gerät aushandeln kann.
Die Leistungserfassung schlägt mit …..VF:nn fehl, Fehler: Kein Zugriff…	Sie haben Ihren DII-Collector für die Verwendung von SNMPv3 auf einem Gerät mit mehreren aktivierten virtuellen Fabrics konfiguriert, aber der SNMPv3-Benutzer verfügt NICHT über Rechte für VF NN. DII unterstützt keine teilweise Erkennung eines physischen Assets. Sie sollten DII immer proaktiv Zugriff auf alle 128 möglichen VFs gewähren, da DII immer versucht, Leistungsdaten für alle vorhandenen VFs auf einem bestimmten physischen Gerät abzurufen.

Weitere Informationen finden Sie in der"Support" Seite oder in der"Datensammler-Supportmatrix" .

Brocade FOS REST-Datenkollektor

Data Infrastructure Insights verwendet den Brocade FOS REST-Collector, um Inventar und Leistung für Brocade -Switch-Geräte mit FabricOS (FOS)-Firmware 8.2 und höher zu ermitteln. Bitte beachten Sie, dass frühe 8.2-FOS-Versionen möglicherweise REST-API-Fehler aufweisen. Es wird dringend empfohlen, die neuste FOS-Version auszuführen, die Ihre Plattform unterstützt.

Bitte beachten Sie: Die standardmäßige „Benutzer“-Ebene von FOS ist für Data Infrastructure Insights nicht leistungsfähig genug, um alle logischen Aspekte eines Geräts anzuzeigen. Wir benötigen ein Benutzerkonto mit aktivierter „Chassis-Rolle“ sowie Berechtigungen für alle auf einem Switch konfigurierten virtuellen Fabrics.

Hier ist ein Beispiel, wie Sie ein Benutzerkonto mit den geringsten Berechtigungen für die Verwendung von Data Infrastructure Insights in einer SSH-Sitzung mit einem FOS-Gerät erstellen können:

userConfig --add NetAppCIUser -r Benutzer -l 1-128 -c Benutzer -p Qwerty!

Dadurch wird ein Benutzer „NetAppCIUser“ mit dem Kennwort „Qwerty!“ erstellt. Dieser Benutzer hat die Rolle „Benutzer“ (-r) für alle 128 möglichen virtuellen Fabrics (-l). Dieser Benutzer verfügt zusätzlich über die erforderliche „Chassis“-Rolle (-c) mit zugewiesenem Zugriff auf Benutzerebene.

Standardmäßig versucht dieser Collector, alle FOS-Geräte zu erkennen, die Teil aller Fabrics sind, zu denen der Switch gehört.

Bitte beachten Sie: Der standardmäßige schreibgeschützte Benutzer „Benutzer“ von FOS verfügt NICHT über Anzeigeberechtigungen für alle virtuellen Fabrics und auch nicht über Berechtigungen für die „Chassis-Rolle“. Dies bedeutet, dass die Erfolgsaussichten bei der Verwendung von „Benutzer“ mit Data Infrastructure Insights gering sind, da hierfür sowohl die physische als auch die logische Konfiguration des FOS-Geräts bekannt sein muss.

Terminologie

Data Infrastructure Insights erhält die folgenden Bestandsinformationen vom Brocade FOS REST-Datensammler. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Schalten	Schalten
Hafen	Hafen
Virtuelles Gewebe, physisches Gewebe	Stoff
Zone	Zone
Logischer Switch	Logischer Switch
LSAN-Zone	IVR-Zone

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Anforderungen

- Es muss eine TCP-Konnektivität zu allen Switches im Fabric bestehen. Dieser Datensammlertyp probiert nahtlos sowohl HTTP als auch HTTPS für jedes Gerät im Fabric aus. Wenn Sie das Kontrollkästchen „Alle Switches im Fabric erkennen“ aktivieren, identifiziert Data Infrastructure Insights alle Switches im Fabric. Allerdings ist für die Erkennung dieser zusätzlichen Switches eine TCP-Verbindung erforderlich.
- Für alle Switches im Fabric ist global dasselbe Konto erforderlich. Sie können den Zugriff über die Weboberfläche des Geräts bestätigen.

Konfiguration

Feld	Beschreibung
IP wechseln	IP-Adresse oder vollqualifizierter Domänenname des FOS-Switches
Benutzername	Benutzername für den Switch
Passwort	Passwort für den Switch

Erweiterte Konfiguration

Feld	Beschreibung
Ausgeschlossene Geräte	Durch Kommas getrennte Liste von Geräte-IPv4-Adressen, die von der Abfrage ausgeschlossen werden sollen.
Inventarabfrageintervall (min)	Intervall zwischen den Bestandsabfragen. Der Standardwert ist 60.
Entdecken Sie alle Switches im Fabric	Wählen Sie diese Option aus, um alle Switches im Fabric zu erkennen.
Wählen Sie HBA gegenüber Zonenaliasen	Wählen Sie, ob HBA- oder Zonenaliase bevorzugt werden sollen.
Anschlussart	HTTP oder HTTPS.
Beachten Sie, dass diese Einstellung nur ändert, welches Protokoll CI zuerst pro Gerät zu verwenden versucht. CI versucht automatisch das entgegengesetzte Protokoll, wenn die Standardeinstellung fehlschlägt.	TCP-Port überschreiben
Geben Sie einen Port an, wenn Sie nicht den Standardport verwenden.	Leistungsabfrageintervall (Sek.)

Fehlerbehebung

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Inventar

Problem:	Versuchen Sie Folgendes:
Die Testfunktion warnt mich, dass auf ein Protokoll nicht zugegriffen werden kann	Ein bestimmtes Brocade FOS 8.2+-Gerät möchte nur über HTTP oder HTTPS kommunizieren. Wenn auf einem Switch ein digitales Zertifikat installiert ist, gibt der Switch HTTP-Fehler aus, wenn versucht wird, mit ihm über unverschlüsseltes HTTP statt HTTPS zu kommunizieren. Die Testfunktion versucht, sowohl mit HTTP als auch mit HTTPS zu kommunizieren. Wenn der Test ergibt, dass ein Protokoll erfolgreich ist, können Sie den Collector sicher speichern und müssen sich keine Sorgen machen, dass das andere Protokoll nicht erfolgreich war. Der Collector versucht während der Erfassung beide Protokolle und schlägt nur fehl, wenn keines von beiden funktioniert.
Fehler: Inventarisierung schlägt mit 401 Unauthorized fehl…Ungültiger Sitzungsschlüssel…	Dies ist ein eindeutiger Fehler in einigen sehr frühen 8.2 FOS-Versionen wie 8.2.1c, die die HTTP-Basisauthentifizierung NICHT richtig unterstützen. Upgrade auf eine spätere Version 8.2 oder 9.*
Fehler: „Data Infrastructure Insights hat eine ungültige Chassis-Rolle erhalten“	Überprüfen Sie, ob dem in dieser Datenquelle konfigurierten Benutzer die Berechtigung für die Chassis-Rolle erteilt wurde.
Fehler: „Nicht übereinstimmende Gehäuse-IP-Adresse“	Ändern Sie die Datenquellenkonfiguration, um die IP-Adresse des Gehäuses zu verwenden.
Die Inventur schlägt mit der Fehlermeldung „403 Forbidden“ fehl	Dies können einfach ungültige Anmeldeinformationen sein oder ein Hinweis darauf, dass Sie versuchen, eine Rolle mit unzureichenden Befugnissen zu verwenden. Bedenken Sie, dass Benutzer auf der Ebene „Benutzer“ NICHT über die erforderlichen Rechte für die „Chassis-Rolle“ verfügen oder keinen Anzeigezugriff auf nicht standardmäßige virtuelle Fabrics haben.

Weitere Informationen finden Sie in der"Support" Seite oder in der"Datensammler-Supportmatrix" .

Cisco MDS Fabric Switches Datensammler

Data Infrastructure Insights verwendet den Datensammler von Cisco MDS Fabric Switches, um den Bestand für Cisco MDS Fabric Switches sowie eine Vielzahl von Cisco Nexus FCoE-Switches zu ermitteln, auf denen der FC-Dienst aktiviert ist.

Darüber hinaus können Sie mit diesem Datensammler viele Modelle von Cisco -Geräten entdecken, die im NPV-Modus laufen.

Terminologie

Data Infrastructure Insights erhält die folgenden Bestandsinformationen vom Cisco FC Switch-Datensammler. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Schalten	Schalten
Hafen	Hafen
VSAN	Stoff
Zone	Zone
Logischer Switch	Logischer Switch
Nameserver-Eintrag	Nameserver-Eintrag
Inter-VSAN-Routing (IVR)-Zone	IVR-Zone

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Anforderungen

- Eine IP-Adresse eines Switches im Fabric oder einzelner Switches
- Chassis-Erkennung, um die Fabric-Erkennung zu ermöglichen
- Bei Verwendung von SNMP V2: schreibgeschützter Community-String
- Port 161 wird für den Zugriff auf das Gerät verwendet

Konfiguration

Feld	Beschreibung
Cisco Switch-IP	IP-Adresse oder vollqualifizierter Domänenname des Switches
SNMP -Version	Wählen Sie V1, V2 oder V3. Für die Leistungserfassung ist V2 oder höher erforderlich.
SNMP-Community-String	SNMP-Nur-Lese-Community-String für den Zugriff auf den Switch (gilt nicht für SNMP v3)
Benutzername	Benutzername für den Switch (nur SNMP v3)
Passwort	Für den Switch verwendetes Passwort (nur SNMPv3)

Erweiterte Konfiguration

Feld	Beschreibung
Inventarabfrageintervall (min)	Intervall zwischen den Bestandsabfragen (Standard 40 Minuten)
SNMP-Authentifizierungsprotokoll	SNMP-Authentifizierungsprotokoll (nur SNMPv3)
SNMP-Datenschutzprotokoll	SNMP-Datenschutzprotokoll (nur SNMPv3)
SNMP-Datenschutzkennwort	SNMP-Datenschutzkennwort
SNMP-Wiederholungen	Anzahl der SNMP-Wiederholungsversuche
SNMP-Zeitüberschreitung (ms)	SNMP-Timeout (Standard 5000 ms)

Feld	Beschreibung
Überfüllung aktivieren	Wählen Sie diese Option, um das Trapping zu aktivieren. Wenn Sie Trapping aktivieren, müssen Sie auch SNMP-Benachrichtigungen aktivieren.
Mindestzeit zwischen Traps (Sek.)	Mindestzeit zwischen durch Traps ausgelösten Erfassungsversuchen (Standard 10 Sekunden)
Entdecken Sie alle Fabric Switches	Wählen Sie diese Option aus, um alle Switches im Fabric zu erkennen
Ausgeschlossene Geräte	Durch Kommas getrennte Liste von Geräte-IPs, die von der Abfrage ausgeschlossen werden sollen
Enthaltene Geräte	Durch Kommas getrennte Liste der Geräte-IPs, die in die Abfrage einbezogen werden sollen
Gerätetyp prüfen	Wählen Sie diese Option aus, um nur die Geräte zu akzeptieren, die sich ausdrücklich als Cisco -Geräte ausgeben
Erster Aliastyp	Geben Sie eine erste Präferenz für die Auflösung des Alias an. Wählen Sie aus Folgendem: **Device Alais** Dies ist ein benutzerfreundlicher Name für einen Port-WWN (pWWN), der bei Bedarf in allen Konfigurationsbefehlen verwendet werden kann. Alle Switches der Cisco MDS 9000-Familie unterstützen Distributed Device Alias Services (Gerätealiase). **Keine** Kein Alias melden. **Portbeschreibung** Eine Beschreibung zur Identifizierung des Ports in einer Portliste. **Zonenalias (alle)** Ein benutzerfreundlicher Name für einen Port, der nur für die aktive Konfiguration verwendet werden kann. Dies ist die Standardeinstellung.
Zweiter Aliastyp	Geben Sie eine zweite Präferenz für die Auflösung des Alias an
Dritter Aliastyp	Geben Sie eine dritte Präferenz für die Auflösung des Alias an
Aktivieren Sie die SANTap-Proxy-Modus-Unterstützung	Wählen Sie aus, ob Ihr Cisco Switch SANTap im Proxy-Modus verwendet. Wenn Sie EMC RecoverPoint verwenden, verwenden Sie wahrscheinlich SANTap.
Leistungsabfrageintervall (Sek.)	Intervall zwischen Leistungsabfragen (Standard 300 Sekunden)

Fehlerbehebung

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Inventar

Problem:	Versuchen Sie Folgendes:
Fehler: Chassis konnte nicht erkannt werden – es wurden keine Switches erkannt	• Pingen Sie das Gerät mit der konfigurierten IP an. • Melden Sie sich über die GUI des Cisco Device Managers beim Gerät an. • Melden Sie sich über die CLI beim Gerät an. • Versuchen Sie, SNMP Walk auszuführen.
Fehler: Gerät ist kein Cisco MDS-Switch	• Stellen Sie sicher, dass die für das Gerät konfigurierte Datenquellen-IP richtig ist. • Melden Sie sich über die Cisco Device Manager-GUI beim Gerät an. • Melden Sie sich über die CLI beim Gerät an.
Fehler: Data Infrastructure Insights kann den WWN des Switches nicht abrufen.	Dies ist möglicherweise kein FC- oder FCoE-Switch und wird daher möglicherweise nicht unterstützt. Stellen Sie sicher, dass es sich bei der in der Datenquelle konfigurierten IP/FQDN tatsächlich um einen FC/FCoE-Switch handelt.
Fehler: Es wurden mehrere Knoten gefunden, die am NPV-Switch-Port angemeldet sind.	Deaktivieren Sie die direkte Erfassung des NPV-Schalters
Fehler: Es konnte keine Verbindung zum Switch hergestellt werden	• Stellen Sie sicher, dass das Gerät aktiv ist. • Überprüfen Sie die IP-Adresse und den Abhörport. • Pingen Sie das Gerät an. • Melden Sie sich über die Cisco Device Manager-GUI beim Gerät an. • Melden Sie sich über die CLI beim Gerät an. • Führen Sie einen SNMP-Walk aus.

Performance

Problem:	Versuchen Sie Folgendes:
Fehler: Leistungserfassung wird von SNMP v1 nicht unterstützt	• Datenquelle bearbeiten und Switch-Leistung deaktivieren • Datenquelle und Switch-Konfiguration ändern, um SNMP v2 oder höher zu verwenden

Weitere Informationen finden Sie in der"Support" Seite oder in der"Datensammler-Supportmatrix" .

Cohesity SmartFiles-Datensammler

Dieser auf REST-API basierende Collector erwirbt einen Cohesity-Cluster, erkennt die „Ansichten“ (als interne Volumes von Data Infrastructure Insights) und die verschiedenen Knoten und sammelt Leistungsmetriken.

Konfiguration

Feld	Beschreibung
Cohesity-Cluster-IP	IP-Adresse des Cohesity-Clusters
Benutzername	Benutzername für den Cohesity-Cluster
Passwort	Für den Cohesity-Cluster verwendetes Passwort

Erweiterte Konfiguration

Feld	Beschreibung
TCP-Port	Für die TCP-Kommunikation mit dem Cohesity-Cluster verwendeter Port
Inventarabfrageintervall (min)	Intervall zwischen den Bestandsabfragen. Der Standardwert beträgt 60 Minuten.
Leistungsabfrageintervall (min)	Intervall zwischen Leistungsabfragen. Der Standardwert beträgt 900 Sekunden.

Fehlerbehebung

Weitere Informationen finden Sie in der"Support" Seite oder in der"Datensammler-Supportmatrix" .

Dell

Datensammler der Dell EMC XC-Serie

Data Infrastructure Insights verwendet diesen Datensammler, um Bestands- und Leistungsinformationen für die Speicher-Arrays der Dell EMC XC-Serie zu ermitteln.

Konfiguration

Feld	Beschreibung
Externe Prism-IP-Adresse	IP-Adresse des XC-Servers
Benutzername	Benutzername für den XC-Server
Passwort	Für den XC-Server verwendetes Passwort

Erweiterte Konfiguration

Feld	Beschreibung
TCP-Port	Für die TCP-Kommunikation mit dem XC-Server verwendeter Port
Inventarabfrageintervall (min)	Intervall zwischen den Bestandsabfragen. Der Standardwert beträgt 60 Minuten.
Leistungsabfrageintervall (min)	Intervall zwischen Leistungsabfragen. Der Standardwert beträgt 300 Sekunden.

Fehlerbehebung

Weitere Informationen finden Sie in der"Support" Seite oder in der"Datensammler-Supportmatrix" .

Dell EMC

DELL EMC Data Domain-Datenkollektor

Dieser Datensammler sammelt Bestands- und Leistungsinformationen von DELL EMC Data Domain-Deduplizierungsspeichersystemen. Zum Konfigurieren dieses Datensammlers müssen Sie bestimmte Konfigurationsanweisungen und Verwendungsempfehlungen befolgen.

Terminologie

Data Infrastructure Insights erhält die folgenden Bestandsinformationen vom Data Domain-Datenkollektor. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Scheibe	Scheibe
Anordnung	Storage
FC-Anschluss	Hafen
Dateisystem	Internes Volumen
Quote	Quote
NFS- und CIFS-Freigabe	Dateifreigabe

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Anforderungen

Zur Konfiguration dieses Datensammlers benötigen Sie folgende Informationen:

- IP-Adresse des Data Domain-Geräts
- Nur-Lese-Benutzername und Kennwort für den Data Domain-Speicher
- SSH-Port 22

Konfiguration

Feld	Beschreibung
IP-Adresse	Die IP-Adresse oder der vollqualifizierte Domänenname des Data Domain-Speicherarrays
Benutzername	Der Benutzername für das Data Domain-Speicherarray
Passwort	Das Kennwort für das Data Domain-Speicherarray

Erweiterte Konfiguration

Feld	Beschreibung
Inventarabfrageintervall (min)	Intervall zwischen den Bestandsabfragen. Der Standardwert ist 20.
SSH-Port	SSH-Dienstport

Fehlerbehebung

Weitere Informationen zu diesem Datensammler finden Sie im"Support" Seite oder in der"Datensammler-Supportmatrix" .

Konfigurieren des EMC ECS-Datenkollektors

Dieser Datensammler erfasst Bestands- und Leistungsdaten von EMC ECS-Speichersystemen. Zur Konfiguration benötigt der Datensammler eine IP-Adresse oder den Hostnamen des ECS-Clusters sowie einen Benutzernamen und ein Passwort.

Dell EMC ECS wird zu einem anderen Preis als Raw TB und Managed Unit berechnet. Jede 40 TB unformatierte ECS-Kapazität wird als 1 berechnet"Verwaltete Einheit (MU)" .

Terminologie

Data Infrastructure Insights erhält die folgenden Bestandsinformationen vom ECS-Datensammler. Für jeden erworbenen Vermögenswerttyp wird die am häufigsten verwendete Terminologie für diesen Vermögenswert angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Cluster	Storage
Mieter	Speicherpool
Eimer	Internes Volumen
Scheibe	Scheibe

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Anforderungen

- Eine IP-Adresse oder ein Hostname des ECS-Clusters
- Ein Benutzername und ein Passwort für das ECS-System
- Port 4443 (HTTPS). Erfordert ausgehende Konnektivität zum TCP-Port 4443 auf dem ECS-System.

Konfiguration

Feld	Beschreibung
ECS-Host	IP-Adresse oder vollqualifizierter Domänenname des ECS-Systems

Feld	Beschreibung
ECS-Host-Port	Für die Kommunikation mit dem ECS-Host verwendeter Port
ECS-Benutzer-ID	Benutzer-ID für ECS
Passwort	Für ECS verwendetes Passwort

Erweiterte Konfiguration

Feld	Beschreibung
Inventarabfrageintervall (min)	Der Standardwert beträgt 360 Minuten.

Fehlerbehebung

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Inventar

Problem:	Versuchen Sie Folgendes:
Fehler: Benutzerauthentifizierung fehlgeschlagen.	Stellen Sie sicher, dass Ihre Anmeldeinformationen für dieses Gerät korrekt sind.

Performance

Problem:	Versuchen Sie Folgendes:
Fehler: Nicht genügend Daten gesammelt.	* Überprüfen Sie den Erfassungszeitstempel in der Protokolldatei und ändern Sie das Abfrageintervall entsprechend. * Warten Sie länger
Fehler: Das Leistungsabfrageintervall ist zu groß.	Überprüfen Sie den Erfassungszeitstempel in der Protokolldatei ${logfile} und ändern Sie das Abfrageintervall entsprechend

Weitere Informationen finden Sie in der"Support" Seite oder in der"Datensammler-Supportmatrix" .

Dell EMC PowerScale-Datenkollektor

Data Infrastructure Insights verwendet den SSH-Datensammler Dell EMC PowerScale (früher Isilon), um Bestands- und Leistungsdaten vom PowerScale-Scale-Out-NAS-Speicher zu erfassen.

Terminologie

Data Infrastructure Insights erhält von diesem Datensammler die folgenden Bestandsinformationen. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Fahren	Scheibe
Cluster	Storage
Node	Speicherknoten
Dateisystem	Internes Volumen

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Anforderungen

Zur Konfiguration dieses Datensammlers benötigen Sie folgende Informationen:

- Administratorberechtigungen für den PowerScale-Speicher
- IP-Adresse des PowerScale-Clusters
- SSH-Zugriff auf Port 22

Konfiguration

Feld	Beschreibung
IP-Adresse	Die IP-Adresse oder der vollqualifizierte Domänenname des PowerScale-Clusters
Benutzername	Benutzername für den PowerScale-Cluster
Passwort	Für den PowerScale-Cluster verwendetes Kennwort

Erweiterte Konfiguration

Feld	Beschreibung
Inventarabfrageintervall (min)	Intervall zwischen den Bestandsabfragen. Der Standardwert ist 20.
Leistungsabfrageintervall (Sek.)	Intervall zwischen Leistungsabfragen. Der Standardwert ist 300.
SSH-Port	SSH-Dienstport. Der Standardwert ist 22.

Fehlerbehebung

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Inventar

Problem:	Versuchen Sie Folgendes:
„Ungültige Anmeldeinformationen“ mit der Fehlermeldung „Für die rollenbasierte Verwaltung nicht aktivierte Befehle erfordern Root-Benutzerzugriff“	* Überprüfen Sie, ob der Benutzer über die Berechtigung verfügt, die folgenden Befehle auf dem Gerät auszuführen: > isi version osrelease > isi status -q > isi status -n > isi devices -d %s > isi license * Überprüfen Sie, ob die im Assistenten verwendeten Anmeldeinformationen mit den Anmeldeinformationen des Geräts übereinstimmen
„Interner Fehler“ mit Fehlermeldungen „Ausführung des Befehls <Ihr Befehl> fehlgeschlagen mit Berechtigung: <Ihre aktuelle Berechtigung>.“ Problem mit der Berechtigung zum Ausführen des Sudo-Befehls“	Stellen Sie sicher, dass der Benutzer über Sudo-Berechtigungen verfügt, um den folgenden Befehl auf dem Gerät auszuführen.

Weitere Informationen finden Sie in der"Support" Seite oder in der"Datensammler-Supportmatrix" .

Dell EMC Isilon/PowerScale REST-Datensammler

Data Infrastructure Insights verwendet den Dell EMC Isilon/PowerScale REST-Datensammler, um Bestands- und Leistungsdaten vom Dell EMC Isilon- oder PowerScale-Speicher zu erfassen. Dieser Collector unterstützt Arrays mit OneFS 8.0.0+.

Terminologie

Data Infrastructure Insights erhält von diesem Datensammler die folgenden Bestandsinformationen. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Fahren	Scheibe
Cluster	Storage
Node	Speicherknoten
OneFS-Dateisystem	Internes Volumen
OneFS-Dateisystem	Speicherpool
Qtree	Qtree

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Anforderungen

Zur Konfiguration dieses Datensammlers benötigen Sie folgende Informationen:

- Ein Benutzerkonto und ein Passwort. Dieses Konto muss NICHT admin/root sein, aber Sie MÜSSEN Ihrem Dienstkonto eine beträchtliche Anzahl von Leseberechtigungen erteilen – siehe Tabelle unten
- IP-Adresse / vollqualifizierter Domänenname des Dell EMC Isilon / PowerScale-Clusters

- HTTPS-Zugriff auf Port 8080
- Isilon-/PowerScale-Cluster mit OneFS 8.0.0 oder höher

Berechtigungsname	Beschreibung	r (Lesen) oder rw (Lesen+Schreiben)
ISI_PRIV_LOGIN_PAPI	Plattform-API	R
ISI_PRIV_SYS_TIME	Zeit	R
ISI_PRIV_AUTH	Authentifizierung	R
ISI_PRIV_ROLE	Privileg	R
ISI_PRIV_DEVICES	Geräte	R
ISI_PRIV_EVENT	Ereignis	R
ISI_PRIV_HDFS	HDFS	R
ISI_PRIV_NDMP	NDMP	R
ISI_PRIV_NETWORK	Netzwerk	R
ISI_PRIV_NFS	NFS	R
ISI_PRIV_PAPI_CONFIG	Konfigurieren der Plattform-API	R
ISI_PRIV_QUOTA	Quote	R
ISI_PRIV_SMARTPOOLS	SmartPools	R
ISI_PRIV_SMB	KMU	R
ISI_PRIV_STATISTICS	Statistiken	R
ISI_PRIV_SWIFT	Schnell	R
ISI_PRIV_JOB_ENGINE	Job-Engine	R

Konfiguration

Feld	Beschreibung
Isilon-IP-Adresse	Die IP-Adresse oder der vollqualifizierte Domänenname des Isilon-Speichers
Benutzername	Benutzername für Isilon
Passwort	Für Isilon verwendetes Kennwort

Erweiterte Konfiguration

Feld	Beschreibung
HTTPS-Port	Der Standardwert ist 8080.
Inventarabfrageintervall (min)	Intervall zwischen den Bestandsabfragen. Der Standardwert ist 20.
Leistungsabfrageintervall (Sek.)	Intervall zwischen Leistungsabfragen. Der Standardwert ist 300.

Fehlerbehebung

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Inventar

Problem:	Versuchen Sie Folgendes:
„Ungültige Anmeldeinformationen“ mit der Fehlermeldung „Für die rollenbasierte Verwaltung nicht aktivierte Befehle erfordern Root-Benutzerzugriff“	* Überprüfen Sie, ob der Benutzer über die Berechtigung verfügt, die folgenden Befehle auf dem Gerät auszuführen: > isi version osrelease > isi status -q > isi status -n > isi devices -d %s > isi license * Überprüfen Sie, ob die im Assistenten verwendeten Anmeldeinformationen mit den Anmeldeinformationen des Geräts übereinstimmen
„Interner Fehler“ mit Fehlermeldungen „Ausführung des Befehls <Ihr Befehl> fehlgeschlagen mit Berechtigung: <Ihre aktuelle Berechtigung>.“ Problem mit der Berechtigung zum Ausführen des Sudo-Befehls“	Stellen Sie sicher, dass der Benutzer über Sudo-Berechtigungen verfügt, um den folgenden Befehl auf dem Gerät auszuführen.

Weitere Informationen finden Sie in der"Support" Seite oder in der"Datensammler-Supportmatrix" .

Dell EMC PowerStore-Datenkollektor

Der EMC PowerStore-Datenkollektor sammelt Bestandsinformationen vom EMC PowerStore-Speicher. Zur Konfiguration benötigt der Datensammler die IP-Adresse der Speicherprozessoren sowie einen schreibgeschützten Benutzernamen und ein Passwort.

Der EMC PowerStore-Datenkollektor erfasst die Volume-zu-Volume-Replikationsbeziehungen, die PowerStore über andere Speicher-Arrays hinweg koordiniert. Data Infrastructure Insights zeigt ein Speicherarray für jeden PowerStore-Cluster und sammelt Bestandsdaten für Knoten und Speicherports auf diesem Cluster. Es werden keine Speicherpool- oder Volumedaten erfasst.

Terminologie

Data Infrastructure Insights erhält von diesem Datensammler die folgenden Bestandsinformationen. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Gastgeber	Gastgeber
Host-Volume-Zuordnung	Host-Volume-Zuordnung
Hardware (es hat Laufwerke unter dem Objekt "extra_details"): Laufwerke	Scheibe
Gerät	Speicherpool
Cluster	Speicher-Array
Node	Speicherknoten

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
fc_port	Hafen
Volumen	Volumen
Internes Volumen	Dateisystem

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Anforderungen

Zur Konfiguration dieses Datensammlers sind folgende Angaben erforderlich:

- IP-Adresse oder vollqualifizierter Domänenname des Speicherprozessors
- Benutzername und Kennwort nur zum Lesen

Konfiguration

Feld	Beschreibung
PowerStore-Gateway(s)	IP-Adressen oder vollqualifizierte Domänennamen des PowerStore-Speichers
Benutzername	Benutzername für PowerStore
Passwort	Für PowerStore verwendetes Kennwort

Erweiterte Konfiguration

Feld	Beschreibung
HTTPS-Port	Der Standardwert ist 443
Inventarabfrageintervall (Minuten)	Intervall zwischen den Bestandsabfragen. Der Standardwert beträgt 60 Minuten.

Die PowerStore-Leistungssammlung von Cloud Insight nutzt die Quelldaten von PowerStore mit einer Granularität von 5 Minuten. Daher fragt Data Infrastructure Insights diese Daten alle fünf Minuten ab, und dies ist nicht konfigurierbar.

Fehlerbehebung

Weitere Informationen zu diesem Datensammler finden Sie im"Support" Seite oder in der"Datensammler-Supportmatrix" .

Dell EMC RecoverPoint-Datensammler

Der Hauptanwendungsfall des EMC RecoverPoint-Datensammlers besteht darin, Volume-zu-Volume-Replikationsbeziehungen zu ermitteln, die das RecoverPoint-Speichergerät ermöglicht. Dieser Collector erkennt auch das Recoverpoint-Gerät selbst. Bitte beachten Sie, dass Dell/EMC eine VMware-Backup-Lösung für VMs verkauft – „RecoverPoint für VMs“ – die von diesem Collector nicht unterstützt wird.

Zur Konfiguration benötigt der Datensammler die IP-Adresse der Speicherprozessoren sowie einen schreibgeschützten Benutzernamen und ein Passwort.

Der EMC RecoverPoint-Datenkollektor erfasst die Volume-zu-Volume-Replikationsbeziehungen, die RecoverPoint über andere Speicher-Arrays hinweg koordiniert. Data Infrastructure Insights zeigt ein Speicherarray für jeden RecoverPoint-Cluster und sammelt Inventardaten für Knoten und Speicherports auf diesem Cluster. Es werden keine Speicherpool- oder Volumedaten erfasst.

Anforderungen

Zur Konfiguration dieses Datensammlers sind folgende Angaben erforderlich:

- IP-Adresse oder vollqualifizierter Domänenname des Speicherprozessors
- Benutzername und Kennwort nur zum Lesen
- REST-API-Zugriff über Port 443

Konfiguration

Feld	Beschreibung
Adresse von RecoverPoint	IP-Adresse oder vollqualifizierter Domänenname des RecoverPoint-Clusters
Benutzername	Benutzername für den RecoverPoint-Cluster
Passwort	Für den RecoverPoint-Cluster verwendetes Kennwort

Erweiterte Konfiguration

Feld	Beschreibung
TCP-Port	Für die Verbindung mit dem Recoverpoint-Cluster verwendeter TCP-Port
Inventarabfrageintervall (Minuten)	Intervall zwischen den Bestandsabfragen. Der Standardwert beträgt 20 Minuten.
Ausgeschlossene Cluster	Durch Kommas getrennte Liste von Cluster-IDs oder -Namen, die beim Polling ausgeschlossen werden sollen.

Fehlerbehebung

Weitere Informationen zu diesem Datensammler finden Sie im"Support" Seite oder in der"Datensammler-Supportmatrix" .

DELL EMC ScaleIO / PowerFlex-Datensammler

Der ScaleIO/PowerFlex-Datensammler sammelt Bestandsinformationen vom ScaleIO- und PowerFlex-Speicher. Zur Konfiguration benötigt dieser Datensammler die ScaleIO/PowerFlex-Gateway-Adresse sowie einen Administrator-Benutzernamen und ein Administrator-Passwort.

Terminologie

Data Infrastructure Insights erhält die folgenden Bestandsinformationen vom ScaleIO/PowerFlex-Datensammler. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
MDM-Cluster (Metadaten-Manager)	Storage
SDS (ScaleIO/PowerFlex-Datenserver)	Speicherknoten
Speicherpool	Speicherpool
Volumen	Volumen
Gerät	Scheibe

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Anforderungen

- Nur-Lese-Zugriff auf das Admin-Benutzerkonto
- Portanforderung: HTTPS-Port 443

Konfiguration

Feld	Beschreibung
ScaleIO/PowerFlex-Gateway(s)	IP-Adressen oder FQDNs von ScaleIO/PowerFlex-Gateways, getrennt durch Komma (,) oder Semikolon (;)
Benutzername	Administrator-Benutzername für die Anmeldung beim ScaleIO/PowerFlex-Gerät
Passwort	Kennwort zur Anmeldung beim ScaleIO/PowerFlex-Gerät

Erweiterte Konfiguration

Klicken Sie auf das Kontrollkästchen Inventar, um die Inventarerfassung zu aktivieren.

Feld	Beschreibung
HTTPS-Port	443
Inventarabfrageintervall (min)	Der Standardwert ist 60.
Verbindungs-Timeout (Sek.)	Der Standardwert ist 60.

Fehlerbehebung

Weitere Informationen finden Sie in der"Support" Seite oder in der"Datensammler-Supportmatrix" .

Konfigurieren des EMC Unity-Datenkollektors

Der Datensammler DELL EMC Unity (ehemals VNXe) bietet Inventarunterstützung für VNXe Unified Storage Arrays. Data Infrastructure Insights unterstützt derzeit iSCSI- und NAS-Protokolle.

Anforderungen

- Der Unity-Datensammler ist CLI-basiert. Sie müssen die Unisphere für Unity-CLI (uemcli.exe) auf der Erfassungseinheit installieren, auf der sich Ihr VNXe-Datensammler befindet.
- uemcli.exe verwendet HTTPS als Transportprotokoll, daher muss die Erfassungseinheit in der Lage sein, HTTPS-Verbindungen zur Unity herzustellen.
- IP-Adresse oder vollqualifizierter Domänenname des Unity-Geräts
- Für die Verwendung durch den Datensammler müssen Sie mindestens über einen schreibgeschützten Benutzer verfügen.
- HTTPS auf Port 443 ist erforderlich
- Der EMC Unity-Datenkollektor bietet NAS- und iSCSI-Unterstützung für die Bestandsaufnahme. Fibre-Channel-Volumes werden erkannt, Data Infrastructure Insights meldet jedoch keine FC-Zuordnung, Maskierung oder Speicherports.

Terminologie

Data Infrastructure Insights erhält die folgenden Bestandsinformationen vom Unity-Datensammler. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Scheibe	Scheibe
Speicher-Array	Storage
Prozessor	Speicherknoten
Speicherpool	Speicherpool
Allgemeine iSCSI-Blockinformationen, VMware VMFS	Aktie
Replikations-Remotesystem	Synchronisation
iSCSI-Knoten	iSCSI-Zielknoten
iSCSI-Initiator	iSCSI-Zielinitiator

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diese Datenquelle darstellen.

Konfiguration

Feld	Beschreibung
Unity-Speicher	IP-Adresse oder vollqualifizierter Domänenname des Unity-Geräts

Feld	Beschreibung
Benutzername	Benutzername für das Unity-Gerät
Passwort	Passwort für das Unity-Gerät
Vollständiger Pfad zur ausführbaren UEMCLI	Vollständiger Pfad zum Ordner, der die ausführbare Datei *uemcli.exe* enthält

Erweiterte Konfiguration

Feld	Beschreibung
Inventarabfrageintervall (min)	Intervall zwischen den Bestandsabfragen. Der Standardwert beträgt 40 Minuten
Unity CLI-Port	Für die Unity CLI verwendeter Port
Leistungsabfrageintervall (Sek.)	Der Standardwert ist 300.

Fehlerbehebung

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Inventar

Problem:	Versuchen Sie Folgendes:
„Fehler beim Ausführen des externen Dienstprogramms“ mit der Fehlermeldung „Ausführbare Unisphere-Uemcli konnte nicht gefunden werden“	* Überprüfen Sie, ob die IP-Adresse, der Benutzername und das Kennwort korrekt sind. * Bestätigen Sie, dass Unisphere CLI auf der Data Infrastructure Insights Acquisition Unit installiert ist. * Bestätigen Sie, dass das Installationsverzeichnis von Unisphere CLI in der Datenquellenkonfiguration korrekt ist. * Bestätigen Sie, dass die IP des VNXe in der Konfiguration der Datenquelle korrekt ist. Öffnen Sie in der Data Infrastructure Insights Acquisition Unit eine CMD und wechseln Sie zum konfigurierten Installationsverzeichnis: ${INSTALLDIR. Versuchen Sie, eine Verbindung mit dem VNXe-Gerät herzustellen, indem Sie Folgendes eingeben: uemcli -d <Ihre IP> -u <Ihre ID> /sys/general show

Weitere Informationen finden Sie in der"Support" Seite oder in der"Datensammler-Supportmatrix" .

Datensammler der Dell EMC VMAX- und PowerMax-Gerätefamilie

Data Infrastructure Insights erkennt EMC VMAX- und PowerMax-Speicher-Arrays mithilfe von Solutions Enabler-Symcli-Befehlen in Verbindung mit einem vorhandenen Solutions Enabler-Server in Ihrer Umgebung. Der vorhandene Solutions Enabler-Server verfügt über eine Verbindung zum VMAX/PowerMax-Speicherarray durch Zugriff auf Gatekeeper-Volumes.

Anforderungen

Bevor Sie diesen Datensammler konfigurieren, sollten Sie sicherstellen, dass Data Infrastructure Insights über eine TCP-Konnektivität zu Port 2707 auf dem vorhandenen Solutions Enabler-Server verfügt. Data Infrastructure Insights erkennt alle Symmetrix-Arrays, die für diesen Server „lokal“ sind, wie in der Ausgabe „symcfg list“ von diesem Server zu sehen ist.

- Der EMC Solutions Enabler (CLI) mit der SMI-S-Provider-Anwendung muss auf dem Acquisition Unit-Server installiert sein und die Version muss mit der auf dem Solutions Enabler-Server ausgeführten Version übereinstimmen oder älter sein.
- Eine ordnungsgemäß konfigurierte Datei {installdir}\EMC\SYMAPI\config\netcnfg ist erforderlich. Diese Datei definiert Dienstnamen für Solutions Enabler-Server sowie die Zugriffsmethode (SECURE / NOSECURE /ANY).
- Wenn Sie eine Lese-/Schreiblatenz auf Speicherknotenebene benötigen, muss der SMI-S-Anbieter mit einer laufenden Instanz der UNISPHERE für VMAX-Anwendung kommunizieren.
- IP-Adresse des verwaltenden Solutions Enabler-Servers
- Administratorberechtigungen auf dem Solutions Enabler (SE)-Server
- Nur-Lese-Benutzername und Passwort für die SE-Software
- Die UNISPHERE für VMAX-Anwendung muss ausgeführt werden und Statistiken für die EMC VMAX- und PowerMax-Speicherarrays sammeln, die von der SMI-S Provider-Installation verwaltet werden.
- Zugriffsvalidierung für die Leistung: Gehen Sie in einem Webbrowser auf Ihrer Erfassungseinheit zu *https://<SMI-S-Hostname oder IP>:5989/ecomconfig*, wobei „SMI-S-Hostname oder IP“ die IP-Adresse oder der Hostname Ihres SMI-S-Servers ist. Diese URL führt zu einem Verwaltungsportal für den EMC SMI-S-Dienst (auch bekannt als „ECOM“). Sie erhalten ein Anmelde-Popup.
- Berechtigungen müssen in der Daemon-Konfigurationsdatei des Solutions Enabler-Servers deklariert werden, die sich normalerweise hier befindet: */var/symapi/config/daemon_users*

  Hier ist eine Beispieldatei mit den richtigen Cisys-Berechtigungen.

```
root@cernciaukc101:/root
14:11:25 # tail /var/symapi/config/daemon_users
###
###     Refer to the storrdfd(3) man page for additional details.
###
###     As noted above, only authorized users can perform stordaemon
control
###     operations (e.g., shutdown).
#############################################################################
########
# smith         storrdfd
cisys storapid <all>
```

Terminologie

Data Infrastructure Insights erhält die folgenden Bestandsinformationen aus der EMC VMAX/PowerMax-Datenquelle. Für jeden erworbenen Vermögenswerttyp wird die am häufigsten verwendete Terminologie für diesen Vermögenswert angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses

Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Scheibe	Scheibe
Datenträgergruppe	Datenträgergruppe
Storage	Array-Speicher
Direktor	Speicherknoten
Gerätepool, Speicherressourcenpool (SRP)	Speicherpool
Gerät TDev	Volumen

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Konfiguration

Hinweis: Wenn die SMI-S-Benutzerauthentifizierung nicht aktiviert ist, werden die Standardwerte im Data Infrastructure Insights -Datenkollektor ignoriert.

Feld	Beschreibung
Dienstname	Dienstname wie in der Datei *netcnfg* angegeben
Vollständiger Pfad zur CLI	Vollständiger Pfad zum Ordner, der die Symmetrix CLI enthält
SMI-S-Host-IP-Adresse	IP-Adresse des SMI-S-Hosts

Erweiterte Konfiguration

Feld	Beschreibung
Inventarabfrageintervall (min)	Intervall zwischen den Bestandsabfragen. Der Standardwert beträgt 40 Minuten.
Wählen Sie „Ausschließen“ oder „Einschließen“, um eine Liste anzugeben	Geben Sie an, ob die unten stehende Array-Liste beim Sammeln von Daten ein- oder ausgeschlossen werden soll.
Inventarfilter-Geräteliste	Durch Kommas getrennte Liste der ein- oder auszuschließenden Geräte-IDs

Feld	Beschreibung
Verbindungs-Caching	Wählen Sie die Verbindungs-Caching-Methode: * LOKAL bedeutet, dass der Cloud Insights Acquisition-Dienst auf dem Solutions Enabler-Server ausgeführt wird, der über Fibre Channel-Konnektivität zu den Symmetrix-Arrays verfügt, die Sie ermitteln möchten, und Zugriff auf Gatekeeper-Volumes hat. Dies kann bei einigen Remote Acquisition Unit (RAU)-Konfigurationen auftreten. * REMOTE_CACHED ist die Standardeinstellung und sollte in den meisten Fällen verwendet werden. Dabei werden die NETCNFG-Dateieinstellungen verwendet, um über IP eine Verbindung zum Solutions Enabler-Server herzustellen, der über Fibre Channel-Konnektivität zu den Symmetrix-Arrays verfügen muss, die Sie ermitteln möchten, und Zugriff auf Gatekeeper-Volumes hat. * Falls die Option REMOTE_CACHED dazu führt, dass CLI-Befehle fehlschlagen, verwenden Sie die Option REMOTE. Bedenken Sie, dass sich der Erfassungsprozess dadurch verlangsamt (in Extremfällen möglicherweise um Stunden oder sogar Tage). Die NETCNFG-Dateieinstellungen werden weiterhin für eine IP-Verbindung zum Solutions Enabler-Server verwendet, der über Fibre Channel-Konnektivität zu den erkannten Symmetrix-Arrays verfügt. **Hinweis:** Diese Einstellung ändert nicht das Verhalten von Data Infrastructure Insights in Bezug auf die Arrays, die in der Ausgabe „symcfg list“ als REMOTE aufgeführt sind. Data Infrastructure Insights sammelt Daten nur auf Geräten, die durch diesen Befehl als LOKAL angezeigt werden.
SMI-S-Protokoll	Für die Verbindung mit dem SMI-S-Anbieter verwendetes Protokoll. Zeigt auch den verwendeten Standardport an.
SMIS-Port überschreiben	Wenn das Feld „Verbindungstyp“ leer ist, verwenden Sie den Standardport. Andernfalls geben Sie den zu verwendenden Verbindungsport ein.
SMI-S-Benutzername	Benutzername für den SMI-S Provider-Host
SMI-S-Passwort	Benutzername für den SMI-S Provider-Host
Leistungsabfrageintervall (Sek.)	Intervall zwischen Leistungsabfragen (Standard 1000 Sekunden)
Wählen Sie „Ausschließen“ oder „Einschließen“, um eine Liste anzugeben	Geben Sie an, ob die unten stehende Array-Liste beim Erfassen von Leistungsdaten ein- oder ausgeschlossen werden soll.
Leistungsfilter-Geräteliste	Durch Kommas getrennte Liste der ein- oder auszuschließenden Geräte-IDs

Fehlerbehebung

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Problem:	Versuchen Sie Folgendes:
Fehler: Die angeforderte Funktion ist derzeit nicht lizenziert	Installieren Sie die SYMAPI-Serverlizenz.
Fehler: Es wurden keine Geräte gefunden	Stellen Sie sicher, dass Symmetrix-Geräte für die Verwaltung durch den Solutions Enabler-Server konfiguriert sind: – Führen Sie symcfg list -v aus, um die Liste der konfigurierten Symmetrix-Geräte anzuzeigen.
Fehler: Ein angeforderter Netzwerkdienst wurde in der Dienstdatei nicht gefunden	Stellen Sie sicher, dass der Solutions Enabler-Dienstname in der Netcnfg-Datei für Solutions Enabler definiert ist. Diese Datei befindet sich normalerweise unter SYMAPI\config\ in der Solutions Enabler-Clientinstallation.
Fehler: Der Remote-Client/Server-Handshake ist fehlgeschlagen	Überprüfen Sie die aktuellsten storsrvd.log*-Dateien auf dem Solutions Enabler-Host, den wir ermitteln möchten.
Fehler: Allgemeiner Name im Client-Zertifikat ungültig	Bearbeiten Sie die Datei *hosts* auf dem Solutions Enabler-Server, sodass der Hostname der Erfassungseinheit in die IP-Adresse aufgelöst wird, die im storsrvd.log auf dem Solutions Enabler-Server gemeldet wird.
Fehler: Die Funktion konnte keinen Speicher abrufen	Stellen Sie sicher, dass im System genügend freier Speicher zur Ausführung von Solutions Enabler verfügbar ist
Fehler: Solutions Enabler konnte nicht alle erforderlichen Daten bereitstellen.	Untersuchen Sie den Gesundheitszustand und das Lastprofil von Solutions Enabler
Fehler: • Der CLI-Befehl „symcfg list -tdev“ gibt möglicherweise falsche Daten zurück, wenn er mit Solutions Enabler 7.x von einem Solutions Enabler-Server 8.x erfasst wird. • Der CLI-Befehl „symcfg list -srp“ gibt möglicherweise falsche Daten zurück, wenn er mit Solutions Enabler 8.1.0 oder früher von einem Solutions Enabler-Server 8.3 oder höher erfasst wurde.	Stellen Sie sicher, dass Sie dieselbe Hauptversion von Solutions Enabler verwenden

Problem:	Versuchen Sie Folgendes:
Ich sehe Datenerfassungsfehler mit der Meldung: „unbekannter Code“	Diese Meldung wird möglicherweise angezeigt, wenn in der Daemon-Konfigurationsdatei des Solutions Enabler-Servers keine Berechtigungen deklariert sind (siheAnforderungen über.) Dies setzt voraus, dass Ihre SE-Clientversion mit Ihrer SE-Serverversion übereinstimmt. Dieser Fehler kann auch auftreten, wenn der Benutzer *cisys* (der Solutions Enabler-Befehle ausführt) in der Konfigurationsdatei /var/symapi/config/daemon_users nicht mit den erforderlichen Daemon-Berechtigungen konfiguriert wurde. Um dies zu beheben, bearbeiten Sie die Datei /var/symapi/config/daemon_users und stellen Sie sicher, dass der Cisys-Benutzer über die Berechtigung <all> für den Storapid-Daemon verfügt. Beispiel: 14:11:25 # tail /var/symapi/config/daemon_users … cisys storapid <all>

Weitere Informationen finden Sie in der"Support" Seite oder in der"Datensammler-Supportmatrix" .

Dell EMC VNX Block Storage (NaviCLI)-Datenkollektor

Data Infrastructure Insights verwendet den Datensammler Dell EMC VNX Block Storage (NaviSec) (ehemals CLARiiON), um Bestands- und Leistungsdaten zu erfassen.

Terminologie

Data Infrastructure Insights erhält die folgenden Bestandsinformationen vom EMC VNX Block Storage-Datenkollektor. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Scheibe	Scheibe
Storage	Storage
Speicherprozessor	Speicherknoten
Dieser Pool, RAID-Gruppe	Speicherpool
LUN	Volumen

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diese Datenquelle darstellen.

Anforderungen

Für die Datenerhebung müssen folgende Voraussetzungen erfüllt sein:

- Eine IP-Adresse jedes VNX-Blockspeicherprozessors
- Schreibgeschützter Navisphere-Benutzername und -Passwort für die VNX-Blockspeicher-Arrays

- NaviSecCli muss auf der Data Infrastructure Insights AU installiert sein
- Zugriffsvalidierung: Führen Sie NaviSecCLI von der Data Infrastructure Insights AU mit dem Benutzernamen und dem Kennwort für jedes Array aus.
- Portanforderungen: 80, 443
- Die NaviSecCLI-Version sollte dem neuesten FLARE-Code auf Ihrem Array entsprechen
- Aus Leistungsgründen muss die Statistikprotokollierung aktiviert sein.

Syntax der NaviSphere-Befehlszeilenschnittstelle

naviseccli.exe -h <IP-Adresse> -user <Benutzer> -password <Passwort> -scope <Bereich, verwenden Sie 0 für den globalen Bereich> -port <verwenden Sie standardmäßig 443> Befehl

Konfiguration

Feld	Beschreibung
VNX-Blockspeicher-IP-Adresse	IP-Adresse oder vollqualifizierter Domänenname des VNX-Blockspeichers
Benutzername	Name, der für die Anmeldung beim VNX-Blockspeichergerät verwendet wird.
Passwort	Kennwort zum Anmelden beim VNX-Blockspeichergerät.
CLI-Pfad zu naviseccli.exe	Vollständiger Pfad zum Ordner, der die ausführbare Datei *naviseccli.exe* enthält

Erweiterte Konfiguration

Feld	Beschreibung
Inventarabfrageintervall (min)	Intervall zwischen den Bestandsabfragen. Der Standardwert ist 40 Minuten.
Umfang	Der sichere Clientbereich. Die Standardeinstellung ist „Global“.
Leistungsabfrageintervall (Sek.)	Intervall zwischen Leistungsabfragen. Der Standardwert beträgt 300 Sekunden.

Fehlerbehebung

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Inventar

Problem:	Versuchen Sie Folgendes:
Fehler: • Agent wird nicht ausgeführt • Naviseccli konnte nicht gefunden werden • Kein Befehl konnte ausgeführt werden	• Bestätigen Sie, dass NaviSphere CLI auf der Cloud Insight Acquisition Unit installiert ist • Sie haben im Konfigurationsassistenten des Datensammlers nicht die Option „Sicheren Client verwenden“ ausgewählt und keine nicht sichere Version von Naviphere CLI installiert. • Bestätigen Sie, dass das NaviSphere CLI-Installationsverzeichnis in der Datensammlerkonfiguration korrekt ist • Bestätigen Sie, dass die IP des VNX-Blockspeichers in der Datensammlerkonfiguration korrekt ist: • Von der Data Infrastructure Insights Acquisition Unit: ◦ Öffnen Sie eine CMD. ◦ Ändern Sie das Verzeichnis in das konfigurierte Installationsverzeichnis ◦ Versuchen Sie, eine Verbindung mit dem VNX-Blockspeichergerät herzustellen, indem Sie „navicli -h {ip} getagent“ eingeben (ersetzen Sie {ip} durch die tatsächliche IP).
Fehler: 4.29 emc235848 emc241018 getall Fehler beim Parsen der Host-Alias-Informationen	Dies wird wahrscheinlich durch ein FLARE 29-Beschädigungsproblem der Host-Initiator-Datenbank auf dem Array selbst verursacht. Siehe EMC-Wissensdatenbankartikel: emc235848, emc241018. Sie können auch überprüfen https://now.netapp.com/Knowledgebase/solutionarea.asp?id=kb58128
Fehler: Meta-LUNs konnten nicht abgerufen werden. Fehler beim Ausführen von java -jar navicli.jar	• Ändern Sie die Datensammlerkonfiguration, um den sicheren Client zu verwenden (empfohlen) • Installieren Sie navicli.jar im CLI-Pfad zu navicli.exe ODER naviseccli.exe • Hinweis: navicli.jar ist ab EMC Navisphere Version 6.26 veraltet. • Die navicli.jar ist möglicherweise verfügbar auf http://powerlink.emc.com
Fehler: Speicherpools melden keine Datenträger auf dem Serviceprozessor unter der konfigurierten IP-Adresse	Konfigurieren Sie den Datensammler mit beiden Serviceprozessor-IPs, getrennt durch ein Komma

Problem:	Versuchen Sie Folgendes:
Fehler: Revisionskonflikt	• Dies wird normalerweise dadurch verursacht, dass die Firmware auf dem VNX-Blockspeichergerät aktualisiert wird, nicht jedoch die Installation von NaviCLI.exe. Dies kann auch daran liegen, dass auf verschiedenen Geräten unterschiedliche Firmwares vorhanden sind, aber nur eine CLI (mit einer anderen Firmware-Version) installiert ist. • Stellen Sie sicher, dass auf dem Gerät und dem Host identische Versionen der Software ausgeführt werden: ◦ Öffnen Sie in der Data Infrastructure Insights Acquisition Unit ein Befehlszeilenfenster ◦ Ändern Sie das Verzeichnis in das konfigurierte Installationsverzeichnis ◦ Stellen Sie eine Verbindung mit dem CLARiiON-Gerät her, indem Sie „navicli -h <ip> getagent“ eingeben. ◦ Suchen Sie in den ersten Zeilen nach der Versionsnummer. Beispiel: „Agent Rev: 6.16.2 (0.1)“ ◦ Suchen und vergleichen Sie die Version in der ersten Zeile. Beispiel: „Navisphere CLI Revision 6.07.00.04.07“
Fehler: Nicht unterstützte Konfiguration – Keine Fibre Channel-Ports	Das Gerät ist nicht mit Fibre-Channel-Ports konfiguriert. Derzeit werden nur FC-Konfigurationen unterstützt. Überprüfen Sie, ob diese Version/Firmware unterstützt wird.

Weitere Informationen finden Sie in der"Support" Seite oder in der"Datensammler-Supportmatrix" .

DELL EMC VNX File (früher Celerra Unified Storage System) Datenkollektor

Dieser Datensammler ruft Inventarinformationen vom VNX File Storage System ab. Zur Konfiguration benötigt dieser Datensammler die IP-Adresse der Speicherprozessoren sowie einen schreibgeschützten Benutzernamen und ein Passwort.

Terminologie

Data Infrastructure Insights erhält die folgenden Bestandsinformationen vom VNX File-Datenkollektor. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Celerra-Netzwerkserver/Celerra-Speicherpool	Speicherpool
Dateisystem	Internes Volumen
Datenverschieber	Regler
Auf einem Data Mover gemountetes Dateisystem	Dateifreigabe
CIFS- und NFS-Exporte	Aktie
Datenträgervolumen	Backend-LUN

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Anforderungen

Zur Konfiguration dieses Datensammlers benötigen Sie Folgendes:

- Die IP-Adresse des Speicherprozessors
- Benutzername und Kennwort nur zum Lesen
- SSH-Port 22

Konfiguration

Feld	Beschreibung
VNX-Datei-IP-Adresse	IP-Adresse oder vollqualifizierter Domänenname des VNX-Dateigeräts
Benutzername	Name, der für die Anmeldung beim VNX-Dateigerät verwendet wird
Passwort	Kennwort zum Anmelden beim VNX-Dateigerät

Erweiterte Konfiguration

Feld	Beschreibung
Inventarabfrageintervall (Minuten)	Intervall zwischen den Bestandsabfragen. Der Standardwert beträgt 20 Minuten.

Fehlerbehebung

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Inventar

Problem:	Versuchen Sie Folgendes:
Fehler: Fortfahren nicht möglich, während DART-Update läuft	Mögliche Lösung: Halten Sie den Datensammler an und warten Sie, bis das DART-Upgrade abgeschlossen ist, bevor Sie eine weitere Erfassungsanforderung versuchen.

Weitere Informationen finden Sie in der"Support" Seite oder in der"Datensammler-Supportmatrix" .

Konfigurieren des Dell EMC VNX Unified-Datenkollektors

Zur Konfiguration benötigt der Dell EMC VNX Unified (SSH)-Datensammler die IP-Adresse der Control Station sowie einen schreibgeschützten Benutzernamen und ein Kennwort.

Terminologie

Data Infrastructure Insights erhält von diesem Datensammler die folgenden Bestandsinformationen. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Scheibe	Scheibe
Datenträgerordner	Datenträgergruppe
Dateisystem	Internes Volumen
Storage	Storage
Speicherprozessor	Speicherknoten
Speicherpool, RAID-Gruppe	Speicherpool
LUN	Volumen
Datenverschieber	Regler
Auf einem Data Mover gemountetes Dateisystem	Dateifreigabe
CIFS- und NFS-Exporte	Aktie
Datenträgervolumen	Backend-LUN

Anforderungen

Zum Konfigurieren des VNX (SSH)-Datenkollektors benötigen Sie Folgendes:

- VNX-IP-Adresse und Anmeldeinformationen für die Celerra Control Station.
- Benutzername und Passwort sind schreibgeschützt.
- Der Datensammler kann NaviCLI/NaviSecCLI-Befehle auf dem Backend-Array ausführen, indem er die DART OS NAS-Köpfe nutzt.

Konfiguration

Feld	Beschreibung
VNX-IP-Adresse	IP-Adresse oder vollqualifizierter Domänenname der VNX Control Station
Benutzername	Benutzername für die VNX Control Station
Passwort	Passwort für die VNX Control Station

Erweiterte Konfiguration

Feld	Beschreibung
Inventarabfrageintervall (min)	Intervall zwischen den Bestandsabfragen. Der Standardwert beträgt 40 Minuten.
Leistungsabfrageintervall (Sek.).	Intervall zwischen Leistungsabfragen. Der Standardwert beträgt 300 Sekunden.

Fehlerbehebung

Weitere Informationen zu diesem Datensammler finden Sie im"Support" Seite oder in der"Datensammler-Supportmatrix" .

Konfigurieren des EMC VPLEX-Datenkollektors

Dieser Datensammler erfasst Bestands- und Leistungsdaten von EMC VPLEX-Speichersystemen. Zur Konfiguration benötigt der Datensammler eine IP-Adresse des VPLEX-Servers und ein Domänenkonto auf Administratorebene.

Für die Leistungserfassung von Data Infrastructure Insights aus Vplex-Clustern muss der Leistungsarchivdienst betriebsbereit sein, um die CSV-Dateien und Protokolle zu füllen, die Data Infrastructure Insights über SCP-basierte Dateikopien abruft. NetApp hat festgestellt, dass diese Funktionalität bei vielen Vplex-Firmware-Upgrades/Management-Station-Updates nicht mehr funktioniert. Kunden, die solche Upgrades planen, möchten Dell/EMC möglicherweise proaktiv fragen, ob diese Funktionalität durch das geplante Upgrade nicht mehr funktionsfähig ist, und wenn ja, wie sie sie wieder aktivieren können, um Lücken in der Leistungstransparenz zu minimieren. Der Vplex-Leistungscode von Cloud Insight prüft bei jeder Abfrage, ob alle erwarteten Dateien vorhanden sind und ob sie ordnungsgemäß aktualisiert werden. Wenn sie fehlen oder veraltet sind, protokolliert Data Infrastructure Insights Leistungserfassungsfehler.

Terminologie

Data Infrastructure Insightst erhält die folgenden Bestandsinformationen vom VPLEX-Datensammler. Für jeden erworbenen Vermögenswerttyp wird die am häufigsten verwendete Terminologie für diesen Vermögenswert angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Cluster	Storage
Motor	Speicherknoten
Gerät, Systemumfang	Backend-Speicherpool
Virtuelles Volume	Volumen
Front-End-Port, Back-End-Port	Hafen
Verteiltes Gerät	Speichersynchronisierung
Speicheransicht	Volumenkarte, Volumenmaske
Speichervolumen	Backend-LUN

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
ITLs	Backend-Pfad

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Anforderungen

- Eine IP-Adresse der VPLEX-Verwaltungskonsole
- Domänenkonto auf Administratorebene für den VPLEX-Server
- Port 443 (HTTPS). Erfordert ausgehende Konnektivität zum TCP-Port 443 auf der VPLEX-Verwaltungsstation.
- Aus Leistungsgründen sind Benutzername und Kennwort für den SSH-/SCP-Zugriff schreibgeschützt.
- Aus Leistungsgründen ist Port 22 erforderlich.

Konfiguration

Feld	Beschreibung
IP-Adresse der VPLEX-Verwaltungskonsole	IP-Adresse oder vollqualifizierter Domänenname der VPLEX-Verwaltungskonsole
Benutzername	Benutzername für VPLEX CLI
Passwort	Für VPLEX CLI verwendetes Kennwort
Leistung Remote-IP-Adresse	Leistung Remote-IP-Adresse der VPLEX-Verwaltungskonsole
Performance Remote-Benutzername	Leistung Remote-Benutzername der VPLEX-Verwaltungskonsole
Performance Remote-Passwort	Leistungs-Remotekennwort der VPLEX-Verwaltungskonsole

Erweiterte Konfiguration

Feld	Beschreibung
Kommunikationsanschluss	Für VPLEX CLI verwendeter Port. Der Standardwert ist 443.
Inventarabfrageintervall (min)	Der Standardwert beträgt 20 Minuten.
Anzahl der Verbindungsversuche	Der Standardwert ist 3.
Leistungsabfrageintervall (Sek.)	Intervall zwischen Leistungsabfragen. Der Standardwert beträgt 600 Sekunden.
Anzahl der Wiederholungsversuche	Der Standardwert ist 2.

Fehlerbehebung

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Inventar

Problem:	Versuchen Sie Folgendes:
Fehler: Benutzerauthentifizierung fehlgeschlagen.	Stellen Sie sicher, dass Ihre Anmeldeinformationen für dieses Gerät korrekt sind.

Performance

Problem:	Versuchen Sie Folgendes:
Fehler: Die VPLEX-Leistung für Versionen unter 5.3 wird nicht unterstützt.	Aktualisieren Sie VPLEX auf 5.3 oder höher
Fehler: Nicht genügend Daten gesammelt.	• Prüfen Sie den Erfassungszeitstempel in der Protokolldatei und ändern Sie das Abfrageintervall entsprechend. • Warten Sie länger
Fehler: Perpetual-Log-Dateien werden nicht aktualisiert.	Bitte kontaktieren Sie den EMC-Support, um die Aktualisierung der permanenten Protokolldateien zu aktivieren
Fehler: Das Leistungsabfrageintervall ist zu groß.	Überprüfen Sie den Erfassungszeitstempel in der Protokolldatei ${logfile} und ändern Sie das Abfrageintervall entsprechend
Fehler: Die Remote-IP-Adresse der VPLEX-Verwaltungskonsole ist nicht konfiguriert.	Bearbeiten Sie die Datenquelle, um die Performance-Remote-IP-Adresse der VPLEX-Verwaltungskonsole festzulegen.
Fehler: Keine Leistungsdaten vom Direktor gemeldet	• Überprüfen Sie, ob die Systemleistungsmonitore ordnungsgemäß ausgeführt werden. • Wenden Sie sich an den EMC-Support, um die Aktualisierung der Protokolldateien des Systemleistungsmonitors zu ermöglichen.

Weitere Informationen finden Sie in der"Support" Seite oder in der"Datensammler-Supportmatrix" .

Dell EMC XtremeIO-Datenkollektor

Der EMC XtremIO-Datenkollektor erfasst Bestands- und Leistungsdaten vom EMC XtremIO-Speichersystem.

Anforderungen

Zum Konfigurieren des EMC XtremIO (HTTP)-Datenkollektors benötigen Sie:

- Die Hostadresse des XtremIO Management Servers (XMS)
- Ein Konto mit Administratorrechten
- Zugriff auf Port 443 (HTTPS)

Terminologie

Data Infrastructure Insights erhält die folgenden Bestandsinformationen vom EMC XtremIO-Datenkollektor. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten verwendete Terminologie

für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieser Datenquelle die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Festplatte (SSD)	Scheibe
Cluster	Storage
Regler	Speicherknoten
Volumen	Volumen
LUN-Karte	Volumenkarte
Ziel-FC-Initiator	Volumenmaske

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diese Datenquelle darstellen.

Anforderungen

- Die Host-IP-Adresse des XtremIO Management Server (XMS)
- Administratorbenutzername und -kennwort für XtremIO

Konfiguration

Feld	Beschreibung
XMS-Host	IP-Adresse oder vollqualifizierter Domänenname des XtremIO-Managementservers
Benutzername	Benutzername für den XtremIO-Managementserver
Passwort	Kennwort für den XtremIO-Managementserver

Erweiterte Konfiguration

Feld	Beschreibung
TCP-Port	TCP-Port, der für die Verbindung mit dem XTremIO-Verwaltungsserver verwendet wird. Der Standardwert ist 443.
Inventarabfrageintervall (min)	Intervall zwischen den Bestandsabfragen. Der Standardwert beträgt 60 Minuten.
Leistungsabfrageintervall (Sek.)	Intervall zwischen Leistungsabfragen. Der Standardwert beträgt 300 Sekunden.

Fehlerbehebung

Weitere Informationen zu diesem Datensammler finden Sie im"Support" Seite oder in der"Datensammler-Supportmatrix" .

Fujitsu Eternus Datensammler

Der Fujitsu Eternus-Datenkollektor erfasst Inventardaten mithilfe des Administratorzugriffs auf das Speichersystem.

Terminologie

Data Infrastructure Insights erfasst die folgenden Bestandsinformationen vom Fujitsu Eternus-Speicher. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Scheibe	Scheibe
Storage	Storage
Thin Pool, Flexible Tier Pool, Raid-Gruppe	Speicherpool
Standard-Volume, Snap-Daten-Volume (SDV), Snap-Daten-Pool-Volume (SDPV), Thin-Provisioning-Volume (TPV), Flexible-Tier-Volume (FTV), Wide-Striping-Volume (WSV)	Volumen
Kanaladapter	Regler

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Anforderungen

Zur Konfiguration dieses Datensammlers sind folgende Voraussetzungen erforderlich:

- Eine IP-Adresse des Eternus-Speichers, die nicht durch Kommas getrennt sein darf
- Benutzername und Kennwort auf SSH-Administrationsebene
- Port 22
- Stellen Sie sicher, dass das Scrollen der Seite deaktiviert ist (clienv-show-more-scroll disable)

Konfiguration

Feld	Beschreibung
IP-Adresse des Eternus-Speichers	IP-Adresse des Eternus-Speichers
Benutzername	Benutzername für Eternus-Speicher
Passwort	Passwort für den Eternus-Speicher

Erweiterte Konfiguration

Feld	Beschreibung
Inventarabfrageintervall (min)	Der Standardwert beträgt 20 Minuten.

Fehlerbehebung

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Inventar

Problem:	Versuchen Sie Folgendes:
„Fehler beim Abrufen der Daten“ mit den Fehlermeldungen „Fehler beim Suchen der Eingabeaufforderung CLI“ oder „Fehler beim Suchen der Eingabeaufforderung am Ende der Shell-Ergebnisse“	Wahrscheinliche Ursache: Im Speichersystem ist das Scrollen von Seiten aktiviert. Mögliche Lösung: * Versuchen Sie, das Scrollen der Seite zu deaktivieren, indem Sie den folgenden Befehl ausführen: set clienv-show-more -scroll disable
„Verbindungsfehler“ mit den Fehlermeldungen „Fehler beim Herstellen einer SSH-Verbindung zum Speicher“ oder „Fehler beim Herstellen einer Verbindung zu VirtualCenter“	Mögliche Ursachen: * Falsche Anmeldeinformationen. * Falsche IP-Adresse. * Netzwerkproblem. * Der Speicher ist möglicherweise ausgefallen oder reagiert nicht. Mögliche Lösungen: * Überprüfen Sie die eingegebenen Anmeldeinformationen und die IP-Adresse. * Versuchen Sie, über den SSH-Client mit dem Speicher zu kommunizieren.

Weitere Informationen finden Sie in der"Support" Seite oder in der"Datensammler-Supportmatrix" .

NetApp Google Compute-Datenkollektor

Dieser Datensammler unterstützt die Bestands- und Leistungserfassung von Google Compute-Cloud-Plattformkonfigurationen. Dieser Collector versucht, alle Rechenressourcen in allen Projekten einer Google-Organisation zu ermitteln. Wenn Sie mehrere Google-Organisationen haben, die Sie mit Data Infrastructure Insights ermitteln möchten, sollten Sie pro Organisation einen Data Infrastructure Insights -Collector bereitstellen.

Anforderungen für Dienstkonten

- Sie müssen ein Dienstkonto erstellen, indem Sie den Anweisungen in"Erstellen/Verwalten von Dienstkonten" . Ein solches Dienstkonto wird durch eine eindeutige ID identifiziert, die als *clientId* bezeichnet wird und als Benutzername verwendet wird.
- Erstellen Sie außerdem einen Dienstkontoschlüssel, indem Sie den Anweisungen in"Erstellen/Verwalten von Dienstkontoschlüsseln" . Dieser Schlüssel kann als JSON-Datei heruntergeladen werden, deren Inhalt als Passwort verwendet wird.
- Das Dienstkonto muss auf *compute.readonly*, *monitoring.read* und *cloud-platform* beschränkt sein.

Konfiguration

Feld	Beschreibung
Organisations-ID	Die Organisations-ID, die Sie mit diesem Collector ermitteln möchten. Dieses Feld ist erforderlich, wenn Ihr Servicekonto mehr als eine Organisation sehen kann

Feld	Beschreibung
Wählen Sie „Ausschließen“ oder „Einschließen“, um GCP-Projekte nach IDs zu filtern	Wenn Sie einschränken möchten, welche Projektressourcen in Data Infrastructure Insights eingebracht werden.
Projekt-IDs	Die Liste der Projekt-IDs, die Sie je nach Wert des Werts „Wählen Sie ‚Ausschließen‘ …“ in die Erkennung ein- oder ausfiltern möchten. Die Standardliste ist leer
Client-ID	Client-ID für die Google Cloud Platform-Konfiguration
Kopieren Sie den Inhalt Ihrer Google-Anmeldeinformationsdatei und fügen Sie ihn hier ein.	Kopieren Sie Ihre Google-Anmeldeinformationen für das Cloud Platform-Konto in dieses Feld

Erweiterte Konfiguration

Feld	Beschreibung
Inventarabfrageintervall (min)	Der Standardwert ist 60 Minuten
Wählen Sie „Ausschließen“ oder „Einschließen“, um VMs nach Labels zu filtern.	Geben Sie an, ob VMs beim Sammeln von Daten anhand von Labels ein- oder ausgeschlossen werden sollen. Wenn „Einschließen“ ausgewählt ist, darf das Feld „Beschriftungsschlüssel“ nicht leer sein.
Label-Schlüssel und -Werte zum Filtern von VMs	Klicken Sie auf **+ Bezeichnung filtern**, um auszuwählen, welche VMs (und zugehörigen Datenträger) ein-/ausgeschlossen werden sollen, indem Sie nach Schlüsseln und Werten filtern, die mit den Schlüsseln und Werten der Bezeichnungen auf der VM übereinstimmen. Der Beschriftungsschlüssel ist erforderlich, der Beschriftungswert ist optional. Wenn der Labelwert leer ist, wird die VM gefiltert, solange sie mit dem Labelschlüssel übereinstimmt.
Leistungsabfrageintervall (Sek.)	Der Standardwert ist 1800 Sekunden

Fehlerbehebung

Weitere Informationen zu diesem Datensammler finden Sie im"Support" Seite oder in der"Datensammler-Supportmatrix" .

Google Cloud NetApp Volumes Datensammler

Dieser Datensammler unterstützt die Bestands- und Leistungserfassung von Google Cloud NetApp Volumes -Konfigurationen. Der Collector erkennt NetApp -Volumes und Speicherressourcen in allen Projekten innerhalb einer Google-Organisation. Wenn Sie mehrere Google-Organisationen haben, die Sie mit Data Infrastructure Insights überwachen möchten, stellen Sie einen Collector pro Organisation bereit.

Anforderungen für Dienstkonten

- Sie müssen ein Dienstkonto erstellen, indem Sie den Anweisungen in"Erstellen/Verwalten von

Dienstkonten" . Dieses Dienstkonto wird durch eine eindeutige ID identifiziert, die als *clientId* bezeichnet wird und als Benutzername verwendet wird.

- Erstellen Sie außerdem einen Dienstkontoschlüssel, indem Sie den Anweisungen in"Erstellen/Verwalten von Dienstkontoschlüsseln" . Dieser Schlüssel kann als JSON-Datei heruntergeladen werden, deren Inhalt als Passwort verwendet wird.
- Das Dienstkonto muss auf *compute.readonly*, *monitoring.read* und *cloud-platform* beschränkt sein.

Konfiguration

Feld	Beschreibung
Organisations-ID	Die Organisations-ID, die Sie mit diesem Collector ermitteln möchten. Dieses Feld ist erforderlich, wenn Ihr Servicekonto mehr als eine Organisation sehen kann
Wählen Sie „Ausschließen“ oder „Einschließen“, um GCNV-Assets nach Standort zu filtern	Die Standardeinstellung ist „Ausschließen“, da dieser Collector standardmäßig alle GCNV-Volumes weltweit innerhalb Ihrer Organisation ermitteln soll.
GCNV-Standorte ausschließen/einschließen	Dies ist standardmäßig leer und wird in Verbindung mit der Option „Wählen Sie ‚Ausschließen‘ oder ‚Einschließen‘“ verwendet. Wenn Sie Assets nur in bestimmten Regionen entdecken möchten, verwenden Sie diese beiden Optionen, um den Umfang dieses Collectors einzuschränken.
Projekt-IDs	Die Liste der Projekt-IDs, die Sie je nach Wert des Werts „Wählen Sie ‚Ausschließen‘ …“ in die Erkennung ein- oder ausfiltern möchten. Die Standardliste ist leer
Client-ID	Client-ID für die Google Cloud Platform-Konfiguration
Kopieren Sie den Inhalt Ihrer Google-Anmeldeinformationsdatei und fügen Sie ihn hier ein.	Kopieren Sie Ihre Google-Anmeldeinformationen für das Cloud Platform-Konto in dieses Feld

Erweiterte Konfiguration

Feld	Beschreibung
Inventarabfrageintervall (min)	Der Standardwert ist 60 Minuten
Verwenden Sie den AU-Proxy für REST-API-Aufrufe	Wählen Sie diese Option, damit der Collector denselben Proxy verwendet wie die Erfassungseinheit, auf der sich der Collector befindet. Standardmäßig ist dies deaktiviert, was bedeutet, dass der Collector versucht, HTTPS-API-Aufrufe direkt an Google zu senden.

Feld	Beschreibung
Label-Schlüssel und -Werte zum Filtern von VMs	Klicken Sie auf **+ Bezeichnung filtern**, um auszuwählen, welche VMs (und zugehörigen Datenträger) ein-/ausgeschlossen werden sollen, indem Sie nach Schlüsseln und Werten filtern, die mit den Schlüsseln und Werten der Bezeichnungen auf der VM übereinstimmen. Der Beschriftungsschlüssel ist erforderlich, der Beschriftungswert ist optional. Wenn der Labelwert leer ist, wird die VM gefiltert, solange sie mit dem Labelschlüssel übereinstimmt.
Leistungsabfrageintervall (Sek.)	Der Standardwert ist 300 Sekunden

Fehlerbehebung

Weitere Informationen zu diesem Datensammler finden Sie im"Support" Seite oder in der"Datensammler-Supportmatrix" .

HP Unternehmen

HP Enterprise Alletra 9000 / Primera Storage Datensammler

Data Infrastructure Insights verwendet den Datensammler HP Enterprise Alletra 9000 / HP Enterprise Primera (früher 3PAR), um Inventar und Leistung zu ermitteln.

Terminologie

Data Infrastructure Insights erhält von diesem Datensammler die folgenden Bestandsinformationen. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Feld	Beschreibung
Physische Festplatte	Scheibe
Speichersystem	Storage
Controller-Knoten	Speicherknoten
Gemeinsame Bereitstellungsgruppe	Speicherpool
Virtuelles Volume	Volumen

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Anforderungen

Zur Konfiguration dieses Datensammlers sind folgende Voraussetzungen erforderlich:

- IP-Adresse oder FQDN des InServ-Clusters
- Für die Bestandsaufnahme sind Benutzername und Kennwort für den StoreServ-Server schreibgeschützt.

- Aus Leistungsgründen Lese-/Schreibzugriff auf den Benutzernamen und das Kennwort für den StoreServ-Server
- Portanforderungen: 22 (Inventarerfassung), 5988 oder 5989 (Leistungserfassung) [Hinweis: Leistung wird für StoreServ OS 3.x+ unterstützt]
- Bestätigen Sie zur Leistungserfassung, dass SMI-S aktiviert ist, indem Sie sich per SSH beim Array anmelden.

Konfiguration

Feld	Beschreibung
Speicher-IP-Adresse	Speicher-IP-Adresse oder vollqualifizierter Domänenname des StoreServ-Clusters
Benutzername	Benutzername für den StoreServ-Server
Passwort	Für den StoreServ-Server verwendetes Kennwort
SMI-S-Benutzername	Benutzername für den SMI-S Provider-Host
SMI-S-Passwort	Für den SMI-S-Provider-Host verwendetes Kennwort

Erweiterte Konfiguration

Feld	Beschreibung
Inventarabfrageintervall (min)	Intervall zwischen den Bestandsabfragen. Der Standardwert beträgt 40 Minuten.
SMI-S-Konnektivität	Für die Verbindung mit dem SMI-S-Provider verwendetes Protokoll
SMI-S-Standardport überschreiben	Wenn leer, verwenden Sie den Standardport von SMI-S Connectivity, andernfalls geben Sie den zu verwendenden Verbindungsport ein
Leistungsabfrageintervall (Sek.)	Intervall zwischen Leistungsabfragen. Der Standardwert beträgt 300 Sekunden.

Fehlerbehebung

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Inventar

Problem:	Versuchen Sie Folgendes:
Der Befehl „showsys“ gibt kein Ergebnis zurück.	Führen Sie „showsys“ und „showversion -a“ von der Befehlszeile aus und prüfen Sie, ob die Version vom Array unterstützt wird.

Performance

Problem:	Versuchen Sie Folgendes:
Verbindung oder Anmeldung fehlgeschlagen. Die Initialisierung des Anbieters ist fehlgeschlagen.	Ein rein numerischer Array-Name kann Probleme mit dem SMI-S-Server verursachen. Versuchen Sie, den Array-Namen zu ändern.
Der konfigurierte SMI-S-Benutzer hat keine Domäne	Gewähren Sie dem konfigurierten SMI-S-Benutzer entsprechende Domänenberechtigungen
Data Infrastructure Insights gibt an, dass keine Verbindung zum SMI-S-Dienst hergestellt bzw. keine Anmeldung möglich ist.	Stellen Sie sicher, dass sich zwischen der CI AU und dem Array keine Firewall befindet, die die CI AU daran hindern würde, TCP-Verbindungen zu 5988 oder 5989 herzustellen. Wenn dies erledigt ist und Sie bestätigt haben, dass keine Firewall vorhanden ist, sollten Sie per SSH auf das Array zugreifen und zur Bestätigung den Befehl „showcim“ verwenden. Überprüfen Sie, ob: * der Dienst aktiviert ist * HTTPS aktiviert ist * der HTTPS-Port 5989 sein sollte. Wenn dies alles der Fall ist, können Sie versuchen, „stopcim“ und dann „startcim“ auszuführen, um das CIM (d. h. den SMI-S-Dienst) neu zu starten.

Weitere Informationen finden Sie in der"Support" Seite oder in der"Datensammler-Supportmatrix" .

HP Enterprise Command View-Datensammler

Der HP Enterprise Command View Advanced Edition-Datensammler unterstützt die Erkennung von XP- und P9500-Arrays über den Command View Advanced Edition (CVAE)-Server. Data Infrastructure Insights kommuniziert mit CVAE über die standardmäßige Command View-API, um Bestands- und Leistungsdaten zu erfassen.

Terminologie

Data Infrastructure Insights erhält die folgenden Bestandsinformationen vom HP Enterprise Command View-Datensammler. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
PDEV	Scheibe
Zeitschriftenpool	Datenträgergruppe
Speicher-Array	Storage
Port-Controller	Speicherknoten
Array-Gruppe, DP-Pool	Speicherpool
Logische Einheit, LDEV	Volumen

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Inventaranforderungen

Um Bestandsdaten erfassen zu können, benötigen Sie Folgendes:

- IP-Adresse des CVAE-Servers
- Nur-Lese-Benutzername und Passwort für die CVAE-Software und Peer-Berechtigungen
- Portanforderung: 2001

Leistungsanforderungen

Um Leistungsdaten erfassen zu können, müssen folgende Voraussetzungen erfüllt sein:

- HDS USP-, USP V- und VSP-Leistung
  - Performance Monitor muss lizenziert sein.
  - Der Überwachungsschalter muss aktiviert sein.
  - Das Exporttool (Export.exe) muss in die Data Infrastructure Insights AU kopiert und an einen Speicherort extrahiert werden. Stellen Sie auf CI Linux AUs sicher, dass „cisys“ über Lese- und Ausführungsberechtigungen verfügt.
  - Die Version des Exporttools muss mit der Mikrocodeversion des Zielarrays übereinstimmen.
- AMS-Leistung:
  - Performance Monitor muss lizenziert sein.
  - Das CLI-Dienstprogramm Storage Navigator Modular 2 (SNM2) muss auf der Data Infrastructure Insights AU installiert werden.
- Netzwerkanforderungen
  - Die Exporttools basieren auf Java und verwenden RMI, um mit dem Array zu kommunizieren. Diese Tools sind möglicherweise nicht Firewall-freundlich, da sie bei jedem Aufruf die Quell- und Ziel-TCP-Ports dynamisch aushandeln. Außerdem können sich die Export-Tools verschiedener Modell-Arrays im Netzwerk unterschiedlich verhalten. Wenden Sie sich an HPE, um die Anforderungen Ihres Modells zu erfahren.

Konfiguration

Feld	Beschreibung
Command View Server	IP-Adresse oder vollqualifizierter Domänenname des Command View-Servers
Benutzername	Benutzername für den Command View-Server.
Passwort	Für den Command View-Server verwendetes Kennwort.
Geräte - VSP G1000 (R800), VSP (R700), HUS VM (HM700) und USP-Speicher	Geräteliste für VSP G1000 (R800), VSP (R700), HUS VM (HM700) und USP-Speicher. Jeder Speicher benötigt: * Array-IP: IP-Adresse des Speichers * Benutzername: Benutzername für den Speicher * Passwort: Passwort für den Speicher * Ordner mit den JAR-Dateien des Export-Dienstprogramms

Feld	Beschreibung
SNM2Devices – WMS/SMS/AMS-Speicher	Geräteliste für WMS/SMS/AMS-Speicher. Jeder Speicher benötigt: * Array-IP: IP-Adresse des Speichers * Storage Navigator CLI-Pfad: SNM2 CLI-Pfad * Gültige Kontoauthentifizierung: Wählen Sie diese Option, um eine gültige Kontoauthentifizierung auszuwählen * Benutzername: Benutzername für den Speicher * Passwort: Passwort für den Speicher
Wählen Sie Tuning Manager für die Leistung	Andere Leistungsoptionen außer Kraft setzen
Tuning Manager Host	IP-Adresse oder vollqualifizierter Domänenname des Tuning-Managers
Tuning Manager-Port	Für Tuning Manager verwendeter Port
Tuning Manager-Benutzername	Benutzername für Tuning Manager
Tuning Manager-Passwort	Passwort für Tuning Manager

Hinweis: In HDS USP, USP V und VSP kann jede Festplatte zu mehr als einer Array-Gruppe gehören.

Erweiterte Konfiguration

Feld	Beschreibung
Command View-Server-Port	Für den Command View Server verwendeter Port
HTTPs aktiviert	Auswählen, um HTTPs zu aktivieren
Inventarabfrageintervall (min)	Intervall zwischen den Bestandsabfragen. Der Standardwert ist 40.
Wählen Sie „Ausschließen“ oder „Einschließen“, um eine Liste anzugeben	Geben Sie an, ob die unten stehende Array-Liste beim Sammeln von Daten ein- oder ausgeschlossen werden soll.
Geräte ausschließen oder einschließen	Durch Kommas getrennte Liste von Geräte-IDs oder Array-Namen, die ein- oder ausgeschlossen werden sollen
Abfrage-Host-Manager	Auswählen, um den Host-Manager abzufragen
Leistungsabfrageintervall (Sek.)	Intervall zwischen Leistungsabfragen. Der Standardwert ist 300.

Fehlerbehebung

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Inventar

Problem:	Versuchen Sie Folgendes:
Fehler: Der Benutzer verfügt nicht über ausreichende Berechtigungen	Verwenden Sie ein anderes Benutzerkonto mit mehr Berechtigungen oder erhöhen Sie die Berechtigungen des im Datensammler konfigurierten Benutzerkontos

Problem:	Versuchen Sie Folgendes:
Fehler: Die Speicherliste ist leer. Entweder sind die Geräte nicht konfiguriert oder der Benutzer verfügt nicht über ausreichende Berechtigungen	* Verwenden Sie DeviceManager, um zu überprüfen, ob die Geräte konfiguriert sind. * Verwenden Sie ein anderes Benutzerkonto mit mehr Berechtigungen oder erhöhen Sie die Berechtigungen des Benutzerkontos
Fehler: Das HDS-Speicherarray wurde einige Tage lang nicht aktualisiert	Untersuchen Sie, warum dieses Array in HP CommandView AE nicht aktualisiert wird.

Performance

Problem:	Versuchen Sie Folgendes:
Fehler: * Fehler beim Ausführen des Export-Dienstprogramms * Fehler beim Ausführen des externen Befehls	* Bestätigen Sie, dass das Export Utility auf der Data Infrastructure Insights Acquisition Unit installiert ist. * Bestätigen Sie, dass der Speicherort des Export Utility in der Datensammlerkonfiguration korrekt ist. * Bestätigen Sie, dass die IP des USP/R600-Arrays in der Konfiguration des Datensammlers korrekt ist. * Bestätigen Sie, dass Benutzername und Kennwort in der Konfiguration des Datensammlers korrekt sind. * Bestätigen Sie, dass die Version des Export Utility mit der Mikrocodeversion des Speicherarrays kompatibel ist. * Öffnen Sie von der Data Infrastructure Insights Acquisition Unit aus eine CMD-Eingabeaufforderung und führen Sie folgende Schritte aus: - Ändern Sie das Verzeichnis in das konfigurierte Installationsverzeichnis. - Versuchen Sie, eine Verbindung mit dem konfigurierten Speicherarray herzustellen, indem Sie die Batchdatei runWin.bat ausführen.
Fehler: Anmeldung beim Exporttool für Ziel-IP fehlgeschlagen	* Bestätigen Sie, dass Benutzername/Passwort korrekt sind. * Erstellen Sie eine Benutzer-ID hauptsächlich für diesen HDS-Datensammler. * Bestätigen Sie, dass keine anderen Datensammler für die Erfassung dieses Arrays konfiguriert sind.
Fehler: Die Exporttools haben „Zeitbereich für Überwachung konnte nicht abgerufen werden“ protokolliert.	* Bestätigen Sie, dass die Leistungsüberwachung auf dem Array aktiviert ist. * Versuchen Sie, die Exporttools außerhalb von Data Infrastructure Insights aufzurufen, um zu bestätigen, dass das Problem außerhalb von Data Infrastructure Insights liegt.
Fehler: * Konfigurationsfehler: Speicher-Array wird vom Export-Dienstprogramm nicht unterstützt * Konfigurationsfehler: Speicher-Array wird von Storage Navigator Modular CLI nicht unterstützt	* Konfigurieren Sie nur unterstützte Speicher-Arrays. * Verwenden Sie „Geräteliste filtern“, um nicht unterstützte Speicher-Arrays auszuschließen.
Fehler: * Fehler beim Ausführen des externen Befehls * Konfigurationsfehler: Speicherarray nicht vom Inventar gemeldet * Konfigurationsfehler: Exportordner enthält keine JAR-Dateien	* Überprüfen Sie den Speicherort des Export-Dienstprogramms. * Prüfen Sie, ob das betreffende Speicherarray im Command View-Server konfiguriert ist. * Legen Sie das Leistungsabfrageintervall auf ein Vielfaches von 60 Sekunden fest.

Problem:	Versuchen Sie Folgendes:
Fehler: * Fehler Storage Navigator CLI * Fehler beim Ausführen des Auperform-Befehls * Fehler beim Ausführen des externen Befehls	* Bestätigen Sie, dass Storage Navigator Modular CLI auf der Data Infrastructure Insights Acquisition Unit installiert ist. * Bestätigen Sie, dass der Speicherort von Storage Navigator Modular CLI in der Datensammlerkonfiguration korrekt ist. * Bestätigen Sie, dass die IP des WMS/SMS/SMS-Arrays in der Konfiguration des Datensammlers korrekt ist. * Bestätigen Sie, dass die Version von Storage Navigator Modular CLI mit der Mikrocodeversion des im Datensammler konfigurierten Speicherarrays kompatibel ist. * Öffnen Sie von der Data Infrastructure Insights Acquisition Unit aus eine CMD-Eingabeaufforderung und führen Sie folgende Schritte aus: - Ändern Sie das Verzeichnis in das konfigurierte Installationsverzeichnis. - Versuchen Sie, eine Verbindung mit dem konfigurierten Speicherarray herzustellen, indem Sie den folgenden Befehl „auunitref.exe“ ausführen.
Fehler: Konfigurationsfehler: Speicherarray nicht vom Inventar gemeldet	Überprüfen Sie, ob das betreffende Speicherarray im Command View-Server konfiguriert ist
Fehler: * Kein Array ist bei der Storage Navigator Modular 2 CLI registriert * Array ist nicht bei der Storage Navigator Modular 2 CLI registriert * Konfigurationsfehler: Speicher-Array nicht bei der StorageNavigator Modular CLI registriert	* Öffnen Sie die Eingabeaufforderung und wechseln Sie zum konfigurierten Verzeichnis. * Führen Sie den Befehl „set=STONAVM_HOME=“ aus. * Führen Sie den Befehl „auunitref“ aus. * Bestätigen Sie, dass die Befehlsausgabe Details zum Array mit IP enthält. * Wenn die Ausgabe keine Array-Details enthält, registrieren Sie das Array mit der Storage Navigator-CLI: – Öffnen Sie die Eingabeaufforderung und wechseln Sie zum konfigurierten Verzeichnis. – Führen Sie den Befehl „set=STONAVM_HOME=“ aus. – Führen Sie den Befehl „auunitaddauto -ip ${ip}“ aus. Ersetzen Sie ${ip} durch die echte IP

Weitere Informationen finden Sie in der"Support" Seite oder in der"Datensammler-Supportmatrix" .

HPE Alletra 6000 Datenkollektor

Der HP Enterprise Alletra 6000 (früher Nimble) Datensammler unterstützt Inventar- und Leistungsdaten für Alletra 6000-Speicherarrays.

Terminologie

Data Infrastructure Insights erhält von diesem Collector die folgenden Bestandsinformationen. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Anordnung	Storage

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Scheibe	Scheibe
Volumen	Volumen
Pool	Speicherpool
Initiator	Speicherhost-Alias
Regler	Speicherknoten
Fibre-Channel-Schnittstelle	Regler

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Anforderungen

Um Inventar- und Konfigurationsdaten vom Speicherarray zu erfassen, müssen Sie über Folgendes verfügen:

- Das Array muss installiert und konfiguriert sein und vom Client über seinen vollqualifizierten Domänennamen (FQDN) oder die Array-Verwaltungs-IP-Adresse erreichbar sein.
- Auf dem Array muss NimbleOS 2.3.x oder höher ausgeführt werden.
- Sie müssen über einen gültigen Benutzernamen und ein gültiges Kennwort für das Array verfügen und mindestens über die Rolle „Operator“ verfügen. Die Rolle „Gast“ verfügt nicht über ausreichend Zugriff, um die Initiatorkonfigurationen zu verstehen.
- Port 5392 muss auf dem Array geöffnet sein.

Um Leistungsdaten vom Speicherarray zu erfassen, müssen Sie über Folgendes verfügen:

- Auf dem Array muss NimbleOS 4.0.0 oder höher ausgeführt werden.
- Für das Array müssen Volumes konfiguriert sein. Die einzige Performance-API, die NimbleOS hat, ist für Volumes, und alle statistischen Data Infrastructure Insights -Berichte werden aus den Statistiken zu Volumes abgeleitet

Konfiguration

Feld	Beschreibung
Array-Management-IP-Adresse	Vollqualifizierter Domänenname (FQDN) oder IP-Adresse für die Array-Verwaltung.
Benutzername	Benutzername für das Array
Passwort	Passwort für das Array

Erweiterte Konfiguration

Feld	Beschreibung
Hafen	Von der Nimble REST API verwendeter Port. Der Standardwert ist 5392.
Inventarabfrageintervall (min)	Intervall zwischen den Bestandsabfragen. Der Standardwert beträgt 60 Minuten.

Hinweis: Das Standardintervall für die Leistungsabfrage beträgt 300 Sekunden und kann nicht geändert werden. Dies ist das einzige von HPE Alletra 6000 unterstützte Intervall.

Hitachi-Datensysteme

Datensammler der Hitachi Vantara Command Suite

Der Datensammler der Hitachi Vantara Command Suite unterstützt den HiCommand Device Manager-Server. Data Infrastructure Insights kommuniziert mit dem HiCommand Device Manager-Server über die standardmäßige HiCommand-API.

Terminologie

Data Infrastructure Insights erhält die folgenden Bestandsinformationen vom Datensammler der Hitachi Vantara Command Suite. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
PDEV	Scheibe
Zeitschriftenpool	Datenträgergruppe
Speicher-Array	Storage
Port-Controller	Speicherknoten
Array-Gruppe, HDS-Pool	Speicherpool
Logische Einheit, LDEV	Volumen

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Storage

Die folgenden Bedingungen gelten für Objekte oder Referenzen, die Sie möglicherweise auf den Zielseiten von HDS-Speicherressourcen finden. Viele dieser Begriffe gelten auch für andere Datensammler.

- Name – kommt direkt aus dem „Name“-Attribut des HDS HiCommand Device Managers über den GetStorageArray XML-API-Aufruf
- Modell – kommt direkt vom „arrayType“-Attribut des HDS HiCommand Device Manager über den GetStorageArray XML-API-Aufruf
- Anbieter – HDS
- Familie – kommt direkt vom Attribut „arrayFamily“ des HDS HiCommand Device Manager über den GetStorageArray XML-API-Aufruf
- IP – dies ist die Verwaltungs-IP-Adresse des Arrays, keine vollständige Liste aller IP-Adressen auf dem Array
- Rohkapazität – ein Basiswert 2, der die Summe der Gesamtkapazität aller Festplatten in diesem System darstellt, unabhängig von der Festplattenrolle.

Speicherpool

Die folgenden Bedingungen gelten für Objekte oder Referenzen, die Sie möglicherweise auf den Zielseiten der HDS-Speicherpool-Assets finden. Viele dieser Begriffe gelten auch für andere Datensammler.

- Typ: Der Wert hier ist einer der folgenden:
  - RESERVIERT – wenn dieser Pool für andere Zwecke als Datenvolumes vorgesehen ist, z. B. Journaling, Snapshots
  - Thin Provisioning – wenn es sich um einen HDP-Pool handelt
  - Raid-Gruppe – diese werden Sie aus mehreren Gründen wahrscheinlich nicht sehen:

    Data Infrastructure Insights vertritt die strikte Haltung, eine doppelte Zählkapazität um jeden Preis zu vermeiden. Auf HDS muss man normalerweise RAID-Gruppen aus Festplatten erstellen, Pool-Volumes auf diesen RAID-Gruppen erstellen und Pools (oft HDP, können aber auch Spezialzwecken dienen) aus diesen Pool-Volumes erstellen. Wenn Data Infrastructure Insights sowohl die zugrunde liegenden RAID-Gruppen als auch die Pools unverändert melden würde, würde die Summe ihrer Rohkapazität die Summe der Festplatten bei weitem übersteigen.

  Stattdessen verkleinert der HDS Command Suite-Datensammler von Data Infrastructure Insights die Größe von RAID-Gruppen willkürlich um die Kapazität von Pool-Volumes. Dies kann dazu führen, dass Data Infrastructure Insights die Raid-Gruppe überhaupt nicht meldet. Darüber hinaus werden alle resultierenden Raid-Gruppen so gekennzeichnet, dass sie in der Data Infrastructure Insights WebUI nicht sichtbar sind, aber in das Data Infrastructure Insights Data Warehouse (DWH) fließen. Der Zweck dieser Entscheidungen besteht darin, eine überladene Benutzeroberfläche für Dinge zu vermeiden, die für die meisten Benutzer unwichtig sind. Wenn Ihr HDS-Array über RAID-Gruppen mit 50 MB freiem Speicherplatz verfügt, können Sie diesen freien Speicherplatz wahrscheinlich nicht sinnvoll nutzen.

- Knoten – N/A, da HDS-Pools nicht an einen bestimmten Knoten gebunden sind
- Redundanz – die RAID-Ebene des Pools. Möglicherweise mehrere Werte für einen HDP-Pool, der aus mehreren RAID-Typen besteht
- Kapazität % – der Prozentsatz, der vom Pool für die Datennutzung verwendet wird, mit den verwendeten GB und der gesamten logischen GB-Größe des Pools
- Überbelegte Kapazität – ein abgeleiteter Wert, der besagt, dass „die logische Kapazität dieses Pools um diesen Prozentsatz überbelegt ist, da die Summe der logischen Volumes die logische Kapazität des Pools um diesen Prozentsatz übersteigt“.
- Snapshot – zeigt die für die Snapshot-Nutzung in diesem Pool reservierte Kapazität an

Speicherknoten

Die folgenden Bedingungen gelten für Objekte oder Referenzen, die Sie möglicherweise auf den Zielseiten der HDS-Speicherknoten-Assets finden. Viele dieser Begriffe gelten auch für andere Datensammler.

- Name – Der Name des Front-End-Directors (FED) oder Kanaladapters auf monolithischen Arrays oder der Name des Controllers auf einem modularen Array. Ein bestimmtes HDS-Array verfügt über 2 oder mehr Speicherknoten
- Volumes – Die Volume-Tabelle zeigt alle Volumes an, die einem Port zugeordnet sind, der diesem Speicherknoten gehört.

Inventaranforderungen

Um Bestandsdaten erfassen zu können, benötigen Sie Folgendes:

- IP-Adresse des HiCommand Device Manager-Servers
- Nur-Lese-Benutzername und Passwort für die HiCommand Device Manager-Software und Peer-Berechtigungen
- Portanforderungen: 2001 (http) oder 2443 (https)
- Melden Sie sich mit Benutzername und Passwort bei der HiCommand Device Manager-Software an
- Überprüfen Sie den Zugriff auf HiCommand Device Manager http://<HiCommand_Device_Manager_IP>:2001/service/StorageManager

Leistungsanforderungen

Um Leistungsdaten erfassen zu können, müssen folgende Voraussetzungen erfüllt sein:

- HDS USP-, USP V- und VSP-Leistung
  - Performance Monitor muss lizenziert sein.
  - Der Überwachungsschalter muss aktiviert sein.
  - Das Exporttool (Export.exe) muss in die Data Infrastructure Insights AU kopiert werden.
  - Die Version des Exporttools muss mit der Mikrocodeversion des Zielarrays übereinstimmen.
- AMS-Leistung:
  - NetApp empfiehlt dringend, auf AMS-Arrays ein dediziertes Servicekonto für Data Infrastructure Insights zu erstellen, um Leistungsdaten abzurufen. Storage Navigator erlaubt einem Benutzerkonto nur eine gleichzeitige Anmeldung beim Array. Wenn Data Infrastructure Insights dasselbe Benutzerkonto wie Verwaltungsskripte oder HiCommand verwendet, kann dies dazu führen, dass Data Infrastructure Insights, Verwaltungsskripte oder HiCommand aufgrund der Beschränkung auf ein gleichzeitiges Benutzerkonto nicht mit dem Array kommunizieren können.
  - Performance Monitor muss lizenziert sein.
  - Das CLI-Dienstprogramm Storage Navigator Modular 2 (SNM2) muss auf der Data Infrastructure Insights AU installiert werden.

Konfiguration

Feld	Beschreibung
HiCommand Server	IP-Adresse oder vollqualifizierter Domänenname des HiCommand Device Manager-Servers
Benutzername	Benutzername für den HiCommand Device Manager-Server.
Passwort	Für den HiCommand Device Manager-Server verwendetes Passwort.
Geräte - VSP G1000 (R800), VSP (R700), HUS VM (HM700) und USP-Speicher	Geräteliste für VSP G1000 (R800), VSP (R700), HUS VM (HM700) und USP-Speicher. Jeder Speicher benötigt: * Array-IP: IP-Adresse des Speichers * Benutzername: Benutzername für den Speicher * Passwort: Passwort für den Speicher * Ordner mit den JAR-Dateien des Export-Dienstprogramms

Feld	Beschreibung
SNM2Devices – WMS/SMS/AMS-Speicher	Geräteliste für WMS/SMS/AMS-Speicher. Jeder Speicher benötigt: * Array-IP: IP-Adresse des Speichers * Storage Navigator CLI-Pfad: SNM2 CLI-Pfad * Gültige Kontoauthentifizierung: Wählen Sie diese Option, um eine gültige Kontoauthentifizierung auszuwählen * Benutzername: Benutzername für den Speicher * Passwort: Passwort für den Speicher
Wählen Sie Tuning Manager für die Leistung	Andere Leistungsoptionen außer Kraft setzen
Tuning Manager Host	IP-Adresse oder vollqualifizierter Domänenname des Tuning-Managers
Tuning Manager-Port überschreiben	Wenn leer, verwenden Sie den Standardport im Feld „Tuning Manager für Leistung auswählen“, andernfalls geben Sie den zu verwendenden Port ein.
Tuning Manager-Benutzername	Benutzername für Tuning Manager
Tuning Manager-Passwort	Passwort für Tuning Manager

Hinweis: In HDS USP, USP V und VSP kann jede Festplatte zu mehr als einer Array-Gruppe gehören.

Erweiterte Konfiguration

Feld	Beschreibung
Verbindungstyp	HTTPS oder HTTP, zeigt auch den Standardport an
HiCommand-Server-Port	Für den HiCommand Device Manager verwendeter Port
Inventarabfrageintervall (min)	Intervall zwischen den Bestandsabfragen. Der Standardwert ist 40.
Wählen Sie „Ausschließen“ oder „Einschließen“, um eine Liste anzugeben	Geben Sie an, ob die unten stehende Array-Liste beim Sammeln von Daten ein- oder ausgeschlossen werden soll.
Geräteliste filtern	Durch Kommas getrennte Liste der Geräteseriennummern, die ein- oder ausgeschlossen werden sollen
Leistungsabfrageintervall (Sek.)	Intervall zwischen Leistungsabfragen. Der Standardwert ist 300.
Export-Timeout in Sekunden	Zeitüberschreitung beim Export-Dienstprogramm. Der Standardwert ist 300.

Fehlerbehebung

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Inventar

Problem:	Versuchen Sie Folgendes:
Fehler: Der Benutzer verfügt nicht über ausreichende Berechtigungen	Verwenden Sie ein anderes Benutzerkonto mit mehr Berechtigungen oder erhöhen Sie die Berechtigungen des im Datensammler konfigurierten Benutzerkontos
Fehler: Die Speicherliste ist leer. Entweder sind die Geräte nicht konfiguriert oder der Benutzer verfügt nicht über ausreichende Berechtigungen	* Verwenden Sie DeviceManager, um zu überprüfen, ob die Geräte konfiguriert sind. * Verwenden Sie ein anderes Benutzerkonto mit mehr Berechtigungen oder erhöhen Sie die Berechtigungen des Benutzerkontos
Fehler: Das HDS-Speicherarray wurde einige Tage lang nicht aktualisiert	Untersuchen Sie, warum dieses Array in HDS HiCommand nicht aktualisiert wird.

Performance

Problem:	Versuchen Sie Folgendes:
Fehler: * Fehler beim Ausführen des Export-Dienstprogramms * Fehler beim Ausführen des externen Befehls	* Bestätigen Sie, dass das Export Utility auf der Data Infrastructure Insights Acquisition Unit installiert ist. * Bestätigen Sie, dass der Speicherort des Export Utility in der Datensammlerkonfiguration korrekt ist. * Bestätigen Sie, dass die IP des USP/R600-Arrays in der Konfiguration des Datensammlers korrekt ist. * Bestätigen Sie, dass Benutzername und Kennwort in der Konfiguration des Datensammlers korrekt sind. * Bestätigen Sie, dass die Version des Export Utility mit der Mikrocodeversion des Speicherarrays kompatibel ist. * Öffnen Sie von der Data Infrastructure Insights Acquisition Unit aus eine CMD-Eingabeaufforderung und führen Sie folgende Schritte aus: - Ändern Sie das Verzeichnis in das konfigurierte Installationsverzeichnis. - Versuchen Sie, eine Verbindung mit dem konfigurierten Speicherarray herzustellen, indem Sie die Batchdatei runWin.bat ausführen.
Fehler: Anmeldung beim Exporttool für Ziel-IP fehlgeschlagen	* Bestätigen Sie, dass Benutzername/Passwort korrekt sind. * Erstellen Sie eine Benutzer-ID hauptsächlich für diesen HDS-Datensammler. * Bestätigen Sie, dass keine anderen Datensammler für die Erfassung dieses Arrays konfiguriert sind.
Fehler: Die Exporttools haben „Zeitbereich für Überwachung konnte nicht abgerufen werden“ protokolliert.	* Bestätigen Sie, dass die Leistungsüberwachung auf dem Array aktiviert ist. * Versuchen Sie, die Exporttools außerhalb von Data Infrastructure Insights aufzurufen, um zu bestätigen, dass das Problem außerhalb von Data Infrastructure Insights liegt.
Fehler: * Konfigurationsfehler: Speicher-Array wird vom Export-Dienstprogramm nicht unterstützt * Konfigurationsfehler: Speicher-Array wird von Storage Navigator Modular CLI nicht unterstützt	* Konfigurieren Sie nur unterstützte Speicher-Arrays. * Verwenden Sie „Geräteliste filtern“, um nicht unterstützte Speicher-Arrays auszuschließen.

Problem:	Versuchen Sie Folgendes:
Fehler: * Fehler beim Ausführen des externen Befehls * Konfigurationsfehler: Speicherarray nicht vom Inventar gemeldet * Konfigurationsfehler: Exportordner enthält keine JAR-Dateien	* Überprüfen Sie den Speicherort des Export-Dienstprogramms. * Prüfen Sie, ob das betreffende Speicherarray im HiCommand-Server konfiguriert ist. * Legen Sie das Leistungsabfrageintervall auf ein Vielfaches von 60 Sekunden fest.
Fehler: * Fehler Storage Navigator CLI * Fehler beim Ausführen des Auperform-Befehls * Fehler beim Ausführen des externen Befehls	* Bestätigen Sie, dass Storage Navigator Modular CLI auf der Data Infrastructure Insights Acquisition Unit installiert ist. * Bestätigen Sie, dass der Speicherort von Storage Navigator Modular CLI in der Datensammlerkonfiguration korrekt ist. * Bestätigen Sie, dass die IP des WMS/SMS/SMS-Arrays in der Konfiguration des Datensammlers korrekt ist. * Bestätigen Sie, dass die Version von Storage Navigator Modular CLI mit der Mikrocodeversion des im Datensammler konfigurierten Speicherarrays kompatibel ist. * Öffnen Sie von der Data Infrastructure Insights Acquisition Unit aus eine CMD-Eingabeaufforderung und führen Sie folgende Schritte aus: - Ändern Sie das Verzeichnis in das konfigurierte Installationsverzeichnis. - Versuchen Sie, eine Verbindung mit dem konfigurierten Speicherarray herzustellen, indem Sie den folgenden Befehl „auunitref.exe“ ausführen.
Fehler: Konfigurationsfehler: Speicherarray nicht vom Inventar gemeldet	Überprüfen Sie, ob das betreffende Speicherarray im HiCommand-Server konfiguriert ist
Fehler: * Kein Array ist bei der Storage Navigator Modular 2 CLI registriert * Array ist nicht bei der Storage Navigator Modular 2 CLI registriert * Konfigurationsfehler: Speicher-Array nicht bei der StorageNavigator Modular CLI registriert	* Öffnen Sie die Eingabeaufforderung und wechseln Sie zum konfigurierten Verzeichnis. * Führen Sie den Befehl „set=STONAVM_HOME=“ aus. * Führen Sie den Befehl „auunitref“ aus. * Bestätigen Sie, dass die Befehlsausgabe Details zum Array mit IP enthält. * Wenn die Ausgabe keine Array-Details enthält, registrieren Sie das Array mit der Storage Navigator-CLI: – Öffnen Sie die Eingabeaufforderung und wechseln Sie zum konfigurierten Verzeichnis. – Führen Sie den Befehl „set=STONAVM_HOME=“ aus. - Führen Sie den Befehl „auunitaddauto -ip <ip>“ aus. Ersetzen Sie <ip> durch die richtige IP.

Weitere Informationen finden Sie in der"Support" Seite oder in der"Datensammler-Supportmatrix" .

Konfigurieren des Hitachi Vantara NAS-Datenkollektors

Der Hitachi Vantara NAS-Datensammler ist ein Inventar- und Konfigurationsdatensammler, der die Erkennung von HDS NAS-Clustern unterstützt. Data Infrastructure Insights unterstützt die Erkennung von NFS- und CIFS-Freigaben, Dateisystemen (internen Volumes) und Spans (Speicherpools).

Terminologie

Data Infrastructure Insights erhält die folgenden Bestandsinformationen vom HNAS-Datensammler. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Stufe	Datenträgergruppe
Cluster	Storage
Node	Speicherknoten
Spanne	Speicherpool
Systemlaufwerk	Backend-Lun
Dateisystem	Internes Volumen

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Anforderungen

- IP-Adresse des Geräts
- Port 22, SSH-Protokoll
- Benutzername und Passwort – Berechtigungsstufe: Supervisor
- Hinweis: Dieser Datensammler ist SSH-basiert, daher muss die AU, die ihn hostet, in der Lage sein, SSH-Sitzungen zu TCP 22 auf dem HNAS selbst oder der Systems Management Unit (SMU), mit der der Cluster verbunden ist, zu initiieren.

Konfiguration

Feld	Beschreibung
HNAS-Host	IP-Adresse oder vollqualifizierter Domänenname des HNAS-Verwaltungshosts
Benutzername	Benutzername für HNAS CLI
Passwort	Für HNAS CLI verwendetes Passwort

Erweiterte Konfiguration

Feld	Beschreibung
Inventarabfrageintervall (min)	Intervall zwischen den Bestandsabfragen. Der Standardwert beträgt 30 Minuten.

Fehlerbehebung

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Inventar

Problem:	Versuchen Sie Folgendes:
„Fehler beim Verbinden“ mit den Fehlermeldungen „Fehler beim Einrichten des Shell-Kanals:“ oder „Fehler beim Öffnen des Shell-Kanals“	Wird wahrscheinlich durch Probleme mit der Netzwerkverbindung oder eine falsche SSH-Konfiguration verursacht. Bestätigen Sie die Verbindung mit einem alternativen SSH-Client
„Timeout“ oder „Fehler beim Abrufen der Daten“ mit der Fehlermeldung „Befehl: XXX hat eine Zeitüberschreitung.“	* Versuchen Sie den Befehl mit einem anderen SSH-Client. * Erhöhen Sie das Timeout.
„Fehler beim Verbinden“ oder „Ungültige Anmeldeinformationen“ mit der Fehlermeldung „Konnte nicht mit dem Gerät kommunizieren:“	* IP-Adresse prüfen * Benutzernamen und Passwort prüfen * Verbindung mit alternativem SSH-Client bestätigen

Weitere Informationen finden Sie in der"Support" Seite oder in der"Datensammler-Supportmatrix" .

Hitachi Ops Center-Datensammler

Dieser Datensammler verwendet die integrierte Anwendungssuite von Hitachi Ops Center, um auf Inventar- und Leistungsdaten mehrerer Speichergeräte zuzugreifen. Zur Inventar- und Kapazitätsermittlung muss Ihre Ops Center-Installation sowohl die Komponenten „Common Services“ als auch „Administrator“ enthalten. Für die Leistungserfassung müssen Sie zusätzlich „Analyzer“ bereitgestellt haben.

Terminologie

Data Infrastructure Insights erhält von diesem Datensammler die folgenden Bestandsinformationen. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Speichersysteme	Storage
Volumen	Volumen
Paritätsgruppen	Speicherpool (RAID), Datenträgergruppen
Scheibe	Scheibe
Speicherpool	Speicherpool (Thin, SNAP)
Externe Paritätsgruppen	Speicherpool (Backend), Datenträgergruppen
Hafen	Speicherknoten → Controllerknoten → Port
Hostgruppen	Volumenzuordnung und -maskierung
Volumenpaare	Speichersynchronisierung

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Inventaranforderungen

Um Bestandsdaten erfassen zu können, benötigen Sie Folgendes:

- IP-Adresse oder Hostname des Ops Center-Servers, auf dem die Komponente „Common Services“ gehostet wird
- Root-/Sysadmin-Benutzerkonto und -Passwort, die auf allen Servern vorhanden sind, auf denen Ops Center-Komponenten gehostet werden. HDS hat die REST-API-Unterstützung für die Verwendung durch LDAP/SSO-Benutzer erst ab Ops Center 10.8 implementiert.

Leistungsanforderungen

Um Leistungsdaten erfassen zu können, müssen folgende Voraussetzungen erfüllt sein:

Das HDS Ops Center „Analyzer“-Modul muss installiert sein. Speicher-Arrays müssen das Ops Center „Analyzer“-Modul versorgen.

Konfiguration

Feld	Beschreibung
IP-Adresse des Hitachi Ops Center	IP-Adresse oder vollqualifizierter Domänenname des Ops Center-Servers, auf dem die Komponente „Common Services“ gehostet wird
Benutzername	Benutzername für den Ops Center-Server.
Passwort	Für den Ops Center-Server verwendetes Kennwort.

Erweiterte Konfiguration

Feld	Beschreibung
Verbindungstyp	HTTPS (Port 443) ist die Standardeinstellung
TCP-Port überschreiben	Geben Sie den zu verwendenden Port an, wenn dieser nicht der Standardport ist.
Inventarabfrageintervall (min)	Intervall zwischen den Bestandsabfragen. Der Standardwert ist 40.
Wählen Sie „Ausschließen“ oder „Einschließen“, um eine Liste anzugeben	Geben Sie an, ob die unten stehende Array-Liste beim Sammeln von Daten ein- oder ausgeschlossen werden soll.
Geräteliste filtern	Durch Kommas getrennte Liste der Geräteseriennummern, die ein- oder ausgeschlossen werden sollen
Leistungsabfrageintervall (Sek.)	Intervall zwischen Leistungsabfragen. Der Standardwert ist 300.

Weitere Informationen finden Sie in der"Support" Seite oder in der"Datensammler-Supportmatrix" .

Infinidat InfiniBox Datensammler

Der Infinidat InfiniBox (HTTP)-Datensammler wird zum Sammeln von

Bestandsinformationen vom Infinidat InfiniBox-Speichersystem verwendet.

Terminologie

Data Infrastructure Insights erhält die folgenden Bestandsinformationen vom Infinidat InfiniBox-Datensammler. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Speicherpool	Speicherpool
Node	Regler
Dateisystem	Internes Volumen
Dateisystem	Dateifreigabe
Dateisystemexporte	Aktie

Anforderungen

Im Folgenden sind die Anforderungen für die Konfiguration dieses Datensammlers aufgeführt.

- IP-Adresse oder FQDN des InfiniBox-Verwaltungsknotens
- Administrator-Benutzer-ID und -Passwort
- Port 443 über REST-API

Konfiguration

Feld	Beschreibung
InfiniBox-Host	IP-Adresse oder vollqualifizierter Domänenname des InfiniBox-Verwaltungsknotens
Benutzername	Benutzername für den InfiniBox-Verwaltungsknoten
Passwort	Passwort für den InfiniBox-Verwaltungsknoten

Erweiterte Konfiguration

Feld	Beschreibung
TCP-Port	TCP-Port, der für die Verbindung mit dem InfiniBox-Server verwendet wird. Der Standardwert ist 443.
Inventarabfrageintervall	Intervall zwischen den Bestandsabfragen. Der Standardwert beträgt 60 Minuten.

Fehlerbehebung

Weitere Informationen zu diesem Datensammler finden Sie im"Support" Seite oder in der"Datensammler-Supportmatrix" .

Huawei OceanStor Datensammler

Data Infrastructure Insights verwendet den Huawei OceanStor (REST/HTTPS)-Datensammler, um Inventar und Leistung für Huawei OceanStor- und OceanStor Dorado-Speicher zu ermitteln.

Terminologie

Data Infrastructure Insights erhält die folgenden Bestands- und Leistungsinformationen vom Huawei OceanStor. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Speicherpool	Speicherpool
Dateisystem	Internes Volumen
Regler	Speicherknoten
FC-Port (zugeordnet)	Volumenkarte
Host-FC-Initiator (zugeordnet)	Volumenmaske
NFS/CIFS-Freigabe	Aktie
iSCSI-Link-Ziel	iSCSI-Zielknoten
iSCSI-Link-Initiator	iSCSI-Initiatorknoten
Scheibe	Scheibe
LUN	Volumen

Anforderungen

Zum Konfigurieren dieses Datensammlers sind die folgenden Voraussetzungen erforderlich:

- IP-Adresse des Geräts
- Anmeldeinformationen für den Zugriff auf den OceanStor-Gerätemanager
- Port 8088 muss verfügbar sein

Konfiguration

Feld	Beschreibung
OceanStor-Host-IP-Adresse	IP-Adresse oder vollqualifizierter Domänenname des OceanStor Device Managers
Benutzername	Name, der für die Anmeldung beim OceanStor Device Manager verwendet wird
Passwort	Passwort zur Anmeldung beim OceanStor Device Manager

Erweiterte Konfiguration

Feld	Beschreibung
TCP-Port	TCP-Port, der für die Verbindung mit dem OceanStor Device Manager verwendet wird. Der Standardwert ist 8088.
Inventarabfrageintervall (min)	Intervall zwischen den Bestandsabfragen. Der Standardwert beträgt 60 Minuten.
Leistungsabfrageintervall (Sek.).	Der Standardwert beträgt 300 Sekunden.

Fehlerbehebung

Weitere Informationen zu diesem Datensammler finden Sie im"Support" Seite oder in der"Datensammler-Supportmatrix" .

IBM

IBM Cleversafe-Datenkollektor

Data Infrastructure Insights verwendet diesen Datenkollektor, um Bestands- und Leistungsdaten für IBM Cleversafe-Speichersysteme zu ermitteln.

Für IBM Cleversafe gilt ein anderer Tarif als für verwaltete Einheiten (Raw TB). Für jeweils 40 TB unformatierte IBM Cleversafe-Kapazität wird 1"Verwaltete Einheit (MU)" .

Terminologie

Data Infrastructure Insights erhält die folgenden Bestandsinformationen vom IBM Cleversafe-Datenkollektor. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Speicherpool	Speicherpool
Container	Internes Volumen
Container	Dateifreigabe
NFS-Freigabe	Aktie

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Anforderungen

- Die IP-Adresse der externen Datendienste für den Cluster
- Administrator-Benutzername und -Passwort
- Port 9440

Konfiguration

Feld	Beschreibung
Manager-IP oder Hostname	IP-Adresse oder Hostname des Verwaltungsknotens
Benutzername	Benutzername für das Benutzerkonto mit Superuser- oder Systemadministratorrolle
Passwort	Kennwort für das Benutzerkonto mit der Rolle „Superuser“ oder „Systemadministrator“

Erweiterte Konfiguration

Feld	Beschreibung
Inventarabfrageintervall (min)	Intervall zwischen den Bestandsabfragen.
HTTP-Verbindungs-Timeout (Sek.)	HTTP-Timeout in Sekunden.

Fehlerbehebung

Weitere Informationen zu diesem Datensammler finden Sie im"Support" Seite oder in der"Datensammler-Supportmatrix" .

IBM CS-Datenkollektor

Data Infrastructure Insights verwendet diesen Datensammler, um Bestands- und Leistungsdaten für IBM CS-Speichersysteme zu ermitteln.

Terminologie

Data Infrastructure Insights erhält die folgenden Bestandsinformationen vom IBM CS-Datenkollektor. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Speicherpool	Speicherpool
Container	Internes Volumen
Container	Dateifreigabe
NFS-Freigabe	Aktie

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Anforderungen

- Die IP-Adresse der externen Datendienste für den Cluster
- Administrator-Benutzername und -Passwort
- Port 9440

Konfiguration

Feld	Beschreibung
Externe Prism-IP-Adresse	Die IP-Adresse der externen Datendienste für den Cluster
Benutzername	Benutzername für das Admin-Konto
Passwort	Passwort für das Admin-Konto

Erweiterte Konfiguration

Feld	Beschreibung
TCP-Port	TCP-Port, der für die Verbindung mit dem IBM CS-Array verwendet wird. Der Standardwert ist 9440.
Inventarabfrageintervall (min)	Intervall zwischen den Bestandsabfragen. Der Standardwert beträgt 60 Minuten.
Leistungsabfrageintervall (Sek.)	Intervall zwischen Leistungsabfragen. Der Standardwert beträgt 300 Sekunden.

Fehlerbehebung

Weitere Informationen zu diesem Datensammler finden Sie im"Support" Seite oder in der"Datensammler-Supportmatrix" .

Datenkollektor der IBM System Storage DS8000-Serie

Der IBM DS (CLI)-Datenkollektor unterstützt die Erfassung von Inventar- und Leistungsdaten für DS6xxx- und DS8xxx-Geräte.

DS3xxx-, DS4xxx- und DS5xxx-Geräte werden unterstützt von"NetApp E-Series Datenkollektor" . Informationen zu unterstützten Modellen und Firmware-Versionen finden Sie in der Supportmatrix von Data Infrastructure Insights .

Terminologie

Data Infrastructure Insights erhält die folgenden Bestandsinformationen vom IBM DS-Datenkollektor. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Festplattenmodul	Scheibe
Speicherimage	Storage
Extent-Pool	Speicherknoten
Festes Blockvolumen	Volumen
Host-FC-Initiator (zugeordnet)	Volumenmaske

Hinweis: Dies sind nur allgemeine Terminologiezuordnungen und stellen möglicherweise nicht jeden Fall für

diesen Datensammler dar.

Anforderungen

Zur Konfiguration dieses Datensammlers benötigen Sie Folgendes:

- IP-Adresse jedes DS-Arrays
- Nur-Lese-Benutzername und Passwort auf jedem DS-Array
- Auf der Data Infrastructure Insights AU installierte Drittanbietersoftware: IBM *dscli*
- Zugriffsvalidierung: Führen Sie *dscli*-Befehle mit dem Benutzernamen und dem Kennwort aus
- Portanforderungen: 80, 443 und 1750

Konfiguration

Feld	Beschreibung
DS-Speicher	IP-Adresse oder vollqualifizierter Domänenname des DS-Geräts
Benutzername	Benutzername für die DS CLI
Passwort	Passwort für die DS CLI
dscli ausführbarer Pfad	Vollständiger Pfad zur ausführbaren Datei *dscli*

Erweiterte Konfiguration

Feld	Beschreibung
Inventarabfrageintervall (min)	Intervall zwischen Bestandsabfragen (min). Der Standardwert ist 40.
Speicheranzeigename	Name des IBM DS-Speicherarrays
Aus dem Inventar ausgeschlossene Geräte	Durch Kommas getrennte Liste der Geräteseriennummern, die von der Inventarerfassung ausgeschlossen werden sollen
Leistungsabfrageintervall (Sek.)	Der Standardwert ist 300.
Leistungsfiltertyp	Einschließen: Nur von Geräten auf der Liste erfasste Daten. Ausschließen: Von diesen Geräten werden keine Daten erfasst
Leistungsfilter-Geräteliste	Durch Kommas getrennte Liste von Geräte-IDs, die in die Leistungserfassung einbezogen oder davon ausgeschlossen werden sollen

Fehlerbehebung

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Inventar

Problem:	Versuchen Sie Folgendes:
Fehler mit: CMUC00192E, CMUC00191E oder CMUC00190E	* Überprüfen Sie die eingegebenen Anmeldeinformationen und die IP-Adresse. * Versuchen Sie, über die Webverwaltungskonsole https://<ip>:8452/DS8000/Console mit dem Array zu kommunizieren. Ersetzen Sie <ip> durch die für den Datensammler konfigurierte IP.
Fehler: * Programm kann nicht ausgeführt werden * Fehler beim Ausführen des Befehls	* Öffnen Sie von der Data Infrastructure Insights Acquisition Unit aus ein CMD. * Öffnen Sie die Datei CLI.CFG im Stammverzeichnis/der Bibliothek der CLI und überprüfen Sie die Eigenschaft JAVA_INSTALL. Bearbeiten Sie den Wert, damit er Ihrer Umgebung entspricht. * Zeigen Sie die auf diesem Computer installierte Java-Version an, indem Sie „java -version“ eingeben. * Pingen Sie die IP-Adresse des IBM-Speichergeräts an, das im ausgegebenen CLI-Befehl angegeben ist. * Wenn alles oben genannte gut funktioniert hat, führen Sie manuell einen CLI-Befehl aus

Weitere Informationen finden Sie in der"Support" Seite oder in der"Datensammler-Supportmatrix" .

Konfigurieren des IBM PowerVM-Datenkollektors

Der IBM PowerVM (SSH)-Datenkollektor wird zum Sammeln von Informationen über virtuelle Partitionen verwendet, die auf IBM POWER-Hardwareinstanzen ausgeführt werden, die von einer Hardware Management Console (HMC) verwaltet werden.

Terminologie

Data Infrastructure Insights erfasst Bestandsinformationen von den virtuellen Partitionen, die auf IBM POWER-Hardwareinstanzen ausgeführt werden. Für jeden erworbenen Vermögenswerttyp wird die am häufigsten verwendete Terminologie für den Vermögenswert angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Festplatte	Virtuelle Festplatte
Verwaltetes System	Gastgeber
LPAR, VIO-Server	Virtuelle Maschine
Volumengruppe	Datenspeicher
Physisches Volumen	LUN

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Anforderungen

Zur Konfiguration und Nutzung dieses Datensammlers müssen folgende Voraussetzungen erfüllt sein:

- IP-Adresse der Hardware Management Console (HMC)
- Benutzername und Kennwort, die den Zugriff auf die Hardware Management Console (HMC) über SSH ermöglichen
- Portanforderung SSH-22
- Anzeigeberechtigung für alle Verwaltungssysteme und Sicherheitsdomänen logischer Partitionen

  Der Benutzer muss außerdem über die Berechtigung zum Anzeigen von HMC-Konfigurationen und zum Sammeln von VPD-Informationen für die Sicherheitsgruppierung der HMC-Konsole verfügen. Dem Benutzer muss außerdem der Zugriff auf Virtual IO Server Commands unter der Sicherheitsgruppierung „Logische Partition“ gestattet sein. Es empfiehlt sich, mit der Rolle eines Operators zu beginnen und dann alle Rollen zu entfernen. Nur-Lese-Benutzer auf der HMC haben keine Berechtigung zum Ausführen von Proxy-Befehlen auf AIX-Hosts.

- Die bewährte Vorgehensweise von IBM besteht darin, die Geräte von zwei oder mehr HMCs überwachen zu lassen. Beachten Sie, dass dies dazu führen kann, dass OnCommand Insight doppelte Geräte meldet. Daher wird dringend empfohlen, redundante Geräte zur Liste „Geräte ausschließen“ in der erweiterten Konfiguration für diesen Datensammler hinzuzufügen.

Konfiguration

Feld	Beschreibung
IP-Adresse der Hardware Management Console (HMC)	IP-Adresse oder vollqualifizierter Domänenname der PowerVM Hardware Management Console
HMC-Benutzer	Benutzername für die Hardware Management Console
Passwort	Für die Hardware Management Console verwendetes Kennwort

Erweiterte Konfiguration

Feld	Beschreibung
Inventarabfrageintervall (min)	Intervall zwischen den Bestandsabfragen. Der Standardwert beträgt 20 Minuten.
SSH-Port	Für SSH zur PowerVM verwendeter Port
Passwort	Für die Hardware Management Console verwendetes Kennwort
Anzahl der Wiederholungsversuche	Anzahl der Inventarisierungswiederholungsversuche
Geräte ausschließen	Durch Kommas getrennte Liste der auszuschließenden Geräte-IDs oder Anzeigenamen

Fehlerbehebung

Weitere Informationen zu diesem Datensammler finden Sie im"Support" Seite oder in der"Datensammler-Supportmatrix" .

Konfigurieren des IBM SAN Volume Controller-Datenkollektors

Der IBM SAN Volume Controller (SVC)-Datenkollektor sammelt Inventar- und Leistungsdaten mithilfe von SSH und unterstützt eine Vielzahl von Geräten, auf denen das SVC-Betriebssystem ausgeführt wird.

Die Liste der unterstützten Geräte umfasst Modelle wie SVC, v7000, v5000 und v3700. Informationen zu unterstützten Modellen und Firmware-Versionen finden Sie in der Data Infrastructure Insights Supportmatrix.

Terminologie

Data Infrastructure Insights erhält die folgenden Bestandsinformationen vom IBM SVC-Datenkollektor. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Fahren	Scheibe
Cluster	Storage
Node	Speicherknoten
Mdisk-Gruppe	Speicherpool
Vdisk	Volumen
MDisk	Backend-LUNs und -Pfade

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Inventaranforderungen

- IP-Adresse jedes SVC-Clusters
- Port 22 verfügbar
- Benutzername und Kennwort nur zum Lesen

Leistungsanforderungen

- SVC-Konsole, die für jeden SVC-Cluster obligatorisch und für das SVC Discovery Foundation-Paket erforderlich ist.
- Für die Anmeldeinformationen ist nur zum Kopieren von Leistungsdateien von Clusterknoten auf den Konfigurationsknoten eine Administratorzugriffsebene erforderlich.
- Aktivieren Sie die Datenerfassung, indem Sie per SSH eine Verbindung zum SVC-Cluster herstellen und Folgendes ausführen: *svctask startstats -interval 1*

  Hinweis: Alternativ können Sie die Datenerfassung über die SVC-Verwaltungsbenutzeroberfläche aktivieren.

Konfiguration

Feld	Beschreibung
Cluster-IP-Adressen	IP-Adressen oder vollqualifizierte Domänennamen des SVC-Speichers
Inventar-Benutzername	Benutzername für die SVC-CLI
Inventarkennwort	Passwort für die SVC-CLI

Erweiterte Konfiguration

Feld	Beschreibung
Inventarabfrageintervall (min)	Intervall zwischen den Bestandsabfragen. Der Standardwert beträgt 40 Minuten.
Leistungsabfrageintervall (Sek.)	Intervall zwischen Leistungsabfragen. Der Standardwert beträgt 300 Sekunden.
So bereinigen Sie gedumpte Statistikdateien	Aktivieren Sie dieses Kontrollkästchen, um die gespeicherten Statistikdateien zu bereinigen.

Fehlerbehebung

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Problem:	Versuchen Sie Folgendes:
Fehler: „Der Befehl kann nicht initiiert werden, da er nicht auf dem Konfigurationsknoten ausgeführt wurde.“	Der Befehl muss auf dem Konfigurationsknoten ausgeführt werden.

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Problem:	Versuchen Sie Folgendes:
Fehler: „Der Befehl kann nicht initiiert werden, da er nicht auf dem Konfigurationsknoten ausgeführt wurde.“	Der Befehl muss auf dem Konfigurationsknoten ausgeführt werden.

Weitere Informationen zu diesem Datensammler finden Sie im"Support" Seite oder in der"Datensammler-Supportmatrix" .

Konfigurieren des IBM XIV/A9000-Datenkollektors

Der IBM XIV- und A9000-Datenkollektor (CLI) verwendet die XIV-Befehlszeilenschnittstelle zum Erfassen von Inventardaten, während die Leistungserfassung durch SMI-S-Aufrufe an das XIV/A9000-Array erfolgt, auf dem ein SMI-S-Anbieter auf Port 7778 ausgeführt wird.

Terminologie

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Scheibe	Scheibe

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Speichersystem	Storage
Speicherpool	Speicherpool
Volumen	Volumen

Anforderungen

Zur Konfiguration und Nutzung dieses Datensammlers müssen folgende Voraussetzungen erfüllt sein:

- Portanforderung: TCP-Port 7778
- Benutzername und Kennwort nur zum Lesen
- Die XIV CLI muss auf der AU installiert sein

Leistungsanforderungen

Voraussetzungen für die Leistungserfassung sind:

- SMI-S Agent 1.4 oder höher
- SMI-S-kompatibler CIMService, der auf dem Array ausgeführt wird. Auf den meisten XIV-Arrays ist standardmäßig ein CIMServer installiert.
- Für den CIMServer muss eine Benutzeranmeldung bereitgestellt werden. Die Anmeldung muss über vollständigen Lesezugriff auf die Array-Konfiguration und -Eigenschaften verfügen.
- SMI-S-Namespace. Der Standardwert ist root/ibm. Dies ist im CIMServer konfigurierbar.
- Portanforderungen: 5988 für HTTP, 5989 für HTTPS.
- Unter folgendem Link erfahren Sie, wie Sie ein Konto für die SMI-S-Leistungserfassung erstellen: https://www.ibm.com/docs/en/products?topic=/com.ibm.tpc_V41.doc/fqz0_t_adding_cim_agent.html

Konfiguration

Feld	Beschreibung
XIV IP-Adresse	IP-Adresse oder vollqualifizierter Domänenname des XIV-Speichers
Benutzername	Benutzername für den XIV-Speicher
Passwort	Passwort für den XIV-Speicher
Vollständiger Pfad zum XIV CLI-Verzeichnis	Vollständiger Pfad zum Ordner, der die XIV CLI enthält
SMI-S-Host-IP-Adresse	IP-Adresse des SMI-S-Hosts

Erweiterte Konfiguration

Feld	Beschreibung
Inventarabfrageintervall (min)	Intervall zwischen den Bestandsabfragen. Der Standardwert beträgt 40 Minuten.

Feld	Beschreibung
SMI-S-Protokoll	Für die Verbindung mit dem SMI-S-Anbieter verwendetes Protokoll. Zeigt auch den Standardport an.
SMI-S-Port überschreiben	Wenn das Feld „Verbindungstyp“ leer ist, verwenden Sie den Standardport. Andernfalls geben Sie den zu verwendenden Verbindungsport ein.
Benutzername	Benutzername für den SMI-S Provider-Host
Passwort	Kennwort für den SMI-S-Provider-Host
Leistungsabfrageintervall (Sek.)	Intervall zwischen Leistungsabfragen. Der Standardwert beträgt 300 Sekunden.

Fehlerbehebung

Weitere Informationen zu diesem Datensammler finden Sie im"Support" Seite oder in der"Datensammler-Supportmatrix" .

Lenovo Datensammler

Data Infrastructure Insights verwendet den Lenovo-Datensammler, um Bestands- und Leistungsdaten für Lenovo HX-Speichersysteme zu ermitteln.

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Anforderungen

- Externe Prism-IP-Adresse
- Administrator-Benutzername und -Passwort
- TCP-Port-Anforderung: 9440

Konfiguration

Feld	Beschreibung
Externe Prism-IP-Adresse	Die IP-Adresse der externen Datendienste für den Cluster
Benutzername	Benutzername für das Admin-Konto
Passwort	Passwort für das Admin-Konto

Erweiterte Konfiguration

Feld	Beschreibung
TCP-Port	TCP-Port, der für die Verbindung mit dem Array verwendet wird. Der Standardwert ist 9440.

Feld	Beschreibung
Inventarabfrageintervall (min)	Intervall zwischen den Bestandsabfragen. Der Standardwert beträgt 60 Minuten.
Leistungsabfrageintervall (Sek.)	Intervall zwischen Leistungsabfragen. Der Standardwert beträgt 300 Sekunden.

Fehlerbehebung

Weitere Informationen zu diesem Datensammler finden Sie im"Support" Seite oder in der"Datensammler-Supportmatrix" .

Microsoft

Konfigurieren des Azure NetApp Files Datensammlers

Data Infrastructure Insights verwendet den Azure NetApp Files Datensammler, um Bestands- und Leistungsdaten zu erfassen.

Anforderungen

Zur Konfiguration dieses Datensammlers benötigen Sie folgende Informationen.

- Portanforderung: 443 HTTPS
- Azure Management Rest-IP (management.azure.com)
- Azure-Dienstprinzipal-Client-ID (Benutzerkonto)
- Azure-Dienstprinzipal-Authentifizierungsschlüssel (Benutzerkennwort)
- Sie müssen für die Data Infrastructure Insights Erkennung ein Azure-Konto einrichten.

  Sobald das Konto ordnungsgemäß konfiguriert ist und Sie die Anwendung in Azure registrieren, verfügen Sie über die erforderlichen Anmeldeinformationen, um die Azure-Instanz mit Data Infrastructure Insights zu ermitteln. Unter folgendem Link wird beschrieben, wie Sie das Konto für die Erkennung einrichten:

https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal

Konfiguration

Geben Sie die Daten in die Felder des Datensammlers gemäß der folgenden Tabelle ein:

Feld	Beschreibung
Azure-Dienstprinzipal-Client-ID	Anmelde-ID für Azure
Azure-Mandanten-ID	Azure-Mandanten-ID
Azure-Dienstprinzipalauthentifizierungsschlüssel	Login-Authentifizierungsschlüssel
Mir ist bekannt, dass Microsoft mir API-Anfragen in Rechnung stellt.	Aktivieren Sie dies, um zu bestätigen, dass Sie verstanden haben, dass Microsoft Ihnen für API-Anfragen, die durch Insight-Polling gestellt werden, eine Rechnung stellt.

Erweiterte Konfiguration

Feld	Beschreibung
Inventarabfrageintervall (min)	Der Standardwert ist 60

Fehlerbehebung

- Die von Ihrem ANF-Datensammler verwendeten Anmeldeinformationen müssen Zugriff auf alle Azure-Abonnements haben, die ANF-Volumes enthalten.
- Wenn die Leistungserfassung aufgrund des Leserzugriffs fehlschlägt, versuchen Sie, dem Mitwirkenden Zugriff auf Ressourcengruppenebene zu gewähren.

Weitere Informationen zu diesem Datensammler finden Sie im"Support" Seite oder in der"Datensammler-Supportmatrix" .

Microsoft Hyper-V-Datensammler

Der Microsoft Hyper-V-Datensammler erfasst Inventar- und Leistungsdaten aus der virtualisierten Server-Computerumgebung. Dieser Datensammler kann einen eigenständigen Hyper-V-Host oder einen ganzen Cluster erkennen – erstellen Sie einen Sammler pro eigenständigem Host oder Cluster.

Terminologie

Data Infrastructure Insights erhält die folgenden Bestandsinformationen von Microsoft Hyper-V (WMI). Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Virtuelle Festplatte	Virtuelle Festplatte
Gastgeber	Gastgeber
Virtuelle Maschine	Virtuelle Maschine
Cluster Shared Volumes (CSV), Partitionsvolume	Datenspeicher
Internet-SCSI-Gerät, Multi-Path-SCSI-LUN	LUN
Fiber Channel-Anschluss	Hafen

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Anforderungen

Zur Konfiguration dieses Datensammlers sind folgende Voraussetzungen erforderlich:

- Für Hyper-V muss Port 5985 für die Datenerfassung und den Remotezugriff/die Remoteverwaltung geöffnet sein.
- IP-Adresse oder FQDN des Clusters oder eigenständigen Hypervisors. Die Verwendung des Floating-Cluster-Hostnamens oder der IP ist wahrscheinlich der zuverlässigste Ansatz, anstatt den Collector auf nur

einen bestimmten Knoten in einem Cluster zu richten.

- Benutzerkonto auf Administratorebene, das auf allen Hypervisoren im Cluster funktioniert.
- WinRM muss aktiviert sein und auf allen Hypervisoren lauschen
- Portanforderungen: Port 135 über WMI und dynamische TCP-Ports zugewiesen 1024-65535 für Windows 2003 und älter und 49152-65535 für Windows 2008.
- Die DNS-Auflösung muss erfolgreich sein, auch wenn der Datensammler nur auf eine IP-Adresse verweist.
- Bei jedem Hyper-V-Hypervisor muss die „Ressourcenmessung“ für jede VM auf jedem Host aktiviert sein. Dadurch stehen jedem Hypervisor auf jedem Gast mehr Daten für Data Infrastructure Insights zur Verfügung. Wenn dies nicht festgelegt ist, werden für jeden Gast weniger Leistungsmetriken erfasst. Weitere Informationen zur Ressourcenmessung finden Sie in der Microsoft-Dokumentation:

  "Übersicht über die Hyper-V-Ressourcenmessung"

  "Aktivieren Sie VMResourceMetering"

Der Hyper-V-Datensammler erfordert eine Windows-Erfassungseinheit.

Konfiguration

Feld	Beschreibung
Cluster-IP-Adresse oder Floating-Cluster-FQDN	Die IP-Adresse oder der vollqualifizierte Domänenname für den Cluster oder einen eigenständigen, nicht geclusterten Hypervisor
Benutzername	Administrator-Benutzername für den Hypervisor
Passwort	Passwort für den Hypervisor
DNS-Domänensuffix	Das Hostnamensuffix, das mit dem einfachen Hostnamen kombiniert wird, um den FQDN eines Hypervisors darzustellen

Erweiterte Konfiguration

Feld	Beschreibung
Inventarabfrageintervall (min)	Der Standardwert beträgt 20 Minuten.

Fehlerbehebung

Weitere Informationen zu diesem Datensammler finden Sie im"Support" Seite oder in der"Datensammler-Supportmatrix" .

NetApp

NetApp Cloud Volumes ONTAP Datenkollektor

Dieser Datensammler unterstützt die Bestandserfassung von Cloud Volumes ONTAP -Konfigurationen.

Konfiguration

Feld	Beschreibung
NetApp -Verwaltungs-IP-Adresse	IP-Adresse für Cloud Volumes ONTAP
Benutzername	Benutzername für Cloud Volumes ONTAP
Passwort	Passwort für den oben genannten Benutzer

Erweiterte Konfiguration

Feld	Beschreibung
Verbindungstyp	HTTPS empfohlen. Zeigt auch den Standardport an.
Kommunikationsanschluss überschreiben	Zu verwendender Port, wenn nicht Standard.
Inventarabfrageintervall (min)	Der Standardwert ist 60 Minuten.
Inventar gleichzeitige Thread-Anzahl	Anzahl gleichzeitiger Threads.
TLS für HTTPS erzwingen	TLS über HTTPS erzwingen
Netzgruppen automatisch suchen	Netzgruppen automatisch suchen
Netgroup-Erweiterung	Shell oder Datei auswählen
HTTP-Lesezeitlimit (Sekunden)	Der Standardwert ist 30 Sekunden
Erzwingen Sie Antworten als UTF-8	Erzwingen Sie Antworten als UTF-8
Leistungsabfrageintervall (min)	Der Standardwert ist 900 Sekunden.
Leistung: Gleichzeitige Threadanzahl	Anzahl gleichzeitiger Threads.
Erweiterte Zählerdatenerfassung	Aktivieren Sie diese Option, damit Data Infrastructure Insights die erweiterten Metriken aus der folgenden Liste erfasst.

Fehlerbehebung

Weitere Informationen zu diesem Datensammler finden Sie im"Support" Seite oder in der"Datensammler-Supportmatrix" .

NetApp Cloud Volumes Services für AWS-Datensammler

Dieser Datensammler unterstützt die Bestandserfassung von NetApp Cloud Volumes Services für AWS-Konfigurationen.

Konfiguration

Feld	Beschreibung
Cloud Volumes-Region	Region der NetApp Cloud Volumes Services für AWS
API-Schlüssel	Cloud Volumes API-Schlüssel
Geheimschlüssel	Geheimer Schlüssel für Cloud Volumes

Erweiterte Konfiguration

Feld	Beschreibung
Inventarabfrageintervall (min)	Der Standardwert ist 60 Minuten

Fehlerbehebung

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Problem:	Versuchen Sie Folgendes:
Ich habe einen ähnlichen Fehler wie diesen erhalten: „Fehler beim Ausführen der Anforderung: Verbindung zu <AWS-Region-Endpunkt>:8080 [<AWS-Region-Endpunkt>/AWS-Region-Endpunkt-IP>] fehlgeschlagen: Verbindungs-Timeout: GET https://<AWS-Region-Endpunkt-FQDN>:8080/v1/Storage/IPRanges HTTP/1.1“	Der"Proxy" Wird von Data Infrastructure Insights zur Kommunikation mit der Erfassungseinheit verwendet, erfolgt keine Kommunikation zwischen Data Infrastructure Insights und dem Datensammler selbst. Hier sind einige Dinge, die Sie versuchen können: Stellen Sie sicher, dass die Erfassungseinheit den FQDN auflösen und den erforderlichen Port erreichen kann. Bestätigen Sie, dass kein Proxy erforderlich ist, um den in der Fehlermeldung angegebenen Endpunkt zu erreichen. Mit Curl kann die Kommunikation zwischen der Erfassungseinheit und dem Endpunkt getestet werden. Stellen Sie sicher, dass Sie für diesen Test **keinen** Proxy verwenden. Beispiel: root@acquisitionunit# curl -s -H accept:application/json -H "Content-type: application/json" -H api-key:<in den Anmeldeinformationen des Datensammlers verwendeter API-Schlüssel -H secret-key:<in den Anmeldeinformationen des Datensammlers verwendeter geheimer Schlüssel> -X GET https://<Regionaler AWS-Endpunkt>:8080/v1/Storage/IPRanges

Weitere Informationen zu diesem Datensammler finden Sie im"Support" Seite oder in der"Datensammler-Supportmatrix" .

NetApp ONTAP ASA r2 (All-SAN Array) Datenkollektor

Dieser Datensammler erfasst mithilfe von REST-API-Aufrufen Inventar-, EMS-Protokoll- und Leistungsdaten von Speichersystemen mit ONTAP 9.16.0 und höher.

Anforderungen

Für die Konfiguration und Verwendung dieses Datensammlers gelten die folgenden Voraussetzungen:

- Sie müssen Zugriff auf ein Benutzerkonto mit der erforderlichen Zugriffsebene haben. Beachten Sie, dass zum Erstellen eines neuen REST-Benutzers/einer neuen REST-Rolle Administratorberechtigungen erforderlich sind.
  - Funktional stellt Data Infrastructure Insights in erster Linie Leseanforderungen, für die Registrierung von Data Infrastructure Insights beim ONTAP Array sind jedoch einige Schreibberechtigungen erforderlich. Siehe den *Hinweis zu Berechtigungen* direkt unten.

- ONTAP Version 9.16.0 oder höher.
- Portanforderungen: 443

ASA R2 bezeichnet die Modelle der neuesten Generation der ONTAP ASA Speicherplattform. Dazu gehören die Array-Modelle ASA A1K, A90, A70, A50, A30 und A20.

Für alle ASA -Systeme der vorherigen Generation verwenden Sie bitte die"ONTAP REST" Kollektor.

Ein Hinweis zu Berechtigungen

Da eine Reihe von ONTAP -Dashboards von Data Infrastructure Insights auf erweiterten ONTAP Zählern basieren, sollten Sie im Abschnitt „Erweiterte Konfiguration“ des Datensammlers die Option „Erweiterte Zählerdatenerfassung aktivieren“ aktiviert lassen.

Um ein lokales Konto für Data Infrastructure Insights auf Clusterebene zu erstellen, melden Sie sich bei ONTAP mit dem Benutzernamen/Passwort des Clusterverwaltungsadministrators an und führen Sie die folgenden Befehle auf dem ONTAP -Server aus:

1. Bevor Sie beginnen, müssen Sie mit einem *Administrator*-Konto bei ONTAP angemeldet sein und *Befehle auf Diagnoseebene* müssen aktiviert sein.
2. Rufen Sie den Namen des virtuellen Servers vom Typ *admin* ab. Sie werden diesen Namen in nachfolgenden Befehlen verwenden.

```
 vserver show -type admin
. Erstellen Sie eine Rolle mit den folgenden Befehlen:
```

```
security login rest-role create -role {role name} -api /api -access
readonly
security login rest-role create -role {role name} -api
/api/cluster/agents -access all
vserver services web access create -name spi -role {role name} -vserver
{vserver name as retrieved above}
security login create -user-or-group-name {username} -application http
-authentication-method password -role {role name}
```

3. Erstellen Sie den schreibgeschützten Benutzer mit dem folgenden Befehl. Nachdem Sie den Befehl „Erstellen“ ausgeführt haben, werden Sie aufgefordert, ein Kennwort für diesen Benutzer einzugeben.

```
security login create -username ci_user -application http
-authentication-method password -role ci_readonly
```

Wenn ein AD/LDAP-Konto verwendet wird, sollte der Befehl

```
 security login create -user-or-group-name DOMAIN\aduser/adgroup
-application http -authentication-method domain -role ci_readonly
Die resultierende Rolle und Benutzeranmeldung werden etwa wie folgt
aussehen.  Ihre tatsächliche Ausgabe kann abweichen:
```

```
security login rest-role show -vserver <vserver name> -role restRole

               Role                                    Access
Vserver        Name            API                     Level
----------     -------------   --------------------    ------
<vserver name> restRole        /api                    readonly
                               /api/cluster/agents     all
2 entries were displayed.

security login show -vserver <vserver name> -user-or-group-name restUser

Vserver: <vserver name>
                                                                 Second
User/Group                 Authentication                 Acct
Authentication
Name           Application Method        Role Name        Locked Method
-------------- ----------- ------------- ---------------- ------
--------------
restUser       http        password      restRole         no     none
```

Migration

Um von einem früheren ONTAP Datensammler (ontapi) zum neueren ONTAP REST-Sammler zu migrieren, gehen Sie wie folgt vor:

1. Fügen Sie den REST-Collector hinzu. Es wird empfohlen, die Informationen für einen anderen Benutzer einzugeben als den, der für den vorherigen Collector konfiguriert wurde. Verwenden Sie beispielsweise den im Abschnitt „Berechtigungen“ oben angegebenen Benutzer.
2. Halten Sie den vorherigen Collector an, damit er nicht weiter Daten sammelt.
3. Lassen Sie den neuen REST-Collector mindestens 30 Minuten lang Daten erfassen. Ignorieren Sie während dieser Zeit alle Daten, die nicht „normal“ erscheinen.
4. Nach der Ruhephase sollten sich Ihre Daten stabilisieren, da der REST-Collector weiterhin Daten erfasst.

Mit demselben Verfahren können Sie bei Bedarf zum vorherigen Collector zurückkehren.

Konfiguration

Feld	Beschreibung
ONTAP -Verwaltungs-IP-Adresse	IP-Adresse oder vollqualifizierter Domänenname des NetApp Clusters. Muss eine Cluster-Verwaltungs-IP/ein FQDN sein.
ONTAP REST-Benutzername	Benutzername für NetApp Cluster
ONTAP REST-Passwort	Passwort für NetApp -Cluster

Erweiterte Konfiguration

Feld	Beschreibung
Inventarabfrageintervall (min)	Der Standardwert ist 60 Minuten.
Leistungsabfrageintervall (Sek.)	Der Standardwert ist 60 Sekunden.
Erweiterte Zählerdatenerfassung	Wählen Sie diese Option aus, um ONTAP Advanced Counter-Daten in Umfragen einzubeziehen. Standardmäßig aktiviert.
EMS-Ereigniserfassung aktivieren	Wählen Sie diese Option aus, um ONTAP EMS-Protokollereignisdaten einzuschließen. Standardmäßig aktiviert.
EMS-Abfrageintervall (Sek.)	Der Standardwert ist 60 Sekunden.

Terminologie

Data Infrastructure Insights erfasst Inventar-, Protokoll- und Leistungsdaten vom ONTAP Datensammler. Für jeden erworbenen Vermögenswerttyp wird die am häufigsten verwendete Terminologie für den Vermögenswert angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Scheibe	Scheibe
Raid-Gruppe	Datenträgergruppe
Cluster	Storage
Node	Speicherknoten
Aggregat	Speicherpool
LUN	Volumen
Volumen	Internes Volumen
Virtuelle Speichermaschine/VServer	Virtuelle Speichermaschine

ONTAP Datenmanagement-Terminologie

Die folgenden Bedingungen gelten für Objekte oder Verweise, die Sie möglicherweise auf den Zielseiten der ONTAP Data Management-Speicherressourcen finden. Viele dieser Begriffe gelten auch für andere Datensammler.

Storage

- Modell – Eine durch Kommas getrennte Liste der eindeutigen, diskreten Knotenmodellnamen innerhalb dieses Clusters. Wenn alle Knoten in den Clustern vom gleichen Modelltyp sind, wird nur ein Modellname angezeigt.
- Anbieter – derselbe Anbietername, den Sie sehen würden, wenn Sie eine neue Datenquelle konfigurieren würden.
- Seriennummer – Die Array-UUID
- IP – im Allgemeinen handelt es sich dabei um die in der Datenquelle konfigurierten IPs oder Hostnamen.
- Mikrocode-Version – Firmware.
- Rohkapazität – Summe aller physischen Festplatten im System zur Basis 2, unabhängig von ihrer Rolle.
- Latenz – eine Darstellung der Arbeitslasten, die der Host sowohl beim Lesen als auch beim Schreiben erfährt. Im Idealfall bezieht Data Infrastructure Insights diesen Wert direkt, dies ist jedoch häufig nicht der Fall. Anstelle des Arrays, das dies anbietet, führt Data Infrastructure Insights im Allgemeinen eine IOP-gewichtete Berechnung durch, die aus den Statistiken der einzelnen internen Volumes abgeleitet wird.
- Durchsatz – aggregiert aus internen Volumes. Verwaltung – dies kann einen Hyperlink zur Verwaltungsschnittstelle des Geräts enthalten. Programmgesteuert von der Data Infrastructure Insights Datenquelle als Teil der Bestandsberichterstattung erstellt.

Speicherpool

- Speicher – auf welchem Speicher-Array dieser Pool lebt. Obligatorisch.
- Typ – ein beschreibender Wert aus einer Liste mit aufgezählten Möglichkeiten. Am häufigsten wird „Aggregat“ oder „RAID-Gruppe“ verwendet.
- Knoten – Wenn die Architektur dieses Speicherarrays so ist, dass Pools zu einem bestimmten Speicherknoten gehören, wird sein Name hier als Hyperlink zu seiner eigenen Zielseite angezeigt.
- Verwendet Flash-Pool – Ja/Nein-Wert – verfügt dieser SATA/SAS-basierte Pool über SSDs, die zur Caching-Beschleunigung verwendet werden?
- Redundanz – RAID-Level oder Schutzschema. RAID_DP ist doppelte Parität, RAID_TP ist dreifache Parität.
- Kapazität – die Werte hier sind die logisch genutzte, nutzbare Kapazität und die logische Gesamtkapazität sowie der davon genutzte Prozentsatz.
- Überbelegte Kapazität – Wenn Sie durch den Einsatz von Effizienztechnologien eine Gesamtsumme an Volume- oder internen Volume-Kapazitäten zugewiesen haben, die größer ist als die logische Kapazität des Speicherpools, ist der Prozentwert hier größer als 0 %.
- Snapshot – verwendete und gesamte Snapshot-Kapazitäten, wenn Ihre Speicherpoolarchitektur einen Teil ihrer Kapazität Segmentbereichen ausschließlich für Snapshots zuweist. Bei ONTAP in MetroCluster -Konfigurationen ist dies wahrscheinlich, bei anderen ONTAP Konfigurationen ist dies weniger der Fall.
- Auslastung – ein Prozentwert, der den höchsten Prozentsatz der Festplattenauslastung aller Festplatten anzeigt, die Kapazität zu diesem Speicherpool beitragen. Die Festplattenauslastung weist nicht unbedingt eine starke Korrelation mit der Array-Leistung auf. Die Auslastung kann aufgrund von Festplattenneuaufbauten, Deduplizierungsaktivitäten usw. hoch sein, wenn keine vom Host gesteuerten Workloads vorliegen. Darüber hinaus können Replikationsimplementierungen vieler Arrays die Festplattenauslastung erhöhen, ohne dass dies als internes Volume oder Volume-Workload angezeigt wird.
- IOPS – die Summe der IOPs aller Festplatten, die Kapazität zu diesem Speicherpool beitragen. Durchsatz – der Gesamtdurchsatz aller Festplatten, die Kapazität zu diesem Speicherpool beitragen.

Speicherknoten

- Speicher – zu welchem Speicherarray dieser Knoten gehört. Obligatorisch.
- HA-Partner – auf Plattformen, auf denen ein Knoten auf einen und nur einen anderen Knoten umgeschaltet wird, wird er im Allgemeinen hier angezeigt.
- Status – Integrität des Knotens. Nur verfügbar, wenn das Array fehlerfrei genug ist, um von einer Datenquelle inventarisiert zu werden.
- Modell – Modellname des Knotens.
- Version – Versionsname des Geräts.
- Seriennummer – Die Seriennummer des Knotens.
- Speicher – Basis-2-Speicher, falls verfügbar.
- Auslastung – Bei ONTAP ist dies ein Controller-Stressindex aus einem proprietären Algorithmus. Bei jeder Leistungsabfrage wird eine Zahl zwischen 0 und 100 % gemeldet, die entweder der höheren WAFL Festplattenkonflikt- oder der durchschnittlichen CPU-Auslastung entspricht. Wenn Sie anhaltende Werte > 50 % beobachten, deutet dies auf eine Unterdimensionierung hin – möglicherweise ist ein Controller/Knoten nicht groß genug oder es sind nicht genügend rotierende Festplatten vorhanden, um die Schreibarbeitslast aufzunehmen.
- IOPS – Direkt abgeleitet von ONTAP REST-Aufrufen des Knotenobjekts.
- Latenz – Wird direkt aus ONTAP REST-Aufrufen des Knotenobjekts abgeleitet.
- Durchsatz – Direkt abgeleitet von ONTAP REST-Aufrufen des Knotenobjekts.
- Prozessoren – CPU-Anzahl.

ONTAP Leistungsmetriken

Mehrere ONTAP -Modelle bieten Leistungsmetriken für Data Infrastructure Insights , die zur Überwachung oder für Warnmeldungen verwendet werden können. Die unten stehenden Listen unterstützter und nicht unterstützter Modelle sind nicht vollständig, sollen aber als Orientierung dienen. Im Allgemeinen gilt: Wenn ein Modell zur selben Familie gehört wie eines auf der Liste, sollte auch die Unterstützung dieselbe sein.

Unterstützte Modelle:

A200 A220 A250 A300 A320 A400 A700 A700s A800 A900 C190 FAS2240-4 FAS2552 FAS2650 FAS2720 FAS2750 FAS8200 FAS8300 FAS8700 FAS9000

Nicht unterstützte Modelle:

FAS2620 FAS3250 FAS3270 FAS500f FAS6280 FAS/ AFF 8020 FAS/ AFF 8040 FAS/ AFF 8060 FAS/ AFF 8080

Fehlerbehebung

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Problem:	Versuchen Sie Folgendes:
Beim Versuch, einen ONTAP REST-Datensammler zu erstellen, wird ein Fehler wie der folgende angezeigt: Konfiguration: 10.193.70.14: ONTAP Rest-API unter 10.193.70.14 ist nicht verfügbar: 10.193.70.14 konnte /api/cluster nicht abrufen: 400 Ungültige Anforderung	Dies liegt wahrscheinlich an einem älteren ONTAP Array (z. B. ONTAP 9.6), das über keine REST-API-Funktionen verfügt. ONTAP 9.14.1 ist die minimale ONTAP Version, die vom ONTAP REST Collector unterstützt wird. Bei Versionen vor REST ONTAP sind Antworten vom Typ „400 Bad Request“ zu erwarten. Bei ONTAP Versionen, die REST unterstützen, aber nicht 9.14.1 oder höher sind, wird möglicherweise die folgende ähnliche Meldung angezeigt: Konfiguration: 10.193.98.84: ONTAP Rest-API unter 10.193.98.84 ist nicht verfügbar: 10.193.98.84: ONTAP Rest-API unter 10.193.98.84 ist verfügbar: cheryl5-cluster-2 9.10.1 a3cb3247-3d3c-11ee-8ff3-005056b364a7, hat aber nicht mindestens die Version 9.14.1.
Ich sehe leere oder „0“-Metriken, wo der ONTAP ontapi-Collector Daten anzeigt.	ONTAP REST meldet keine Metriken, die nur intern auf dem ONTAP -System verwendet werden. Beispielsweise werden von ONTAP REST keine Systemaggregate erfasst, sondern nur SVMs vom Typ „Daten“. Weitere Beispiele für ONTAP REST-Metriken, die möglicherweise Null- oder leere Daten melden: InternalVolumes: REST meldet nicht mehr vol0. Aggregate: REST meldet nicht mehr aggr0. Speicher: Die meisten Metriken sind eine Zusammenfassung der Metriken des internen Volumes und werden von den oben genannten Faktoren beeinflusst. Speicher-Virtual Machines: REST meldet keine SVMs mehr vom Typ „Daten“ (z. B. „Cluster“, „MGM“, „Knoten“). Möglicherweise stellen Sie auch eine Änderung im Erscheinungsbild von Diagrammen fest, die Daten enthalten. Grund hierfür ist die Änderung des Standardabfragezeitraums für die Leistung von 15 Minuten auf 5 Minuten. Häufigere Abfragen bedeuten mehr Datenpunkte zum Aufzeichnen.

Weitere Informationen finden Sie in der"Support" Seite oder in der"Datensammler-Supportmatrix" .

Datenkollektor der NetApp ONTAP Data Management Software

Dieser Datensammler erfasst Inventar- und Leistungsdaten von Speichersystemen, auf denen ONTAP ausgeführt wird, mithilfe von schreibgeschützten API-Aufrufen von einem ONTAP Konto. Dieser Datensammler erstellt außerdem einen Datensatz im Cluster-Anwendungsregister, um den Support zu beschleunigen.

Terminologie

Data Infrastructure Insights erfasst Bestands- und Leistungsdaten vom ONTAP Datensammler. Für jeden erworbenen Vermögenswerttyp wird die am häufigsten verwendete Terminologie für den Vermögenswert angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Scheibe	Scheibe
Raid-Gruppe	Datenträgergruppe
Cluster	Storage
Node	Speicherknoten
Aggregat	Speicherpool
LUN	Volumen
Volumen	Internes Volumen

ONTAP Datenmanagement-Terminologie

Die folgenden Bedingungen gelten für Objekte oder Verweise, die Sie möglicherweise auf den Zielseiten der ONTAP Data Management-Speicherressourcen finden. Viele dieser Begriffe gelten auch für andere Datensammler.

Storage

- Modell – Eine durch Kommas getrennte Liste der eindeutigen, diskreten Knotenmodellnamen innerhalb dieses Clusters. Wenn alle Knoten in den Clustern vom gleichen Modelltyp sind, wird nur ein Modellname angezeigt.
- Anbieter – derselbe Anbietername, den Sie sehen würden, wenn Sie eine neue Datenquelle konfigurieren würden.
- Seriennummer – Die Seriennummer des Arrays. Bei Speichersystemen mit Clusterarchitektur wie ONTAP Data Management ist diese Seriennummer möglicherweise weniger nützlich als die Seriennummern der einzelnen „Storage Nodes“.
- IP – im Allgemeinen handelt es sich dabei um die in der Datenquelle konfigurierten IPs oder Hostnamen.
- Mikrocode-Version – Firmware.
- Rohkapazität – Summe aller physischen Festplatten im System zur Basis 2, unabhängig von ihrer Rolle.
- Latenz – eine Darstellung der Arbeitslasten, die der Host sowohl beim Lesen als auch beim Schreiben erfährt. Im Idealfall bezieht Data Infrastructure Insights diesen Wert direkt, dies ist jedoch häufig nicht der Fall. Anstelle des Arrays, das dies anbietet, führt Data Infrastructure Insights im Allgemeinen eine IOP-gewichtete Berechnung durch, die aus den Statistiken der einzelnen internen Volumes abgeleitet wird.
- Durchsatz – aggregiert aus internen Volumes. Verwaltung – dies kann einen Hyperlink zur Verwaltungsschnittstelle des Geräts enthalten. Programmgesteuert von der Data Infrastructure Insights Datenquelle als Teil der Bestandsberichterstattung erstellt.

Speicherpool

- Speicher – auf welchem Speicher-Array dieser Pool lebt. Obligatorisch.
- Typ – ein beschreibender Wert aus einer Liste mit aufgezählten Möglichkeiten. Am häufigsten wird „Aggregat“ oder „RAID-Gruppe“ verwendet.
- Knoten – Wenn die Architektur dieses Speicherarrays so ist, dass Pools zu einem bestimmten Speicherknoten gehören, wird sein Name hier als Hyperlink zu seiner eigenen Zielseite angezeigt.
- Verwendet Flash-Pool – Ja/Nein-Wert – verfügt dieser SATA/SAS-basierte Pool über SSDs, die zur Caching-Beschleunigung verwendet werden?

- Redundanz – RAID-Level oder Schutzschema. RAID_DP ist doppelte Parität, RAID_TP ist dreifache Parität.
- Kapazität – die Werte hier sind die logisch genutzte, nutzbare Kapazität und die logische Gesamtkapazität sowie der davon genutzte Prozentsatz.
- Überbelegte Kapazität – Wenn Sie durch den Einsatz von Effizienztechnologien eine Gesamtsumme an Volume- oder internen Volume-Kapazitäten zugewiesen haben, die größer ist als die logische Kapazität des Speicherpools, ist der Prozentwert hier größer als 0 %.
- Snapshot – verwendete und gesamte Snapshot-Kapazitäten, wenn Ihre Speicherpoolarchitektur einen Teil ihrer Kapazität Segmentbereichen ausschließlich für Snapshots zuweist. Bei ONTAP in MetroCluster -Konfigurationen ist dies wahrscheinlich, bei anderen ONTAP Konfigurationen ist dies weniger der Fall.
- Auslastung – ein Prozentwert, der den höchsten Prozentsatz der Festplattenauslastung aller Festplatten anzeigt, die Kapazität zu diesem Speicherpool beitragen. Die Festplattenauslastung weist nicht unbedingt eine starke Korrelation mit der Array-Leistung auf. Die Auslastung kann aufgrund von Festplattenneuaufbauten, Deduplizierungsaktivitäten usw. hoch sein, wenn keine vom Host gesteuerten Workloads vorliegen. Darüber hinaus können Replikationsimplementierungen vieler Arrays die Festplattenauslastung erhöhen, ohne dass dies als internes Volume oder Volume-Workload angezeigt wird.
- IOPS – die Summe der IOPs aller Festplatten, die Kapazität zu diesem Speicherpool beitragen. Durchsatz – der Gesamtdurchsatz aller Festplatten, die Kapazität zu diesem Speicherpool beitragen.

Speicherknoten

- Speicher – zu welchem Speicherarray dieser Knoten gehört. Obligatorisch.
- HA-Partner – auf Plattformen, auf denen ein Knoten auf einen und nur einen anderen Knoten umgeschaltet wird, wird er im Allgemeinen hier angezeigt.
- Status – Integrität des Knotens. Nur verfügbar, wenn das Array fehlerfrei genug ist, um von einer Datenquelle inventarisiert zu werden.
- Modell – Modellname des Knotens.
- Version – Versionsname des Geräts.
- Seriennummer – Die Seriennummer des Knotens.
- Speicher – Basis-2-Speicher, falls verfügbar.
- Auslastung – Bei ONTAP ist dies ein Controller-Stressindex aus einem proprietären Algorithmus. Bei jeder Leistungsabfrage wird eine Zahl zwischen 0 und 100 % gemeldet, die entweder der höheren WAFL Festplattenkonflikt- oder der durchschnittlichen CPU-Auslastung entspricht. Wenn Sie anhaltende Werte > 50 % beobachten, deutet dies auf eine Unterdimensionierung hin – möglicherweise ist ein Controller/Knoten nicht groß genug oder es sind nicht genügend rotierende Festplatten vorhanden, um die Schreibarbeitslast aufzunehmen.
- IOPS – Direkt abgeleitet von ONTAP ZAPI-Aufrufen des Knotenobjekts.
- Latenz – Wird direkt aus ONTAP ZAPI-Aufrufen des Knotenobjekts abgeleitet.
- Durchsatz – Wird direkt aus ONTAP ZAPI-Aufrufen des Knotenobjekts abgeleitet.
- Prozessoren – CPU-Anzahl.

Anforderungen

Für die Konfiguration und Verwendung dieses Datensammlers gelten die folgenden Voraussetzungen:

- Sie müssen Zugriff auf ein Administratorkonto haben, das für schreibgeschützte API-Aufrufe konfiguriert

ist.

- Zu den Kontodetails gehören Benutzername und Passwort.
- Portanforderungen: 80 oder 443
- Kontoberechtigungen:
  - Nur-Lese-Rollennamen für die Ontapi-Anwendung auf dem Standard-Vserver
  - Möglicherweise benötigen Sie zusätzliche optionale Schreibberechtigungen. Siehe den Hinweis zu Berechtigungen weiter unten.
- ONTAP -Lizenzanforderungen:
  - FCP-Lizenz und zugeordnete/maskierte Volumes für die Fibre-Channel-Erkennung erforderlich

Berechtigungsanforderungen für die Erfassung von ONTAP Switch-Metriken

Data Infrastructure Insights bietet die Möglichkeit, ONTAP Cluster-Switch-Daten als Option im Collector zu sammelnErweiterte Konfiguration Einstellungen. Zusätzlich zur Aktivierung auf dem Data Infrastructure Insights Kollektor müssen Sie auch **das ONTAP -System** selbst konfigurieren, um Folgendes bereitzustellen:"Switch-Informationen" und stellen Sie sicher, dass die richtigeBerechtigungen gesetzt, um die Switch-Daten an Data Infrastructure Insights senden zu können.

Konfiguration

Feld	Beschreibung
NetApp Management IP	IP-Adresse oder vollqualifizierter Domänenname des NetApp -Clusters
Benutzername	Benutzername für NetApp Cluster
Passwort	Passwort für NetApp -Cluster

Erweiterte Konfiguration

Feld	Beschreibung
Anschlussart	Wählen Sie HTTP (Standardport 80) oder HTTPS (Standardport 443). Der Standardwert ist HTTPS
Kommunikationsanschluss überschreiben	Geben Sie einen anderen Port an, wenn Sie nicht den Standardport verwenden möchten
Inventarabfrageintervall (min)	Der Standardwert ist 60 Minuten.
Für TLS für HTTPS	Lassen Sie TLS nur als Protokoll zu, wenn Sie HTTPS verwenden
Netzgruppen automatisch suchen	Aktivieren Sie die automatische Netzgruppensuche für Exportrichtlinienregeln
Netgroup-Erweiterung	Expansionsstrategie der Netgroup. Wählen Sie *Datei* oder *Shell*. Der Standardwert ist *shell*.
HTTP-Lesezeitlimit (Sekunden)	Der Standardwert ist 30
Erzwingen Sie Antworten als UTF-8	Zwingt den Datensammlercode, Antworten von der CLI als in UTF-8 vorliegend zu interpretieren

Feld	Beschreibung
Leistungsabfrageintervall (Sek.)	Der Standardwert ist 900 Sekunden.
Erweiterte Zählerdatenerfassung	Aktivieren Sie die ONTAP Integration. Wählen Sie diese Option aus, um ONTAP Advanced Counter-Daten in Umfragen einzubeziehen. Wählen Sie die gewünschten Zähler aus der Liste aus.
Cluster-Switch-Metriken	Erlauben Sie Data Infrastructure Insights , Cluster-Switch-Daten zu erfassen. Beachten Sie, dass Sie zusätzlich zur Aktivierung auf der Data Infrastructure Insights Seite auch das ONTAP -System so konfigurieren müssen, dass es"Switch-Informationen" und stellen Sie sicher, dass die richtigeBerechtigungen gesetzt, um die Switch-Daten an Data Infrastructure Insights senden zu können. Siehe „Hinweis zu Berechtigungen“ weiter unten.

ONTAP Leistungsmetriken

Mehrere ONTAP -Modelle bieten Leistungsmetriken für Data Infrastructure Insights , die zur Überwachung oder für Warnmeldungen verwendet werden können.

Diese Listen sind nicht vollständig und können sich ändern. Wenn ein Modell zur selben Familie gehört wie ein Modell auf der Liste, sollte die Unterstützung grundsätzlich dieselbe sein, dies kann jedoch nicht garantiert werden. Wenn Sie nicht sicher sind, ob Ihr Modell Leistungsmetriken unterstützt, wenden Sie sich an den ONTAP Support.

Unterstützte Modelle:

A200 A220 A250 A300 A320 A400 A700 A700s A800 A900 C190 FAS2240-4 FAS2552 FAS2650 FAS2720 FAS2750 FAS8200 FAS8300 FAS8700 FAS9000

Nicht unterstützte Modelle:

FAS2620 FAS3250 FAS3270 FAS500f FAS6280 FAS/ AFF 8020 FAS/ AFF 8040 FAS/ AFF 8060 FAS/ AFF 8080

Ein Hinweis zu Berechtigungen

Da eine Reihe von ONTAP -Dashboards von Data Infrastructure Insights auf erweiterten ONTAP -Zählern basieren, müssen Sie im Abschnitt „Erweiterte Konfiguration“ des Datensammlers die Option „Erweiterte Zählerdatenerfassung“ aktivieren.

Sie sollten außerdem sicherstellen, dass die Schreibberechtigung für die ONTAP -API aktiviert ist. Dies erfordert normalerweise ein Konto auf Clusterebene mit den erforderlichen Berechtigungen.

Um ein lokales Konto für Data Infrastructure Insights auf Clusterebene zu erstellen, melden Sie sich bei ONTAP mit dem Benutzernamen/Passwort des Clusterverwaltungsadministrators an und führen Sie die folgenden Befehle auf dem ONTAP -Server aus:

1. Bevor Sie beginnen, müssen Sie mit einem *Administrator*-Konto bei ONTAP angemeldet sein und *Befehle auf Diagnoseebene* müssen aktiviert sein.

2. Erstellen Sie mit den folgenden Befehlen eine schreibgeschützte Rolle.

```
security login role create -role ci_readonly -cmddirname DEFAULT -access
readonly
security login role create -role ci_readonly -cmddirname security
-access readonly
security login role create -role ci_readonly -access all -cmddirname
{cluster application-record create}
```

3. Erstellen Sie den schreibgeschützten Benutzer mit dem folgenden Befehl. Nachdem Sie den Befehl „Erstellen“ ausgeführt haben, werden Sie aufgefordert, ein Kennwort für diesen Benutzer einzugeben.

```
security login create -username ci_user -application ontapi
-authentication-method password -role ci_readonly
```

Wenn ein AD/LDAP-Konto verwendet wird, sollte der Befehl

```
 security login create -user-or-group-name DOMAIN\aduser/adgroup
-application ontapi -authentication-method domain -role ci_readonly
Wenn Sie Cluster-Switch-Daten erfassen:
```

```
security login rest-role create -role ci_readonly_rest -api
/api/network/ethernet -access readonly
security login create -user-or-group-name ci_user -application http
-authmethod password -role ci_readonly_rest
```

Die resultierende Rolle und Benutzeranmeldung werden etwa wie folgt aussehen. Ihre tatsächliche Ausgabe kann abweichen:

```
Role Command/ Access
Vserver Name Directory Query Level
---------- ------------- --------- ------------------ --------
cluster1 ci_readonly DEFAULT read only
cluster1 ci_readonly security readonly
```

```
cluster1:security login> show
Vserver: cluster1
Authentication Acct
UserName    Application   Method      Role Name      Locked
---------   -------      ----------- -------------- --------
ci_user     ontapi      password    ci_readonly   no
```

Wenn die ONTAP Zugriffskontrolle nicht richtig eingestellt ist, können Data Infrastructure Insights REST-Aufrufe fehlschlagen, was zu Datenlücken für das Gerät führt. Wenn Sie es beispielsweise auf dem Data Infrastructure Insights -Collector aktiviert, die Berechtigungen auf dem ONTAP jedoch nicht konfiguriert haben, schlägt die Erfassung fehl. Wenn die Rolle zuvor auf ONTAP definiert wurde und Sie die Rest-API-Funktionen hinzufügen, stellen Sie außerdem sicher, dass *http* zur Rolle hinzugefügt wird.

Fehlerbehebung

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Inventar

Problem:	Versuchen Sie Folgendes:
Erhalten Sie die HTTP-Antwort 401 oder den ZAPI-Fehlercode 13003 und ZAPI gibt „Unzureichende Berechtigungen“ oder „Nicht für diesen Befehl autorisiert“ zurück.	Überprüfen Sie Benutzernamen und Passwort sowie Benutzerrechte/Berechtigungen.
Clusterversion ist < 8.1	Die minimal unterstützte Clusterversion ist 8.1. Aktualisieren Sie auf die minimal unterstützte Version.
ZAPI gibt „Clusterrolle ist nicht cluster_mgmt LIF“ zurück.	AU muss mit der Cluster-Management-IP kommunizieren. Überprüfen Sie die IP und wechseln Sie gegebenenfalls zu einer anderen IP
Fehler: „7-Modus-Filer werden nicht unterstützt“	Dies kann passieren, wenn Sie diesen Datensammler verwenden, um 7-Modus-Filer zu ermitteln. Ändern Sie die IP, sodass sie stattdessen auf den CDOT-Cluster verweist.
ZAPI-Befehl schlägt nach erneutem Versuch fehl	AU hat ein Kommunikationsproblem mit dem Cluster. Überprüfen Sie Netzwerk, Portnummer und IP-Adresse. Der Benutzer sollte auch versuchen, einen Befehl über die Befehlszeile der AU-Maschine auszuführen.
AU konnte keine Verbindung zu ZAPI über HTTP herstellen	Überprüfen Sie, ob der ZAPI-Port Klartext akzeptiert. Wenn AU versucht, Klartext an einen SSL-Socket zu senden, schlägt die Kommunikation fehl.
Die Kommunikation schlägt mit SSLException fehl	AU versucht, SSL an einen Klartext-Port auf einem Filer zu senden. Überprüfen Sie, ob der ZAPI-Port SSL akzeptiert, oder verwenden Sie einen anderen Port.

Problem:	Versuchen Sie Folgendes:
Weitere Verbindungsfehler: Die ZAPI-Antwort hat den Fehlercode 13001, „Datenbank ist nicht geöffnet“. Der ZAPI-Fehlercode ist 60 und die Antwort enthält „API wurde nicht rechtzeitig beendet“. Die ZAPI-Antwort enthält „initialize_session() hat eine NULL-Umgebung zurückgegeben“. Der ZAPI-Fehlercode ist 14007 und die Antwort enthält „Knoten ist nicht fehlerfrei“.	Überprüfen Sie Netzwerk, Portnummer und IP-Adresse. Der Benutzer sollte auch versuchen, einen Befehl über die Befehlszeile der AU-Maschine auszuführen.

Performance

Problem:	Versuchen Sie Folgendes:
Fehler „Leistung konnte nicht von ZAPI erfasst werden“	Dies liegt normalerweise daran, dass die Leistungsstatistik nicht ausgeführt wird. Versuchen Sie auf jedem Knoten den folgenden Befehl: > *system node systemshell -node * -command “spmctl -h cmd –stop; spmctl -h cmd –exec”*

Weitere Informationen finden Sie in der"Support" Seite oder in der"Datensammler-Supportmatrix" .

NetApp ONTAP REST-Datenkollektor

Dieser Datensammler erfasst mithilfe von REST-API-Aufrufen Inventar-, EMS-Protokoll- und Leistungsdaten von Speichersystemen mit ONTAP 9.14.1 und höher. Verwenden Sie für ONTAP -Systeme früherer Versionen den ZAPI-basierten Collectortyp „NetApp ONTAP Data Management Software“.

Der ONTAP REST-Collector kann als Ersatz für den vorherigen ONTAPI-basierten Collector verwendet werden. Daher kann es zu Unterschieden bei den erfassten oder gemeldeten Messwerten kommen. Weitere Informationen zu den Unterschieden zwischen ONTAPI und REST finden Sie im"ONTAP 9.14.1 ONTAPI-zu-REST-Zuordnung" Dokumentation.

Anforderungen

Für die Konfiguration und Verwendung dieses Datensammlers gelten die folgenden Voraussetzungen:

- Sie müssen Zugriff auf ein Benutzerkonto mit der erforderlichen Zugriffsebene haben. Beachten Sie, dass zum Erstellen eines neuen REST-Benutzers/einer neuen REST-Rolle Administratorberechtigungen erforderlich sind.
  - Funktional stellt Data Infrastructure Insights in erster Linie Leseanforderungen, für die Registrierung von Data Infrastructure Insights beim ONTAP Array sind jedoch einige Schreibberechtigungen erforderlich. Siehe den *Hinweis zu Berechtigungen* direkt unten.
- ONTAP Version 9.14.1 oder höher.
- Portanforderungen: 443

Ein Hinweis zu Berechtigungen

Da eine Reihe von ONTAP -Dashboards von Data Infrastructure Insights auf erweiterten ONTAP Zählern basieren, sollten Sie im Abschnitt „Erweiterte Konfiguration“ des Datensammlers die Option „Erweiterte

Zählerdatenerfassung aktivieren“ aktiviert lassen.

Um ein lokales Konto für Data Infrastructure Insights auf Clusterebene zu erstellen, melden Sie sich bei ONTAP mit dem Benutzernamen/Passwort des Clusterverwaltungsadministrators an und führen Sie die folgenden Befehle auf dem ONTAP -Server aus:

1. Bevor Sie beginnen, müssen Sie mit einem *Administrator*-Konto bei ONTAP angemeldet sein und *Befehle auf Diagnoseebene* müssen aktiviert sein.
2. Rufen Sie den Namen des virtuellen Servers vom Typ *admin* ab. Sie werden diesen Namen in nachfolgenden Befehlen verwenden.

```
 vserver show -type admin
. Erstellen Sie eine Rolle mit den folgenden Befehlen:
```

```
security login rest-role create -role {role name} -api /api -access
readonly
security login rest-role create -role {role name} -api
/api/cluster/agents -access all
vserver services web access create -name spi -role {role name} -vserver
{vserver name as retrieved above}
```

3. Erstellen Sie den schreibgeschützten Benutzer mit dem folgenden Befehl. Nachdem Sie den Befehl „Erstellen“ ausgeführt haben, werden Sie aufgefordert, ein Kennwort für diesen Benutzer einzugeben. Beachten Sie, dass wir im folgenden Befehl die auf *ci_readonly* eingestellte Rolle anzeigen. Wenn Sie in Schritt 3 oben eine Rolle mit einem anderen Namen erstellen, verwenden Sie stattdessen diesen benutzerdefinierten Rollennamen.

```
 security login create -user-or-group-name {username} -application http
-authentication-method password -role {role name}
Wenn ein AD/LDAP-Konto verwendet wird, sollte der Befehl
```

```
 security login create -user-or-group-name DOMAIN\aduser/adgroup
-application http -authentication-method domain -role ci_readonly
Die resultierende Rolle und Benutzeranmeldung werden etwa wie folgt
aussehen.  Ihre tatsächliche Ausgabe kann abweichen:
```

```
security login rest-role show -vserver <vserver name> -role restRole

               Role                                    Access
Vserver        Name            API                     Level
----------     -------------   -------------------     ------
<vserver name> restRole        /api                    readonly
                               /api/cluster/agents     all
2 entries were displayed.

security login show -vserver <vserver name> -user-or-group-name restUser

Vserver: <vserver name>
                                                                  Second
User/Group                 Authentication                 Acct
Authentication
Name           Application Method        Role Name        Locked Method
-------------- ----------- ------------- ---------------- ------
--------------
restUser       http        password      restRole         no     none
```

Sie können bei Bedarf den SPI-Zugriff überprüfen:

```
**Vserver:> vserver services web access show -name spi
 Vserver                      Type     Service Name     Role
-------------- -------- ---------------- ----------------
<vserver name >     admin             spi           admin
<vserver name >     admin             spi           csrestrole

2 entries were displayed.**
```

Migration

Um von einem früheren ONTAP Datensammler (ontapi) zum neueren ONTAP REST-Sammler zu migrieren, gehen Sie wie folgt vor:

1. Fügen Sie den REST-Collector hinzu. Es wird empfohlen, die Informationen für einen anderen Benutzer einzugeben als den, der für den vorherigen Collector konfiguriert wurde. Verwenden Sie beispielsweise den im Abschnitt „Berechtigungen“ oben angegebenen Benutzer.
2. Halten Sie den vorherigen Collector an, damit er nicht weiter Daten sammelt.
3. Lassen Sie den neuen REST-Collector mindestens 30 Minuten lang Daten erfassen. Ignorieren Sie während dieser Zeit alle Daten, die nicht „normal“ erscheinen.
4. Nach der Ruhephase sollten sich Ihre Daten stabilisieren, da der REST-Collector weiterhin Daten erfasst.

Mit demselben Verfahren können Sie bei Bedarf zum vorherigen Collector zurückkehren.

Konfiguration

Feld	Beschreibung
ONTAP -Verwaltungs-IP-Adresse	IP-Adresse oder vollqualifizierter Domänenname des NetApp Clusters. Muss eine Cluster-Verwaltungs-IP/ein FQDN sein.
ONTAP REST-Benutzername	Benutzername für NetApp Cluster
ONTAP REST-Passwort	Passwort für NetApp -Cluster

Erweiterte Konfiguration

Feld	Beschreibung
Inventarabfrageintervall (min)	Der Standardwert ist 60 Minuten.
Leistungsabfrageintervall (Sek.)	Der Standardwert ist 60 Sekunden.
Erweiterte Zählerdatenerfassung	Wählen Sie diese Option aus, um ONTAP Advanced Counter-Daten in Umfragen einzubeziehen. Standardmäßig aktiviert.
EMS-Ereigniserfassung aktivieren	Wählen Sie diese Option aus, um ONTAP EMS-Protokollereignisdaten einzuschließen. Standardmäßig aktiviert.
EMS-Abfrageintervall (Sek.)	Der Standardwert ist 60 Sekunden.

Terminologie

Data Infrastructure Insights erfasst Inventar-, Protokoll- und Leistungsdaten vom ONTAP Datensammler. Für jeden erworbenen Vermögenswerttyp wird die am häufigsten verwendete Terminologie für den Vermögenswert angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Scheibe	Scheibe
Raid-Gruppe	Datenträgergruppe
Cluster	Storage
Node	Speicherknoten
Aggregat	Speicherpool
LUN	Volumen
Volumen	Internes Volumen
Virtuelle Speichermaschine/VServer	Virtuelle Speichermaschine

ONTAP Datenmanagement-Terminologie

Die folgenden Bedingungen gelten für Objekte oder Verweise, die Sie möglicherweise auf den Zielseiten der ONTAP Data Management-Speicherressourcen finden. Viele dieser Begriffe gelten auch für andere Datensammler.

Storage

- Modell – Eine durch Kommas getrennte Liste der eindeutigen, diskreten Knotenmodellnamen innerhalb dieses Clusters. Wenn alle Knoten in den Clustern vom gleichen Modelltyp sind, wird nur ein Modellname angezeigt.
- Anbieter – derselbe Anbietername, den Sie sehen würden, wenn Sie eine neue Datenquelle konfigurieren würden.
- Seriennummer – Die Array-UUID
- IP – im Allgemeinen handelt es sich dabei um die in der Datenquelle konfigurierten IPs oder Hostnamen.
- Mikrocode-Version – Firmware.
- Rohkapazität – Summe aller physischen Festplatten im System zur Basis 2, unabhängig von ihrer Rolle.
- Latenz – eine Darstellung der Arbeitslasten, die der Host sowohl beim Lesen als auch beim Schreiben erfährt. Im Idealfall bezieht Data Infrastructure Insights diesen Wert direkt, dies ist jedoch häufig nicht der Fall. Anstelle des Arrays, das dies anbietet, führt Data Infrastructure Insights im Allgemeinen eine IOP-gewichtete Berechnung durch, die aus den Statistiken der einzelnen internen Volumes abgeleitet wird.
- Durchsatz – aggregiert aus internen Volumes. Verwaltung – dies kann einen Hyperlink zur Verwaltungsschnittstelle des Geräts enthalten. Programmgesteuert von der Data Infrastructure Insights Datenquelle als Teil der Bestandsberichterstattung erstellt.

Speicherpool

- Speicher – auf welchem Speicher-Array dieser Pool lebt. Obligatorisch.
- Typ – ein beschreibender Wert aus einer Liste mit aufgezählten Möglichkeiten. Am häufigsten wird „Aggregat“ oder „RAID-Gruppe“ verwendet.
- Knoten – Wenn die Architektur dieses Speicherarrays so ist, dass Pools zu einem bestimmten Speicherknoten gehören, wird sein Name hier als Hyperlink zu seiner eigenen Zielseite angezeigt.
- Verwendet Flash-Pool – Ja/Nein-Wert – verfügt dieser SATA/SAS-basierte Pool über SSDs, die zur Caching-Beschleunigung verwendet werden?
- Redundanz – RAID-Level oder Schutzschema. RAID_DP ist doppelte Parität, RAID_TP ist dreifache Parität.
- Kapazität – die Werte hier sind die logisch genutzte, nutzbare Kapazität und die logische Gesamtkapazität sowie der davon genutzte Prozentsatz.
- Überbelegte Kapazität – Wenn Sie durch den Einsatz von Effizienztechnologien eine Gesamtsumme an Volume- oder internen Volume-Kapazitäten zugewiesen haben, die größer ist als die logische Kapazität des Speicherpools, ist der Prozentwert hier größer als 0 %.
- Snapshot – verwendete und gesamte Snapshot-Kapazitäten, wenn Ihre Speicherpoolarchitektur einen Teil ihrer Kapazität Segmentbereichen ausschließlich für Snapshots zuweist. Bei ONTAP in MetroCluster -Konfigurationen ist dies wahrscheinlich, bei anderen ONTAP Konfigurationen ist dies weniger der Fall.
- Auslastung – ein Prozentwert, der den höchsten Prozentsatz der Festplattenauslastung aller Festplatten anzeigt, die Kapazität zu diesem Speicherpool beitragen. Die Festplattenauslastung weist nicht unbedingt eine starke Korrelation mit der Array-Leistung auf. Die Auslastung kann aufgrund von Festplattenneuaufbauten, Deduplizierungsaktivitäten usw. hoch sein, wenn keine vom Host gesteuerten Workloads vorliegen. Darüber hinaus können Replikationsimplementierungen vieler Arrays die Festplattenauslastung erhöhen, ohne dass dies als internes Volume oder Volume-Workload angezeigt wird.
- IOPS – die Summe der IOPs aller Festplatten, die Kapazität zu diesem Speicherpool beitragen. Durchsatz – der Gesamtdurchsatz aller Festplatten, die Kapazität zu diesem Speicherpool beitragen.

Speicherknoten

- Speicher – zu welchem Speicherarray dieser Knoten gehört. Obligatorisch.
- HA-Partner – auf Plattformen, auf denen ein Knoten auf einen und nur einen anderen Knoten umgeschaltet wird, wird er im Allgemeinen hier angezeigt.
- Status – Integrität des Knotens. Nur verfügbar, wenn das Array fehlerfrei genug ist, um von einer Datenquelle inventarisiert zu werden.
- Modell – Modellname des Knotens.
- Version – Versionsname des Geräts.
- Seriennummer – Die Seriennummer des Knotens.
- Speicher – Basis-2-Speicher, falls verfügbar.
- Auslastung – Bei ONTAP ist dies ein Controller-Stressindex aus einem proprietären Algorithmus. Bei jeder Leistungsabfrage wird eine Zahl zwischen 0 und 100 % gemeldet, die entweder der höheren WAFL Festplattenkonflikt- oder der durchschnittlichen CPU-Auslastung entspricht. Wenn Sie anhaltende Werte > 50 % beobachten, deutet dies auf eine Unterdimensionierung hin – möglicherweise ist ein Controller/Knoten nicht groß genug oder es sind nicht genügend rotierende Festplatten vorhanden, um die Schreibarbeitslast aufzunehmen.
- IOPS – Direkt abgeleitet von ONTAP REST-Aufrufen des Knotenobjekts.
- Latenz – Wird direkt aus ONTAP REST-Aufrufen des Knotenobjekts abgeleitet.
- Durchsatz – Direkt abgeleitet von ONTAP REST-Aufrufen des Knotenobjekts.
- Prozessoren – CPU-Anzahl.

ONTAP Leistungsmetriken

Mehrere ONTAP -Modelle bieten Leistungsmetriken für Data Infrastructure Insights , die zur Überwachung oder für Warnmeldungen verwendet werden können. Die unten stehenden Listen unterstützter und nicht unterstützter Modelle sind nicht vollständig, sollen aber als Orientierung dienen. Im Allgemeinen gilt: Wenn ein Modell zur selben Familie gehört wie eines auf der Liste, sollte auch die Unterstützung dieselbe sein.

Unterstützte Modelle:

A200 A220 A250 A300 A320 A400 A700 A700s A800 A900 C190 FAS2240-4 FAS2552 FAS2650 FAS2720 FAS2750 FAS8200 FAS8300 FAS8700 FAS9000

Nicht unterstützte Modelle:

FAS2620 FAS3250 FAS3270 FAS500f FAS6280 FAS/ AFF 8020 FAS/ AFF 8040 FAS/ AFF 8060 FAS/ AFF 8080

Fehlerbehebung

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Problem:	Versuchen Sie Folgendes:
Beim Versuch, einen ONTAP REST-Datensammler zu erstellen, wird ein Fehler wie der folgende angezeigt: Konfiguration: 10.193.70.14: ONTAP Rest-API unter 10.193.70.14 ist nicht verfügbar: 10.193.70.14 konnte /api/cluster nicht abrufen: 400 Ungültige Anforderung	Dies liegt wahrscheinlich an einem älteren ONTAP Array (z. B. ONTAP 9.6), das über keine REST-API-Funktionen verfügt. ONTAP 9.14.1 ist die minimale ONTAP Version, die vom ONTAP REST Collector unterstützt wird. Bei Versionen vor REST ONTAP sind Antworten vom Typ „400 Bad Request“ zu erwarten. Bei ONTAP Versionen, die REST unterstützen, aber nicht 9.14.1 oder höher sind, wird möglicherweise die folgende ähnliche Meldung angezeigt: Konfiguration: 10.193.98.84: ONTAP Rest-API unter 10.193.98.84 ist nicht verfügbar: 10.193.98.84: ONTAP Rest-API unter 10.193.98.84 ist verfügbar: cheryl5-cluster-2 9.10.1 a3cb3247-3d3c-11ee-8ff3-005056b364a7, hat aber nicht mindestens die Version 9.14.1.
Ich sehe leere oder „0“-Metriken, wo der ONTAP ontapi-Collector Daten anzeigt.	ONTAP REST meldet keine Metriken, die nur intern auf dem ONTAP -System verwendet werden. Beispielsweise werden von ONTAP REST keine Systemaggregate erfasst, sondern nur SVMs vom Typ „Daten“. Weitere Beispiele für ONTAP REST-Metriken, die möglicherweise Null- oder leere Daten melden: InternalVolumes: REST meldet nicht mehr vol0. Aggregate: REST meldet nicht mehr aggr0. Speicher: Die meisten Metriken sind eine Zusammenfassung der Metriken des internen Volumes und werden von den oben genannten Faktoren beeinflusst. Speicher-Virtual Machines: REST meldet keine SVMs mehr vom Typ „Daten“ (z. B. „Cluster“, „MGM“, „Knoten“). Möglicherweise stellen Sie auch eine Änderung im Erscheinungsbild von Diagrammen fest, die Daten enthalten. Grund hierfür ist die Änderung des Standardabfragezeitraums für die Leistung von 15 Minuten auf 5 Minuten. Häufigere Abfragen bedeuten mehr Datenpunkte zum Aufzeichnen.

Weitere Informationen finden Sie in der"Support" Seite oder in der"Datensammler-Supportmatrix" .

NetApp Data ONTAP im 7-Mode-Datenkollektor

Für Speichersysteme mit Data ONTAP -Software im 7-Mode verwenden Sie den 7-Mode-Datenkollektor, der die CLI zum Abrufen von Kapazitäts- und Leistungsdaten nutzt.

Terminologie

Data Infrastructure Insights erhält die folgenden Bestandsinformationen vom NetApp 7-Mode-Datenkollektor. Für jeden erworbenen Vermögenswerttyp wird die am häufigsten verwendete Terminologie für diesen Vermögenswert angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Dieser Datensammler ist"veraltet" .

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Scheibe	Scheibe
Raid-Gruppe	Datenträgergruppe
Filer	Storage
Filer	Speicherknoten
Aggregat	Speicherpool
LUN	Volumen
Volumen	Internes Volumen

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Anforderungen

Zur Konfiguration und Nutzung dieses Datensammlers benötigen Sie Folgendes:

- IP-Adressen des FAS Speichercontrollers und -Partners.
- Port 443
- Ein benutzerdefinierter Benutzername und ein Passwort auf Administratorebene für Controller und Partner-Controller mit den folgenden Rollenfunktionen für 7-Mode:
  - „api-*“: Verwenden Sie dies, um OnCommand Insight die Ausführung aller NetApp Speicher-API-Befehle zu ermöglichen.
  - „login-http-admin“: Verwenden Sie dies, um OnCommand Insight die Verbindung zum NetApp -Speicher über HTTP zu ermöglichen.
  - „security-api-vfiler“: Verwenden Sie dies, um OnCommand Insight die Ausführung von NetApp -Speicher-API-Befehlen zum Abrufen von vFiler-Einheiteninformationen zu ermöglichen.
  - „cli-options“: Verwenden Sie dies, um Speichersystemoptionen zu lesen.
  - „cli-lun“: Greifen Sie auf diese Befehle zum Verwalten von LUNs zu. Zeigt den Status (LUN-Pfad, Größe, Online-/Offline-Status und Freigabestatus) der angegebenen LUN oder LUN-Klasse an.
  - „cli-df“: Verwenden Sie dies, um den freien Speicherplatz anzuzeigen.
  - „cli-ifconfig“: Verwenden Sie dies, um Schnittstellen und IP-Adressen anzuzeigen.

Konfiguration

Feld	Beschreibung
Adresse des Speichersystems	IP-Adresse oder vollqualifizierter Domänenname für das NetApp -Speichersystem
Benutzername	Benutzername für das NetApp -Speichersystem
Passwort	Passwort für das NetApp -Speichersystem
Adresse des HA-Partners im Cluster	IP-Adresse oder vollqualifizierter Domänenname für den HA-Partner
Benutzername des HA-Partners im Cluster	Benutzername für den HA-Partner

Feld	Beschreibung
Kennwort des HA-Partner-Filers im Cluster	Passwort für den HA-Partner

Erweiterte Konfiguration

Feld	Beschreibung
Inventarabfrageintervall (min)	Intervall zwischen den Bestandsabfragen. Der Standardwert beträgt 20 Minuten.
Verbindungstyp	HTTPS oder HTTP, zeigt auch den Standardport an
Verbindungsport überschreiben	Wenn das Feld „Verbindungstyp“ leer ist, verwenden Sie den Standardport. Andernfalls geben Sie den zu verwendenden Verbindungsport ein.
Leistungsabfrageintervall (Sek.)	Intervall zwischen Leistungsabfragen. Der Standardwert beträgt 300 Sekunden.

Speichersystemanbindung

Alternativ zur Verwendung des standardmäßigen Administratorbenutzers für diesen Datensammler können Sie einen Benutzer mit Administratorrechten direkt auf den NetApp -Speichersystemen konfigurieren, sodass dieser Datensammler Daten von NetApp -Speichersystemen abrufen kann.

Für die Verbindung mit NetApp -Speichersystemen muss der Benutzer, der beim Erwerb des Haupt-Pfilers (auf dem sich das Speichersystem befindet) angegeben wird, die folgenden Bedingungen erfüllen:

- Der Benutzer muss sich auf vfiler0 (Root-Filer/Pfiler) befinden.

  Speichersysteme werden beim Erwerb des Haupt-Pfilers erworben.

- Die folgenden Befehle definieren die Funktionen der Benutzerrolle:
  - „api-*“: Verwenden Sie dies, um Data Infrastructure Insights die Ausführung aller NetApp -Speicher-API -Befehle zu ermöglichen.

    Dieser Befehl ist zur Verwendung der ZAPI erforderlich.

  - „login-http-admin“: Verwenden Sie dies, um Data Infrastructure Insights die Verbindung zum NetApp -Speicher über HTTP zu ermöglichen. Dieser Befehl ist zur Verwendung der ZAPI erforderlich.
  - „security-api-vfiler“: Verwenden Sie dies, um Data Infrastructure Insights die Ausführung von NetApp -Speicher-API-Befehlen zum Abrufen von vFiler-Einheiteninformationen zu ermöglichen.
  - „cli-options“: Für den Befehl „Optionen“ und wird für Partner-IP und aktivierte Lizenzen verwendet.
  - „cli-lun“: Greifen Sie auf diese Befehle zum Verwalten von LUNs zu. Zeigt den Status (LUN-Pfad, Größe, Online-/Offline-Status und Freigabestatus) der angegebenen LUN oder LUN-Klasse an.
  - „cli-df“: Für die Befehle „df -s“, „df -r“, „df -A -r“ und wird zum Anzeigen des freien Speicherplatzes verwendet.
  - „cli-ifconfig“: Für den Befehl „ifconfig -a“ und zum Abrufen der Filer-IP-Adresse.
  - „cli-rdfile“: Für den Befehl „rdfile /etc/netgroup“ und zum Abrufen von Netzgruppen verwendet.
  - „cli-date“: Für den Befehl „date“ und wird verwendet, um das vollständige Datum zum Abrufen von Snapshot-Kopien zu erhalten.

◦ „cli-snap“: Für den Befehl „Snap List“ und zum Abrufen von Snapshot-Kopien.

Wenn keine CLI-Date- oder CLI-Snap-Berechtigungen bereitgestellt werden, kann die Erfassung abgeschlossen werden, es werden jedoch keine Snapshot-Kopien gemeldet.

Um eine 7-Mode-Datenquelle erfolgreich zu erwerben und keine Warnungen auf dem Speichersystem zu generieren, sollten Sie eine der folgenden Befehlszeichenfolgen verwenden, um Ihre Benutzerrollen zu definieren. Die zweite hier aufgeführte Zeichenfolge ist eine optimierte Version der ersten:

- Login-http-admin, API-*, Sicherheits-API-vfile, CLI-rdfile, CLI-Optionen, CLI-df, CLI-lun, CLI-ifconfig, CLI-date, CLI-snap,_
- login-http-admin,api-* ,security-api-vfile,cli-

Fehlerbehebung

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Inventar

Problem:	Versuchen Sie Folgendes:
Erhalten Sie die HTTP-Antwort 401 oder den ZAPI-Fehlercode 13003 und ZAPI gibt „Unzureichende Berechtigungen“ oder „Nicht für diesen Befehl autorisiert“ zurück.	Überprüfen Sie Benutzernamen und Passwort sowie Benutzerrechte/Berechtigungen.
Fehler „Befehl konnte nicht ausgeführt werden“	Überprüfen Sie, ob der Benutzer über die folgenden Berechtigungen auf dem Gerät verfügt: • api-* • cli-date • cli-df • cli-ifconfig • cli-lun • cli-operations • cli-rdfile • cli-snap • login-http-admin • security-api-vfiler Überprüfen Sie außerdem, ob die ONTAP Version von Data Infrastructure Insights unterstützt wird, und stellen Sie sicher, dass die verwendeten Anmeldeinformationen mit den Anmeldeinformationen des Geräts übereinstimmen.
Clusterversion ist < 8.1	Die minimal unterstützte Clusterversion ist 8.1. Aktualisieren Sie auf die minimal unterstützte Version.
ZAPI gibt „Clusterrolle ist nicht cluster_mgmt LIF“ zurück.	AU muss mit der Cluster-Management-IP kommunizieren. Überprüfen Sie die IP und wechseln Sie gegebenenfalls zu einer anderen IP
Fehler: „7-Modus-Filer werden nicht unterstützt“	Dies kann passieren, wenn Sie diesen Datensammler verwenden, um 7-Modus-Filer zu ermitteln. Ändern Sie die IP, sodass sie stattdessen auf den CDOT-Filer verweist.
ZAPI-Befehl schlägt nach erneutem Versuch fehl	AU hat ein Kommunikationsproblem mit dem Cluster. Überprüfen Sie Netzwerk, Portnummer und IP-Adresse. Der Benutzer sollte auch versuchen, einen Befehl über die Befehlszeile der AU-Maschine auszuführen.
AU konnte keine Verbindung zu ZAPI herstellen	Überprüfen Sie die IP-/Port-Konnektivität und bestätigen Sie die ZAPI-Konfiguration.

Problem:	Versuchen Sie Folgendes:
AU konnte keine Verbindung zu ZAPI über HTTP herstellen	Überprüfen Sie, ob der ZAPI-Port Klartext akzeptiert. Wenn AU versucht, Klartext an einen SSL-Socket zu senden, schlägt die Kommunikation fehl.
Die Kommunikation schlägt mit SSLException fehl	AU versucht, SSL an einen Klartext-Port auf einem Filer zu senden. Überprüfen Sie, ob der ZAPI-Port SSL akzeptiert, oder verwenden Sie einen anderen Port.
Weitere Verbindungsfehler: Die ZAPI-Antwort hat den Fehlercode 13001, „Datenbank ist nicht geöffnet“. Der ZAPI-Fehlercode ist 60 und die Antwort enthält „API wurde nicht rechtzeitig beendet“. Die ZAPI-Antwort enthält „initialize_session() hat eine NULL-Umgebung zurückgegeben“. Der ZAPI-Fehlercode ist 14007 und die Antwort enthält „Knoten ist nicht fehlerfrei“.	Überprüfen Sie Netzwerk, Portnummer und IP-Adresse. Der Benutzer sollte auch versuchen, einen Befehl über die Befehlszeile der AU-Maschine auszuführen.
Socket-Timeout-Fehler mit ZAPI	Überprüfen Sie die Filer-Konnektivität und/oder erhöhen Sie das Timeout.
Fehler „C-Modus-Cluster werden von der 7-Modus-Datenquelle nicht unterstützt“	Überprüfen Sie die IP und ändern Sie die IP in einen 7-Modus-Cluster.
Fehler „Verbindung zum vFiler fehlgeschlagen“	Überprüfen Sie, ob die Berechtigungen des abrufenden Benutzers mindestens Folgendes umfassen: api-* security-api-vfiler login-http-admin. Bestätigen Sie, dass auf dem Filer mindestens ONTAPI Version 1.7 ausgeführt wird.

Weitere Informationen finden Sie in der"Support" Seite oder in der"Datensammler-Supportmatrix" .

NetApp E-Series Legacy Santricity API-Datenkollektor

Der NetApp E-Series Legacy Santricity API-Datensammler sammelt Inventar- und Leistungsdaten. Der Collector unterstützt Firmware 7.x+ mit denselben Konfigurationen und meldet dieselben Daten.

Terminologie

Cloud Insight erhält die folgenden Bestandsinformationen vom NetApp E-Series-Datenkollektor. Für jeden erworbenen Vermögenswerttyp wird die am häufigsten verwendete Terminologie für diesen Vermögenswert angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Scheibe	Scheibe
Volumengruppe	Datenträgergruppe
Speicher-Array	Storage
Regler	Speicherknoten
Volumengruppe	Speicherpool

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Volumen	Volumen

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

E-Series-Terminologie (Landingpage)

Die folgenden Bedingungen gelten für Objekte oder Referenzen, die Sie möglicherweise auf den Zielseiten der NetApp E-Series-Assets finden. Viele dieser Begriffe gelten auch für andere Datensammler.

Storage

- Modell – Modellname des Geräts.
- Anbieter – derselbe Anbietername, den Sie sehen würden, wenn Sie eine neue Datenquelle konfigurieren würden
- Seriennummer – Die Seriennummer des Arrays. Bei Speichersystemen mit Clusterarchitektur wie NetApp Clustered Data Ontap ist diese Seriennummer möglicherweise weniger nützlich als die Seriennummern der einzelnen „Storage Nodes“.
- IP – im Allgemeinen die IP(s) oder Hostnamen, wie sie in der Datenquelle konfiguriert sind
- Mikrocode-Version – Firmware
- Rohkapazität – Basis-2-Summierung aller physischen Festplatten im System, unabhängig von ihrer Rolle
- Latenz – eine Darstellung der Arbeitslasten, die der Host sowohl beim Lesen als auch beim Schreiben erfährt. Im Idealfall bezieht Data Infrastructure Insights diesen Wert direkt, dies ist jedoch häufig nicht der Fall. Anstelle des Arrays, das dies anbietet, führt Data Infrastructure Insights im Allgemeinen eine IOP-gewichtete Berechnung durch, die aus den Statistiken der einzelnen Volumes abgeleitet wird.
- Durchsatz – der gesamte Host-Durchsatz des Arrays. Idealerweise direkt aus dem Array bezogen, falls nicht verfügbar, summiert Data Infrastructure Insights den Durchsatz der Volumes, um diesen Wert abzuleiten
- Verwaltung – dies kann einen Hyperlink zur Verwaltungsschnittstelle des Geräts enthalten. Programmgesteuert von der Data Infrastructure Insights -Datenquelle als Teil der Bestandsberichterstattung erstellt

Speicherpool

- Speicher – auf welchem Speicher-Array dieser Pool lebt. Obligatorisch
- Typ – ein beschreibender Wert aus einer Liste mit aufgezählten Möglichkeiten. Am häufigsten werden „Thin Provisioning“ oder „RAID-Gruppe“ verwendet.
- Knoten – Wenn die Architektur dieses Speicherarrays so ist, dass Pools zu einem bestimmten Speicherknoten gehören, wird sein Name hier als Hyperlink zu seiner eigenen Zielseite angezeigt.
- Verwendet Flash Pool – Ja/Nein-Wert
- Redundanz – RAID-Level oder Schutzschema. E-Serie meldet „RAID 7“ für DDP-Pools
- Kapazität – die Werte hier sind die logisch genutzte, nutzbare Kapazität und die logische Gesamtkapazität sowie der davon genutzte Prozentsatz. Diese Werte beinhalten beide die „Erhaltungskapazität“ der E-Serie, was dazu führt, dass sowohl die Zahlen als auch der Prozentsatz höher sind als das, was die Benutzeroberfläche der E-Serie möglicherweise anzeigt
- Überbelegte Kapazität – Wenn Sie über Effizienztechnologien eine Gesamtsumme an Volume- oder

internen Volume-Kapazitäten zugewiesen haben, die größer ist als die logische Kapazität des Speicherpools, ist der Prozentwert hier größer als 0 %.

- Snapshot – verwendete und gesamt Snapshot-Kapazitäten, wenn Ihre Speicherpoolarchitektur einen Teil ihrer Kapazität Segmentbereichen ausschließlich für Snapshots zuweist
- Auslastung – ein Prozentwert, der den höchsten Prozentsatz der Festplattenauslastung aller Festplatten anzeigt, die Kapazität zu diesem Speicherpool beitragen. Die Festplattenauslastung weist nicht unbedingt eine starke Korrelation mit der Array-Leistung auf. Die Auslastung kann aufgrund von Festplattenneuaufbauten, Deduplizierungsaktivitäten usw. hoch sein, wenn keine vom Host gesteuerten Workloads vorliegen. Darüber hinaus kann die Replikationsimplementierung vieler Arrays die Festplattenauslastung erhöhen, ohne dass dies als Volume-Arbeitslast angezeigt wird.
- IOPS – die Summe der IOPs aller Festplatten, die Kapazität zu diesem Speicherpool beitragen. Wenn auf einer bestimmten Plattform keine Festplatten-IOPs verfügbar sind, wird dieser Wert aus der Summe der Volume-IOPs für alle Volumes in diesem Speicherpool ermittelt.
- Durchsatz – der Gesamtdurchsatz aller Festplatten, die Kapazität zu diesem Speicherpool beitragen. Wenn auf einer bestimmten Plattform kein Festplattendurchsatz verfügbar ist, wird dieser Wert aus der Summe der Datenträger aller Datenträger in diesem Speicherpool ermittelt.

Speicherknoten

- Speicher – zu welchem Speicherarray dieser Knoten gehört. Obligatorisch
- HA-Partner – auf Plattformen, auf denen ein Knoten auf einen und nur einen anderen Knoten umgeschaltet wird, wird er im Allgemeinen hier angezeigt
- Status – Integrität des Knotens. Nur verfügbar, wenn das Array gesund genug ist, um von einer Datenquelle inventarisiert zu werden
- Modell – Modellname des Knotens
- Version – Versionsname des Geräts.
- Seriennummer – Die Seriennummer des Knotens
- Speicher – Basis-2-Speicher, falls verfügbar
- Auslastung – Im Allgemeinen eine CPU-Auslastungszahl oder im Fall von NetApp Ontap ein Controller-Stressindex. Die Nutzung ist derzeit für die NetApp E-Serie nicht verfügbar
- IOPS – eine Zahl, die die hostgesteuerten IOPs auf diesem Controller darstellt. Idealerweise wird die Quelle direkt aus dem Array bezogen. Wenn sie nicht verfügbar ist, wird sie durch Summieren aller IOPs für Volumes berechnet, die ausschließlich zu diesem Knoten gehören.
- Latenz – eine Zahl, die die typische Host-Latenz oder Reaktionszeit auf diesem Controller darstellt. Idealerweise wird die Quelle direkt aus dem Array bezogen. Wenn sie nicht verfügbar ist, wird sie durch eine IOP-gewichtete Berechnung aus Volumes berechnet, die ausschließlich zu diesem Knoten gehören.
- Durchsatz – eine Zahl, die den hostgesteuerten Durchsatz auf diesem Controller darstellt. Idealerweise wird der Datendurchsatz direkt aus dem Array bezogen. Falls er nicht verfügbar ist, wird er durch Summieren des gesamten Durchsatzes für Volumes berechnet, die ausschließlich zu diesem Knoten gehören.
- Prozessoren – CPU-Anzahl

Anforderungen

- Die IP-Adresse jedes Controllers im Array
- Portanforderung 2463

Konfiguration

Feld	Beschreibung
Durch Kommas getrennte Liste der Array SANtricity Controller-IPs	IP-Adressen und/oder vollqualifizierte Domänennamen für die Array-Controller

Erweiterte Konfiguration

Feld	Beschreibung
Inventarabfrageintervall (min)	Der Standardwert ist 30 Minuten
Leistungsabfrageintervall bis zu 3600 Sekunden	Der Standardwert ist 300 Sekunden

Fehlerbehebung

Weitere Informationen zu diesem Datensammler finden Sie im"Support" Seite oder in der"Datensammler-Supportmatrix" .

NetApp E-Series REST-Datenkollektor

Der REST-Datenkollektor der NetApp E-Serie sammelt Inventar- und Leistungsdaten. Der Collector unterstützt Firmware 7.x+ mit denselben Konfigurationen und meldet dieselben Daten. Der REST-Collector überwacht den Verschlüsselungsstatus von Speicherpools sowie den Verschlüsselungsstatus zugehöriger Festplatten und Volumes und bietet die CPU-Auslastung des Speicherknotens als Leistungsindikator – eine Funktion, die im älteren SANtricity E-Series-Collector nicht verfügbar ist.

Terminologie

Cloud Insight erfasst mithilfe von REST die folgenden Bestandsinformationen von der NetApp E-Serie. Für jeden erworbenen Vermögenswerttyp wird die am häufigsten verwendete Terminologie für diesen Vermögenswert angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Scheibe	Scheibe
Volumengruppe	Datenträgergruppe
Speicher-Array	Storage
Regler	Speicherknoten
Volumengruppe	Speicherpool
Volumen	Volumen

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Anforderungen

- Die IP-Adresse jedes Controllers im Array
- Dieser Collector unterstützt nur E-Series-Modell-Arrays mit **nativen REST-API-Funktionen**. Die E-Series-Organisation liefert eine außerhalb des Arrays installierbare REST-API-Distribution für ältere E-Series-Arrays: Dieser Collector unterstützt dieses Szenario nicht. Benutzer mit älteren Arrays sollten weiterhin Data Infrastructure Insights verwenden."E-Serie SANtricity API" Kollektor.
- Das Feld „IP-Adressen des E-Series-Controllers“ unterstützt eine durch Kommas getrennte Zeichenfolge mit zwei IP-/Hostnamen. Der Collector versucht automatisch, den zweiten IP-/Hostnamen zu verwenden, wenn auf den ersten nicht zugegriffen werden kann.
- HTTPS-Port: Standard ist 8443.

Konfiguration

Feld	Beschreibung
IP-Adressen der E-Serie-Controller	Komma-getrennte IP-Adressen und/oder vollqualifizierte Domänennamen für die Array-Controller

Erweiterte Konfiguration

Feld	Beschreibung
Inventarabfrageintervall (min)	Der Standardwert ist 30 Minuten
Leistungsabfrageintervall bis zu 3600 Sekunden	Der Standardwert ist 300 Sekunden

E-Series-Terminologie (Landingpage)

Die folgenden Bedingungen gelten für Objekte oder Referenzen, die Sie möglicherweise auf den Zielseiten der NetApp E-Series-Assets finden. Viele dieser Begriffe gelten auch für andere Datensammler.

Storage

- Modell – Modellname des Geräts.
- Anbieter – derselbe Anbietername, den Sie sehen würden, wenn Sie eine neue Datenquelle konfigurieren würden
- Seriennummer – Die Seriennummer des Arrays. Bei Speichersystemen mit Clusterarchitektur wie NetApp Clustered Data Ontap ist diese Seriennummer möglicherweise weniger nützlich als die Seriennummern der einzelnen „Storage Nodes“.
- IP – im Allgemeinen die IP(s) oder Hostnamen, wie sie in der Datenquelle konfiguriert sind
- Mikrocode-Version – Firmware
- Rohkapazität – Basis-2-Summierung aller physischen Festplatten im System, unabhängig von ihrer Rolle
- Latenz – eine Darstellung der Arbeitslasten, die der Host sowohl beim Lesen als auch beim Schreiben erfährt. Im Idealfall bezieht Data Infrastructure Insights diesen Wert direkt, dies ist jedoch häufig nicht der Fall. Anstelle des Arrays, das dies anbietet, führt Data Infrastructure Insights im Allgemeinen eine IOP-gewichtete Berechnung durch, die aus den Statistiken der einzelnen Volumes abgeleitet wird.
- Durchsatz – der gesamte Host-Durchsatz des Arrays. Idealerweise direkt aus dem Array bezogen, falls nicht verfügbar, summiert Data Infrastructure Insights den Durchsatz der Volumes, um diesen Wert

abzuleiten

- Verwaltung – dies kann einen Hyperlink zur Verwaltungsschnittstelle des Geräts enthalten. Programmgesteuert von der Data Infrastructure Insights -Datenquelle als Teil der Bestandsberichterstattung erstellt

Speicherpool

- Speicher – auf welchem Speicher-Array dieser Pool lebt. Obligatorisch
- Typ – ein beschreibender Wert aus einer Liste mit aufgezählten Möglichkeiten. Am häufigsten werden „Thin Provisioning“ oder „RAID-Gruppe“ verwendet.
- Knoten – Wenn die Architektur dieses Speicherarrays so ist, dass Pools zu einem bestimmten Speicherknoten gehören, wird sein Name hier als Hyperlink zu seiner eigenen Zielseite angezeigt.
- Verwendet Flash Pool – Ja/Nein-Wert
- Redundanz – RAID-Level oder Schutzschema. E-Serie meldet „RAID 7“ für DDP-Pools
- Kapazität – die Werte hier sind die logisch genutzte, nutzbare Kapazität und die logische Gesamtkapazität sowie der davon genutzte Prozentsatz. Diese Werte beinhalten beide die „Erhaltungskapazität“ der E-Serie, was dazu führt, dass sowohl die Zahlen als auch der Prozentsatz höher sind als das, was die Benutzeroberfläche der E-Serie möglicherweise anzeigt
- Überbelegte Kapazität – Wenn Sie über Effizienztechnologien eine Gesamtsumme an Volume- oder internen Volume-Kapazitäten zugewiesen haben, die größer ist als die logische Kapazität des Speicherpools, ist der Prozentwert hier größer als 0 %.
- Snapshot – verwendete und gesamt Snapshot-Kapazitäten, wenn Ihre Speicherpoolarchitektur einen Teil ihrer Kapazität Segmentbereichen ausschließlich für Snapshots zuweist
- Auslastung – ein Prozentwert, der den höchsten Prozentsatz der Festplattenauslastung aller Festplatten anzeigt, die Kapazität zu diesem Speicherpool beitragen. Die Festplattenauslastung weist nicht unbedingt eine starke Korrelation mit der Array-Leistung auf. Die Auslastung kann aufgrund von Festplattenneuaufbauten, Deduplizierungsaktivitäten usw. hoch sein, wenn keine vom Host gesteuerten Workloads vorliegen. Darüber hinaus kann die Replikationsimplementierung vieler Arrays die Festplattenauslastung erhöhen, ohne dass dies als Volume-Arbeitslast angezeigt wird.
- IOPS – die Summe der IOPs aller Festplatten, die Kapazität zu diesem Speicherpool beitragen. Wenn auf einer bestimmten Plattform keine Festplatten-IOPs verfügbar sind, wird dieser Wert aus der Summe der Volume-IOPs für alle Volumes in diesem Speicherpool ermittelt.
- Durchsatz – der Gesamtdurchsatz aller Festplatten, die Kapazität zu diesem Speicherpool beitragen. Wenn auf einer bestimmten Plattform kein Festplattendurchsatz verfügbar ist, wird dieser Wert aus der Summe der Datenträger aller Datenträger in diesem Speicherpool ermittelt.

Speicherknoten

- Speicher – zu welchem Speicherarray dieser Knoten gehört. Obligatorisch
- HA-Partner – auf Plattformen, auf denen ein Knoten auf einen und nur einen anderen Knoten umgeschaltet wird, wird er im Allgemeinen hier angezeigt
- Status – Integrität des Knotens. Nur verfügbar, wenn das Array gesund genug ist, um von einer Datenquelle inventarisiert zu werden
- Modell – Modellname des Knotens
- Version – Versionsname des Geräts.
- Seriennummer – Die Seriennummer des Knotens

- Speicher – Basis-2-Speicher, falls verfügbar
- Auslastung – Im Allgemeinen eine CPU-Auslastungszahl oder im Fall von NetApp Ontap ein Controller-Stressindex. Die Nutzung ist derzeit für die NetApp E-Serie nicht verfügbar
- IOPS – eine Zahl, die die hostgesteuerten IOPs auf diesem Controller darstellt. Idealerweise wird die Quelle direkt aus dem Array bezogen. Wenn sie nicht verfügbar ist, wird sie durch Summieren aller IOPs für Volumes berechnet, die ausschließlich zu diesem Knoten gehören.
- Latenz – eine Zahl, die die typische Host-Latenz oder Reaktionszeit auf diesem Controller darstellt. Idealerweise wird die Quelle direkt aus dem Array bezogen. Wenn sie nicht verfügbar ist, wird sie durch eine IOP-gewichtete Berechnung aus Volumes berechnet, die ausschließlich zu diesem Knoten gehören.
- Durchsatz – eine Zahl, die den hostgesteuerten Durchsatz auf diesem Controller darstellt. Idealerweise wird der Datendurchsatz direkt aus dem Array bezogen. Falls er nicht verfügbar ist, wird er durch Summieren des gesamten Durchsatzes für Volumes berechnet, die ausschließlich zu diesem Knoten gehören.
- Prozessoren – CPU-Anzahl

Fehlerbehebung

Weitere Informationen zu diesem Datensammler finden Sie im"Support" Seite oder in der"Datensammler-Supportmatrix" .

Konfigurieren des NetApp HCI Management-Server-Datenkollektors

Der Datensammler des NetApp HCI Management-Servers sammelt NetApp HCI Hostinformationen und erfordert schreibgeschützte Berechtigungen für alle Objekte innerhalb des Management-Servers.

Dieser Datensammler ruft Daten nur vom * NetApp HCI Management-Server* ab. Um Daten aus dem Speichersystem zu sammeln, müssen Sie außerdem die"NetApp SolidFire" Datensammler.

Terminologie

Data Infrastructure Insights erhält von diesem Datensammler die folgenden Bestandsinformationen. Für jeden erworbenen Vermögenswerttyp wird die am häufigsten verwendete Terminologie für den Vermögenswert angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Virtuelle Festplatte	Scheibe
Gastgeber	Gastgeber
Virtuelle Maschine	Virtuelle Maschine
Datenspeicher	Datenspeicher
LUN	Volumen
Fibre-Channel-Anschluss	Hafen

Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Anforderungen

Zur Konfiguration dieses Datensammlers sind folgende Angaben erforderlich:

- IP-Adresse des NetApp HCI Management-Servers
- Nur-Lese-Benutzername und -Passwort für den NetApp HCI Management-Server
- Nur Leseberechtigungen für alle Objekte im NetApp HCI Management-Server.
- SDK-Zugriff auf den NetApp HCI Management-Server – normalerweise bereits eingerichtet.
- Portanforderungen: http-80 https-443
- Zugriff validieren:
  - Melden Sie sich mit dem oben genannten Benutzernamen und Kennwort beim NetApp HCI Management-Server an
  - Überprüfen Sie, ob das SDK aktiviert ist: Telnet <vc_ip> 443

Einrichtung und Anschluss

Feld	Beschreibung
Name	Eindeutiger Name für den Datensammler
Erfassungseinheit	Name der Erfassungseinheit

Konfiguration

Feld	Beschreibung
NetApp HCI Storage Cluster MVIP	Virtuelle Verwaltungs-IP-Adresse
SolidFire -Verwaltungsknoten (mNode)	IP-Adresse des Verwaltungsknotens
Benutzername	Benutzername für den Zugriff auf den NetApp HCI Management-Server
Passwort	Kennwort für den Zugriff auf den NetApp HCI -Verwaltungsserver
VCenter-Benutzername	Benutzername für VCenter
VCenter-Passwort	Kennwort für VCenter

Erweiterte Konfiguration

Aktivieren Sie im Bildschirm „Erweiterte Konfiguration“ das Kontrollkästchen **VM-Leistung**, um Leistungsdaten zu erfassen. Die Inventarerfassung ist standardmäßig aktiviert. Die folgenden Felder können konfiguriert werden:

Feld	Beschreibung
Inventarabfrageintervall (min)	Der Standardwert ist 20
Filtern Sie VMs nach	Wählen Sie CLUSTER, DATACENTER oder ESX HOST
Wählen Sie „Ausschließen“ oder „Einschließen“, um eine Liste anzugeben	Angeben, ob VMs ein- oder ausgeschlossen werden sollen

Geräteliste filtern	Liste der zu filternden VMs (durch Komma getrennt oder durch Semikolon getrennt, wenn im Wert ein Komma verwendet wird) zum Filtern nur nach ESX_HOST, CLUSTER und DATACENTER
Leistungsabfrageintervall (Sek.)	Der Standardwert ist 300

Fehlerbehebung

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Inventar

Problem:	Versuchen Sie Folgendes:
Fehler: Die Einschlussliste zum Filtern von VMs darf nicht leer sein	Wenn „Liste einschließen“ ausgewählt ist, listen Sie bitte gültige DataCenter-, Cluster- oder Hostnamen auf, um VMs zu filtern
Fehler: Es konnte keine Verbindung zu VirtualCenter unter IP hergestellt werden	Mögliche Lösungen: * Überprüfen Sie die eingegebenen Anmeldeinformationen und die IP-Adresse. * Versuchen Sie, über den Infrastructure Client mit Virtual Center zu kommunizieren. * Versuchen Sie, über den Managed Object Browser (z. B. MOB) mit Virtual Center zu kommunizieren.
Fehler: VirtualCenter bei IP verfügt über ein nicht konformes Zertifikat, das JVM benötigt	Mögliche Lösungen: * Empfohlen: Generieren Sie das Zertifikat für Virtual Center neu, indem Sie einen stärkeren (z. B. 1024-Bit) RSA-Schlüssel verwenden. * Nicht empfohlen: Ändern Sie die JVM-Konfiguration java.security, um die Einschränkung jdk.certpath.disabledAlgorithms zu nutzen und einen 512-Bit-RSA-Schlüssel zuzulassen. Siehe Versionshinweise zu JDK 7 Update 40 unter"http://www.oracle.com/technetwork/java/javase/7u40-relnotes-2004172.html"

Weitere Informationen finden Sie in der"Support" Seite oder in der"Datensammler-Supportmatrix" .

NetApp SolidFire All-Flash Array-Datenkollektor

Der NetApp SolidFire All-Flash Array-Datenkollektor unterstützt die Bestandsaufnahme und Leistungserfassung von iSCSI- und Fibre Channel SolidFire Konfigurationen.

Der SolidFire Datensammler verwendet die SolidFire REST-API. Die Erfassungseinheit, auf der sich der Datensammler befindet, muss in der Lage sein, HTTPS-Verbindungen zum TCP-Port 443 der SolidFire -Clusterverwaltungs-IP-Adresse herzustellen. Der Datensammler benötigt Anmeldeinformationen, die REST-API-Abfragen im SolidFire Cluster durchführen können.

Terminologie

Data Infrastructure Insights erhält die folgenden Bestandsinformationen vom NetApp SolidFire All-Flash Array-Datenkollektor. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten

verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Fahren	Scheibe
Cluster	Storage
Node	Speicherknoten
Volumen	Volumen
Fibre-Channel-Anschluss	Hafen
Volume-Zugriffsgruppe, LUN-Zuweisung	Volumenkarte
iSCSI-Sitzung	Volumenmaske

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Anforderungen

Für die Konfiguration dieses Datensammlers gelten die folgenden Voraussetzungen:

- Virtuelle Verwaltungs-IP-Adresse
- Benutzername und Anmeldeinformationen sind schreibgeschützt
- Port 443

Konfiguration

Feld	Beschreibung
Virtuelle Verwaltungs-IP-Adresse (MVIP)	Virtuelle IP-Adresse des SolidFire -Clusters verwalten
Benutzername	Name, der für die Anmeldung beim SolidFire -Cluster verwendet wird
Passwort	Kennwort zum Anmelden beim SolidFire -Cluster

Erweiterte Konfiguration

Feld	Beschreibung
Verbindungstyp	Verbindungstyp auswählen
Kommunikationsanschluss	Für die NetApp API verwendeter Port
Inventarabfrageintervall (min)	Der Standardwert ist 20 Minuten
Leistungsabfrageintervall (Sek.)	Der Standardwert ist 300 Sekunden

Fehlerbehebung

Wenn SolidFire einen Fehler meldet, wird dieser in Data Infrastructure Insights wie folgt angezeigt:

Beim Versuch, Daten abzurufen, wurde eine Fehlermeldung von einem SolidFire -Gerät empfangen. Der

Aufruf war <Methode> (<ParameterString>). Die Fehlermeldung des Geräts lautete (siehe Gerätehandbuch): <message>

Wo:

- Die <Methode> ist eine HTTP-Methode, beispielsweise GET oder PUT.
- Der <parameterString> ist eine durch Kommas getrennte Liste von Parametern, die im REST-Aufruf enthalten waren.
- Die <message> ist die vom Gerät zurückgegebene Fehlermeldung.

Weitere Informationen zu diesem Datensammler finden Sie im"Support" Seite oder in der"Datensammler-Supportmatrix" .

NetApp StorageGRID Datenkollektor

Der NetApp StorageGRID Datenkollektor unterstützt die Bestands- und Leistungserfassung von StorageGRID Konfigurationen.

> Um eine konsistente Messung der DII-Berechtigungen über alle StorageGRID -Systeme hinweg unabhängig von der zugrunde liegenden Hardwaretopologie und -konfiguration zu gewährleisten, verwendet Data Infrastructure Insights die gesamte verfügbare Kapazität (storagegrid_storage_utilization_total_space_bytes) anstelle der RAW-Kapazität basierend auf dem physischen Festplattenlayout.
>
> Für Kunden, die das kapazitätsbasierte Lizenzmodell verwenden, wird StorageGRID als „Objekt“-Speicher gemessen.
>
> Für Kunden, die das alte (MU) Lizenzmodell verwenden, wird StorageGRID als Sekundärspeicher mit einem Satz von 40 TiB zu 1 MU gemessen.

Terminologie

Data Infrastructure Insights erhält die folgenden Bestandsinformationen vom NetApp StorageGRID Collector. Für jeden erworbenen Vermögenswerttyp wird die am häufigsten verwendete Terminologie für diesen Vermögenswert angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
StorageGRID	Storage
Node	Node
Mieter	Speicherpool
Eimer	Internes Volumen

Anforderungen

Für die Konfiguration dieser Datenquelle gelten die folgenden Voraussetzungen:

- StorageGRID Host-IP-Adresse
- Ein Benutzername und ein Kennwort für einen Benutzer, dem die Rollen „Metrikabfrage“ und „Mandantenzugriff“ zugewiesen wurden

- Port 443

Konfiguration

Feld	Beschreibung
StorageGRID Host-IP-Adresse	Verwaltung Virtuelle IP-Adresse des StorageGRID -Geräts
Benutzername	Name, der für die Anmeldung beim StorageGRID -Gerät verwendet wird
Passwort	Kennwort zum Anmelden bei der StorageGRID -Appliance

Erweiterte Konfiguration

Feld	Beschreibung
Inventarabfrageintervall (min)	Der Standardwert ist 60 Minuten
Leistungsabfrageintervall (Sek.)	Der Standardwert ist 900 Sekunden

Einmaliges Anmelden (SSO)

Der"StorageGRID" Firmware-Versionen haben entsprechende API-Versionen; 3.0 API und neuere Versionen unterstützen die Single Sign-On-Anmeldung (SSO).

Firmware-Version	API-Version	Unterstützt Single Sign-On (SSO)
11,1	2	Nein
11,2	3,0	Ja
11,5	3,3	Ja

Fehlerbehebung

Weitere Informationen zu diesem Datensammler finden Sie im"Support" Seite oder in der"Datensammler-Supportmatrix" .

Nutanix NX-Datensammler

Data Infrastructure Insights verwendet den Nutanix-Datensammler, um Bestands- und Leistungsdaten für Nutanix NX-Speichersysteme zu ermitteln.

Terminologie

Data Infrastructure Insights erhält die folgenden Bestandsinformationen vom Nutanix-Datensammler. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Speicherpool	Speicherpool

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Nutanix-Container	Internes Volumen
Nutanix-Container	Dateifreigabe
NFS-Freigabe	Aktie

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Anforderungen

- Die IP-Adresse der externen Datendienste für den Cluster
- Nur-Lese-Benutzername und -Passwort, es sei denn, es werden Volume-Gruppen verwendet. In diesem Fall sind der Administrator-Benutzername und das Administrator-Passwort erforderlich.
- Portanforderung: HTTPS 443

Konfiguration

Feld	Beschreibung
Externe Prism-IP-Adresse	Die IP-Adresse der externen Datendienste für den Cluster
Benutzername	Benutzername für das Admin-Konto
Passwort	Passwort für das Admin-Konto

Erweiterte Konfiguration

Feld	Beschreibung
TCP-Port	TCP-Port, der für die Verbindung mit dem Nutanix-Array verwendet wird. Der Standardwert ist 9440.
Inventarabfrageintervall (min)	Intervall zwischen den Bestandsabfragen. Der Standardwert beträgt 60 Minuten.
Leistungsabfrageintervall (Sek.)	Intervall zwischen Leistungsabfragen. Der Standardwert beträgt 300 Sekunden.

Fehlerbehebung

Weitere Informationen zu diesem Datensammler finden Sie im"Support" Seite oder in der"Datensammler-Supportmatrix" .

Oracle ZFS Storage Appliance-Datenkollektor

Data Infrastructure Insights verwendet den Oracle ZFS Storage Appliance-Datensammler, um Bestands- und Leistungsdaten zu erfassen.

Terminologie

Data Infrastructure Insights erfasst Bestandsinformationen mit dem Oracle ZFS-Datenkollektor. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Festplatte (SSD)	Scheibe
Cluster	Storage
Regler	Speicherknoten
LUN	Volumen
LUN-Karte	Volumenkarte
Initiator, Ziel	Volumenmaske
Aktie	Internes Volumen

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diese Datenquelle darstellen.

Anforderungen

- Hostnamen für den ZFS-Controller-1 und den ZFS-Controller-2
- Administrator-Benutzername und -Passwort
- Portanforderung: 215 HTTP/HTTPS

Erforderliche Leistungsmetriken

Oracle ZFS-Geräte bieten Speicheradministratoren große Flexibilität bei der Erfassung von Leistungsstatistiken. Data Infrastructure Insights erwartet, dass Sie *jeden* Controller in einem Hochverfügbarkeitspaar so konfigurieren, dass die folgenden Metriken erfasst werden:

- smb2.ops[teilen]
- nfs3.ops[teilen]
- nfs4.ops[teilen]
- nfs4-1.ops[teilen]

Wenn der Controller einige oder alle dieser Daten nicht erfasst, führt dies wahrscheinlich dazu, dass Data Infrastructure Insights die Arbeitslast auf den „internen Volumes“ nicht erfasst oder zu niedrig angibt.

Konfiguration

Feld	Beschreibung
ZFS-Controller-1-Hostname	Hostname für Speichercontroller 1
ZFS-Controller-2-Hostname	Hostname für Speichercontroller 2

Feld	Beschreibung
Benutzername	Benutzername für das Benutzerkonto des Speichersystemadministrators
Passwort	Kennwort für das Administrator-Benutzerkonto

Erweiterte Konfiguration

Feld	Beschreibung
Verbindungstyp	HTTPS oder HTTP, zeigt auch den Standardport an
Verbindungsport überschreiben	Wenn das Feld „Verbindungstyp“ leer ist, verwenden Sie den Standardport. Andernfalls geben Sie den zu verwendenden Verbindungsport ein.
Inventarabfrageintervall	Der Standardwert beträgt 60 Sekunden
Leistungsabfrageintervall (Sek.)	Der Standardwert ist 300.

Fehlerbehebung

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Inventar

Problem:	Versuchen Sie Folgendes:
„Ungültige Anmeldedaten“	ZFS-Benutzerkonto und Passwort validieren
„Anforderung fehlgeschlagen mit Status 404 https://…..:215/api/access/v1“	Ihr ZFS-Array ist möglicherweise zu alt, um REST-API-Unterstützung zu bieten. AK 2013.1.3.0 war die erste REST-API-fähige ZFS-Betriebssystemversion und nicht alle ZFS-Geräte können darauf aktualisiert werden.
„Konfigurationsfehler“ mit Fehlermeldung „REST-Dienst ist deaktiviert“	Überprüfen Sie, ob der REST-Dienst auf diesem Gerät aktiviert ist.

Problem:	Versuchen Sie Folgendes:
„Konfigurationsfehler“ mit Fehlermeldung „Benutzer nicht autorisiert für Befehl“	Dieser Fehler ist wahrscheinlich darauf zurückzuführen, dass bestimmte Rollen (z. B. „advanced_analytics“) für den konfigurierten Benutzer nicht enthalten sind. Durch Anwenden des Analytics-Bereichs für den Benutzer mit schreibgeschützter Rolle kann der Fehler möglicherweise behoben werden. Gehen Sie folgendermaßen vor: 1. Bewegen Sie im ZFs-System im Bildschirm „Konfiguration → Benutzer“ die Maus über die Rolle und doppelklicken Sie, um die Bearbeitung zu ermöglichen 2. Wählen Sie „Analytics“ aus dem Dropdown-Menü „Bereich“ aus. Es erscheint eine Liste der möglichen Eigenschaften. 3. Klicken Sie auf das oberste Kontrollkästchen, um alle drei Eigenschaften auszuwählen. 4. Klicken Sie auf der rechten Seite auf die Schaltfläche „Hinzufügen“. 5. Klicken Sie oben rechts im Popup-Fenster auf die Schaltfläche „Übernehmen“. Das Popup-Fenster wird geschlossen.

Weitere Informationen finden Sie in der"Support" Seite oder in der"Datensammler-Supportmatrix" .

Pure Storage FlashArray-Datensammler

Data Infrastructure Insights verwendet den Pure Storage FlashArray-Datensammler, um Bestands- und Leistungsdaten zu erfassen.

Terminologie

Für jeden von Data Infrastructure Insights erfassten Asset-Typ wird die am häufigsten verwendete Terminologie für das Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Laufwerk (SSD)	Scheibe
Anordnung	Storage
Regler	Speicherknoten
Volumen	Volumen
LUN-Karte	Volumenkarte
Initiator, Ziel	Volumenmaske

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Anforderungen

- IP-Adresse des Speichersystems
- Benutzername und Passwort für das Administratorkonto des Pure-Speichersystems.
- Portanforderung: HTTP/HTTPS 80/443

Konfiguration

Feld	Beschreibung
FlashArray-Host-IP-Adresse	IP-Adresse des Speichersystems
Benutzername	Benutzername mit Administratorrechten
Kennwort für das Administratorkonto	Passwort

Erweiterte Konfiguration

Feld	Beschreibung
Anschlussart	Wählen Sie HTTP oder HTTPS. Zeigt auch den Standardport an.
TCP-Port überschreiben	Wenn das Feld „Verbindungstyp“ leer ist, verwenden Sie den Standardport. Andernfalls geben Sie den zu verwendenden Verbindungsport ein.
Inventarabfrageintervall (min)	Der Standardwert beträgt 60 Minuten
Leistungsabfrageintervall (Sek.)	Der Standardwert ist 300

Fehlerbehebung

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Inventar

Problem:	Versuchen Sie Folgendes:
„Ungültige Anmeldeinformationen“ mit den Fehlermeldungen „Richtlinie lässt dies nicht zu“ oder „Sie sind nicht autorisiert“	Validieren Sie das Pure-Benutzerkonto und das Passwort über die Pure-HTTP-Schnittstelle

Weitere Informationen finden Sie in der"Support" Seite oder in der"Datensammler-Supportmatrix" .

Red Hat Virtualization-Datenkollektor

Data Infrastructure Insights verwendet den Red Hat Virtualization-Datensammler, um Inventardaten von virtualisierten Linux- und Microsoft Windows-Workloads zu sammeln.

Terminologie

Für jeden von Data Infrastructure Insights erfassten Asset-Typ wird die am häufigsten verwendete Terminologie für das Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Scheibe	Virtuelle Festplatte
Gastgeber	Gastgeber
Virtuelle Maschine	Virtuelle Maschine
Speicherdomäne	Datenspeicher
Logische Einheit	LUN

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Anforderungen

- IP-Adresse des RHEV-Servers über Port 443 per REST-API
- Nur-Lese-Benutzername und -Passwort
- RHEV Version 3.0+

Konfiguration

Feld	Beschreibung
RHEV-Server-IP-Adresse	IP-Adresse des Speichersystems
Benutzername	Benutzername mit Administratorrechten
Kennwort für das Administratorkonto	Passwort

Erweiterte Konfiguration

Feld	Beschreibung
HTTPS-Kommunikationsport	Für die HTTPS-Kommunikation mit RHEV verwendeter Port
Inventarabfrageintervall (min)	Der Standardwert beträgt 20 Minuten.

Fehlerbehebung

Weitere Informationen zu diesem Datensammler finden Sie im"Support" Seite oder in der"Datensammler-Supportmatrix" .

Rubrik CDM-Datensammler

Data Infrastructure Insights verwendet den Rubrik-Datensammler, um Bestands- und Leistungsdaten von Rubrik-Speichergeräten zu erfassen.

Terminologie

Data Infrastructure Insights erhält die folgenden Bestandsinformationen vom Rubrik-Datensammler. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Cluster	Speicher, Speicherpool
Node	Speicherknoten
Scheibe	Scheibe

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diese Datenquelle darstellen.

Anforderungen

Zur Konfiguration dieses Datensammlers sind folgende Voraussetzungen erforderlich:

- Die Data Infrastructure Insights Acquisition Unit initiiert Verbindungen zum TCP-Port 443 zum Rubrik-Cluster. Ein Kollektor pro Cluster.
- IP-Adresse des Rubrik-Clusters.
- Benutzername und Passwort für den Cluster.
- IP-Adresse oder Hostname des Rubrik-Clusters.
- Für die Basisauthentifizierung ein Benutzername und ein Kennwort für den Cluster. Wenn Sie die Authentifizierung auf Basis eines Dienstkontos bevorzugen, benötigen Sie ein Dienstkonto, ein Geheimnis und eine Organisations-ID
- Portanforderung: HTTPS 443

Konfiguration

Feld	Beschreibung
IP	IP-Adresse des Rubrik-Clusters
Benutzername / Dienstkonto	Benutzername für den Cluster
Passwort / Geheimnis	Kennwort für den Cluster
Organisations-ID für das Service-Konto	Dies muss die vollständige Zeichenfolge sein, z. B. „Organization:::nnnnnn-nnnn….“

Erweiterte Konfiguration

Inventarabfrageintervall (min)	Der Standardwert ist 60
Leistungsabfrageintervall (Sek.)	Der Standardwert ist 300

Fehlerbehebung

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Inventar

Problem:	Versuchen Sie Folgendes:
Ich habe eine Nachricht erhalten, dass mehr als ein Speicher erstellt wurde.	Überprüfen Sie, ob der Cluster richtig konfiguriert ist und der Collector auf einen einzelnen Cluster verweist.
Umfrage schlägt mit 400 [Ungültige Anfrage] fehl. … Ungültige ManagedId….	Sie haben das Feld „Organisations-ID“ mit einem Wert ausgefüllt, aber der Rubrik-Cluster glaubt NICHT, dass es sich um eine gültige Organisations-ID handelt, obwohl die Fehlermeldung von Rubrik darauf als „ManagedId“ verweist.

Weitere Informationen finden Sie in der"Support" Seite oder in der"Datensammler-Supportmatrix" .

Konfigurieren des VMware VSphere-Datenkollektors

Der Datensammler für VMware vSphere sammelt Leistungs- und Konfigurationsinformationen von VM-Gästen und ESXi-Hosts und erfordert schreibgeschützte Berechtigungen für alle Objekte innerhalb von vSphere. Ab August 2024 bringt der vSphere-Collector zusätzlich Protokollnachrichten aus vSphere-Umgebungen und einige VMware-spezifische Metriken ein. Bitte beachten Sie, dass Data Infrastructure Insights nur VMware-Protokollinformationen aus Umgebungen mit vSphere 8.0.1 oder höher abrufen kann. Ebenso werden die anbieterspezifischen Metriken nur für vSphere 7+-Umgebungen unterstützt. Daher möchten Sie möglicherweise das Kontrollkästchen „Protokolle“ und/oder „Anbieterspezifische Metriken“ bei einem bestimmten Collector deaktivieren, wenn dieser auf eine ältere vSphere-Instanz verweist.

Terminologie

Data Infrastructure Insights erhält die folgenden Bestandsinformationen vom VMware vSphere-Datenkollektor. Für jeden erworbenen Vermögenswerttyp wird die am häufigsten verwendete Terminologie für den Vermögenswert angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Virtuelle Festplatte	Scheibe
Gastgeber	Gastgeber
Virtuelle Maschine	Virtuelle Maschine
Datenspeicher	Datenspeicher
LUN	Volumen
Fibre-Channel-Anschluss	Hafen

Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Anforderungen

Zur Konfiguration dieses Datensammlers sind folgende Angaben erforderlich:

- IP-Adresse des Virtual Center-Servers
- Benutzername und Kennwort im Virtual Center sind schreibgeschützt
- Wir benötigen nur Leseberechtigungen für alle Objekte im Virtual Center.
- SDK-Zugriff auf den Virtual Center-Server – normalerweise bereits eingerichtet.
- Portanforderungen: http-80 https-443
- Zugriff validieren:
  - Melden Sie sich mit dem oben genannten Benutzernamen und Kennwort beim Virtual Center Client an
  - Überprüfen Sie, ob das SDK aktiviert ist: Telnet <vc_ip> 443

Einrichtung und Anschluss

Feld	Beschreibung
Name	Eindeutiger Name für den Datensammler
Erfassungseinheit	Name der Erfassungseinheit

Konfiguration

Feld	Beschreibung
IP-Adresse des virtuellen Zentrums	IP-Adresse des Virtual Centers
Benutzername	Benutzername für den Zugriff auf das Virtual Center
Passwort	Passwort für den Zugriff auf das Virtual Center

Erweiterte Konfiguration

Aktivieren Sie im Bildschirm „Erweiterte Konfiguration“ das Kontrollkästchen **VM-Leistung**, um Leistungsdaten zu erfassen. Die Inventarerfassung ist standardmäßig aktiviert. Die folgenden Felder können konfiguriert werden:

Feld	Beschreibung
Inventarabfrageintervall (min)	Der Standardwert ist 20
Filtern von VMs	Wählen Sie CLUSTER, DATACENTER oder ESX HOST
Wählen Sie „Ausschließen“ oder „Einschließen“, um eine Liste anzugeben	Erstellen Sie eine Filterliste (CLUSTER, DATACENTER und/oder ESX_HOST).
Anzahl der Wiederholungsversuche	Der Standardwert ist 3
Kommunikationsanschluss	Der Standardwert ist 443

Geräteliste filtern…	Diese Liste muss aus exakten Zeichenfolgenübereinstimmungen bestehen. Wenn Sie nach ESX_HOST filtern möchten, müssen Sie eine durch Kommas getrennte Liste der exakten „Namen“ Ihrer ESX-Hosts erstellen, wie sie sowohl in Data Infrastructure Insights als auch in vSphere gemeldet werden. Bei diesen „Namen“ kann es sich entweder um IP-Adressen, einfache Hostnamen oder vollqualifizierte Domänennamen (FQDNs) handeln. Dies wird dadurch bestimmt, wie diese Hosts benannt wurden, als sie ursprünglich zu vSphere hinzugefügt wurden. Verwenden Sie beim Filtern nach CLUSTER die Clusternamen im Data Infrastructure Insights-Stil, wie sie von CI auf Hypervisoren gemeldet werden – Data Infrastructure Insights stellt dem vSphere-Clusternamen den Namen des vSphere-Rechenzentrums und einen Schrägstrich voran – „DC1/clusterA“ ist der Clustername, den Data Infrastructure Insights auf einem Hypervisor in ClusterA innerhalb des Rechenzentrums DC1 melden würde.
Leistungsabfrageintervall (Sek.)	Der Standardwert ist 300

Zuordnen von VMware-Tags zu Data Infrastructure Insights -Anmerkungen

Mit dem VMware-Datensammler können Sie Data Infrastructure Insights -Anmerkungen mit auf VMware konfigurierten Tags füllen. Der DII-Annotationsname muss mit dem VMware-*Kategorie*namen identisch sein. Das Tag wird dann als Annotationswert einer DII-Annotation mit demselben Namen wie die Kategorie angewendet. Data Infrastructure Insights füllt immer gleichnamige Textanmerkungen aus und unternimmt den bestmöglichen Versuch, Anmerkungen anderer Typen (Zahl, Boolescher Wert usw.) auszufüllen. Wenn Ihre Anmerkung einen anderen Typ hat und der Datensammler sie nicht ausfüllen kann, kann es erforderlich sein, die Anmerkung zu entfernen und als Texttyp neu zu erstellen.

Beachten Sie, dass bei VMware-Tags die Groß- und Kleinschreibung beachtet werden kann, bei Data Infrastructure Insights -Tags hingegen nicht. Wenn Sie also in Data Infrastructure Insights eine Annotation mit dem Namen „OWNER“ und in VMware Tags mit den Namen „OWNER“, „Owner“ und „owner“ erstellen, werden alle diese Variationen von „owner“ der Annotation „OWNER“ von Cloud Insight zugeordnet.

Beachten Sie Folgendes:

- Data Infrastructure Insights veröffentlicht derzeit nur automatisch Supportinformationen für NetApp -Geräte.
- Da diese Supportinformationen in Form von Anmerkungen vorliegen, können Sie sie abfragen oder in Dashboards verwenden.
- Wenn ein Benutzer den Annotationswert überschreibt oder leert, wird der Wert automatisch erneut ausgefüllt, wenn Data Infrastructure Insights die Annotationen aktualisiert, was einmal täglich geschieht.

Fehlerbehebung

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Inventar

Problem:	Versuchen Sie Folgendes:
Fehler: Die Einschlussliste zum Filtern von VMs darf nicht leer sein	Wenn „Liste einschließen“ ausgewählt ist, listen Sie bitte gültige DataCenter-, Cluster- oder Hostnamen auf, um VMs zu filtern
Fehler: Es konnte keine Verbindung zu VirtualCenter unter IP hergestellt werden	Mögliche Lösungen: * Überprüfen Sie die eingegebenen Anmeldeinformationen und die IP-Adresse. * Versuchen Sie, über den VMware Infrastructure Client mit Virtual Center zu kommunizieren. * Versuchen Sie, über den Managed Object Browser (z. B. MOB) mit Virtual Center zu kommunizieren.
Fehler: VirtualCenter bei IP verfügt über ein nicht konformes Zertifikat, das JVM benötigt	Mögliche Lösungen: * Empfohlen: Generieren Sie das Zertifikat für Virtual Center neu, indem Sie einen stärkeren (z. B. 1024-Bit) RSA-Schlüssel verwenden. * Nicht empfohlen: Ändern Sie die JVM-Konfiguration java.security, um die Einschränkung jdk.certpath.disabledAlgorithms zu nutzen und einen 512-Bit-RSA-Schlüssel zuzulassen. Sehen "Versionshinweise zu JDK 7 Update 40" .
Ich sehe die Meldung: „VMware Logs-Paket wird auf VMware unter Version 8.0.1 nicht unterstützt.“	Die Protokollerfassung wird auf VMware-Versionen vor 8.0.1 nicht unterstützt. Aktualisieren Sie Ihre VI Center-Infrastruktur auf Version 8.0.1 oder höher, wenn Sie die Funktion „Protokollsammlungen“ in Data Infrastructure Insights verwenden möchten. Weitere Informationen finden Sie hier"KB-Artikel" .

Weitere Informationen finden Sie in der"Support" Seite oder in der"Datensammler-Supportmatrix" .

Datensammlerreferenz – Dienste

Knotendatenerfassung

Data Infrastructure Insights sammelt Metriken von dem Knoten, auf dem Sie einen Agenten installieren.

Installation

1. Wählen Sie unter **Observability > Collectors** ein Betriebssystem/eine Plattform aus. Beachten Sie, dass durch die Installation eines beliebigen Integrationsdatensammlers (Kubernetes, Docker, Apache usw.) auch die Knotendatenerfassung konfiguriert wird.
2. Befolgen Sie die Anweisungen zum Konfigurieren des Agenten. Die Anweisungen variieren je nach Art des Betriebssystems oder der Plattform, die Sie zum Sammeln von Daten verwenden.

Objekte und Zähler

Die folgenden Objekte und ihre Zähler werden als Knotenmetriken erfasst:

Objekt:	Kennungen:	Merkmale:	Datenpunkte:
Knotendateisystem	Knoten-UUID-Gerätepfadtyp	Knoten-IP Knotenname Knoten-Betriebssystemmodus	Freie Inodes Freie Inodes Gesamtanzahl der verwendeten Inodes Gesamtanzahl der verwendeten Inodes Gesamtanzahl der verwendeten Inodes
Knotendatenträger	Knoten-UUID-Datenträger	Knoten-IP Knotenname Knoten-Betriebssystem	IO-Zeit Laufende IOPS Gesamtanzahl gelesener Bytes (pro Sek.) Lesezeit Gesamtanzahl gelesener Bytes (pro Sek.) Gewichtete IO-Zeit Gesamtanzahl geschriebener Bytes (pro Sek.) Schreibzeit Gesamtanzahl geschriebener Bytes (pro Sek.) Aktuelle Warteschlangenlänge der Festplatte Schreibzeit Lesezeit IO-Zeit
Knoten-CPU	Knoten-UUID-CPU	Knoten-IP Knotenname Knoten-Betriebssystem	System-CPU-Auslastung Benutzer-CPU-Auslastung Leerlauf-CPU-Auslastung Prozessor-CPU-Auslastung Interrupt-CPU-Auslastung DPC-CPU-Auslastung

Objekt:	Kennungen:	Merkmale:	Datenpunkte:
Node	Knoten-UUID	Knoten-IP Knotenname Knoten-Betriebssystem	Kernel-Bootzeit Kernel-Kontextwechsel (pro Sek.) Verfügbare Kernel-Entropie Kernel-Interrupts (pro Sek.) Abgespaltene Kernel-Prozesse (pro Sek.) Aktiver Speicher Verfügbarer Gesamtspeicher Verfügbarer Speicher Gepufferter Speicher Zwischengespeicherter Speicher Commit-Limit Als Speicher festgeschriebener Speicher Dirty Memory Freier Speicher hoch Freier Speicher hoch Gesamtspeicher Größe großer Seiten Speicher Große Seiten Freier Speicher Große Seiten Gesamtspeicher niedrig Freier Speicher niedrig Gesamtspeicher Zugeordneter Speicher Seitentabellen Speicher Gemeinsam genutzter Speicher Slab-Speicher Swap Zwischengespeicherter Speicher Swap Freier Speicher Swap Gesamtspeicher Gesamt verwendeter Speicher Gesamt verwendeter Speicher Speicher Vmalloc-Chunk-Speicher Vmalloc Gesamtspeicher Vmalloc Verwendeter Speicher Verdrahteter Speicher Writeback Gesamter Speicher Writeback Temporärer Speicher Cache-Fehler Speicherbedarf Null-Fehler Speicherseitenfehler Speicherseiten Speicher Nicht ausgelagerter Speicher Ausgelagerter Speicher Cache-Kernspeicher Standby-Cache Normaler Speicher Standby-Cache

Objekt:	Kennungen:	Merkmale:	Datenpunkte:
Knotennetzwerk	Netzwerkschnittstellenknoten-UUID	Knotenname Knoten-IP Knoten-Betriebssystem	Empfangene Bytes Gesendete Bytes Ausgehende Pakete Verworfene Pakete Ausgehende Fehler Empfangene Pakete Verworfene Pakete Empfangene Fehler Empfangene Pakete Gesendete Pakete

Aufstellen

Informationen zur Einrichtung und Fehlerbehebung finden Sie auf der"Konfigurieren eines Agenten" Seite.

ActiveMQ-Datensammler

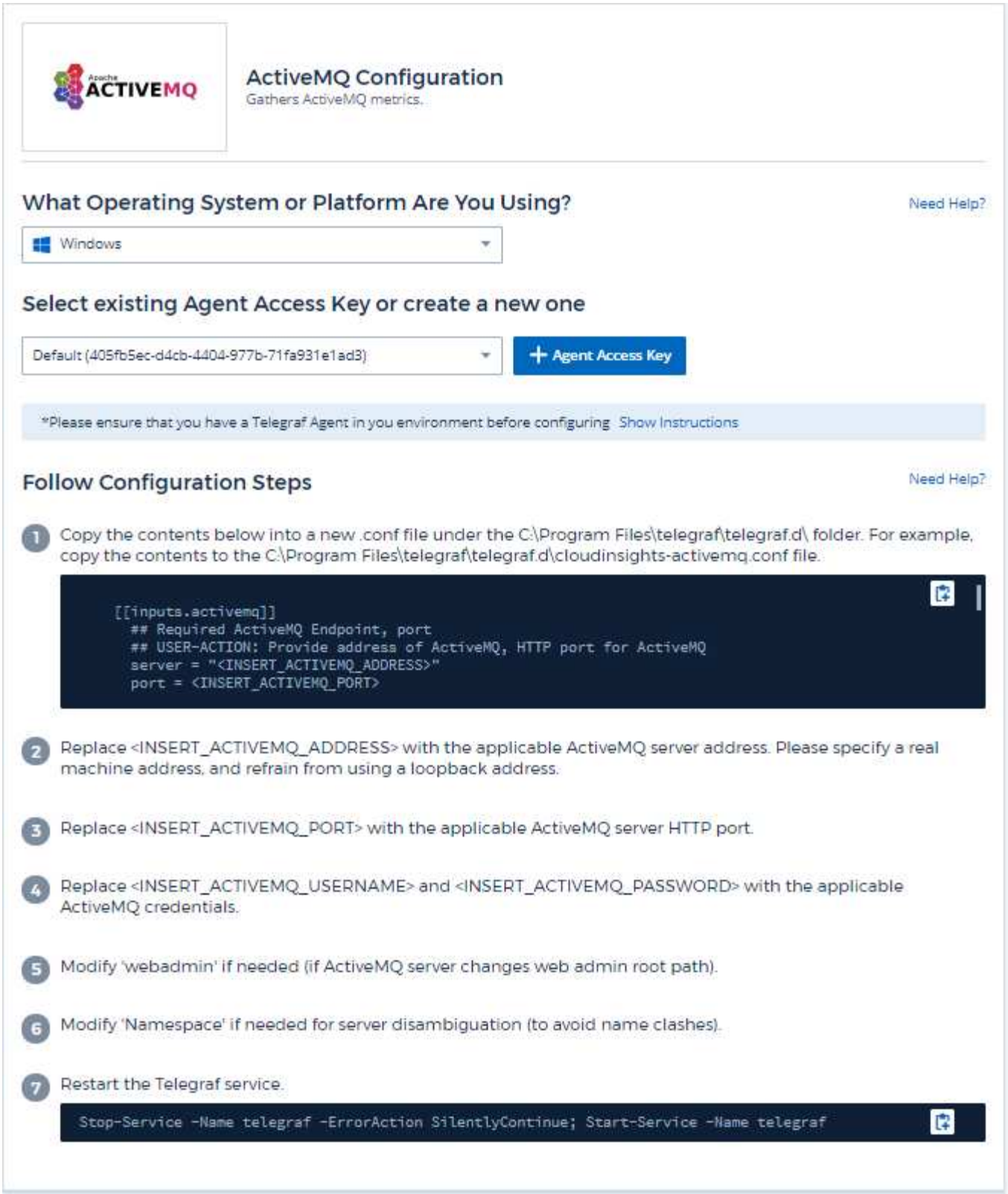
Data Infrastructure Insights verwendet diesen Datensammler, um Metriken von ActiveMQ zu sammeln.

Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie ActiveMQ.

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

2. Wenn Sie noch keinen Agenten für die Sammlung installiert haben oder einen Agenten für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das"Agenteninstallation" Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel zur Verwendung mit diesem Datensammler aus. Sie können einen neuen Agentenzugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agentenzugriffsschlüssel** klicken. Best Practice: Verwenden Sie nur dann einen anderen Agent-Zugriffsschlüssel, wenn Sie Datensammler beispielsweise nach Betriebssystem/Plattform gruppieren möchten.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen variieren je nach Art des Betriebssystems oder der Plattform, die Sie zum Sammeln von Daten verwenden.



Aufstellen

Informationen finden Sie im "ActiveMQ-Dokumentation"

Objekte und Zähler

Die folgenden Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Merkmale:	Datenpunkte:
ActiveMQ-Warteschlange	Namespace-Warteschlangen-Port-Server	Knotenname Knoten-IP Knoten-UUID	Anzahl der Verbraucher Anzahl der Dequeues Anzahl der Enqueues Warteschlangengröße
ActiveMQ-Abonnent	Client-ID Verbindungs-ID Port Server-Namespace	Ist aktiv Zielknotenname Knoten-IP Knoten-UUID Knoten-Betriebssystem-Selektor Abonnement	Anzahl der aus der Warteschlange entfernten Aufgaben Anzahl der versendeten Aufgaben Warteschlangengröße Anzahl der in die Warteschlange entfernten Aufgaben Größe der ausstehenden Warteschlange
ActiveMQ-Thema	Thema Port Server Namespace	Knotenname Knoten-IP Knoten-UUID Knoten-Betriebssystem	Anzahl der Verbraucher Anzahl der Dequeues Anzahl der Enqueues Anzahl der Größe

Fehlerbehebung

Weitere Informationen finden Sie in der"Support" Seite.

Apache-Datensammler

Dieser Datensammler ermöglicht das Sammeln von Daten von Apache-Servern auf Ihrem Mandanten.

Voraussetzungen

- Sie müssen Ihren Apache HTTP-Server eingerichtet und ordnungsgemäß ausgeführt haben
- Sie müssen über Sudo- oder Administratorberechtigungen auf Ihrem Agent-Host/Ihrer VM verfügen
- Normalerweise ist das Apache-Modul *mod_status* 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 Ihres Servers finden Sie in der Apache-Moduldokumentation: https://httpd.apache.org/docs/2.4/mod/mod_status.html#enable

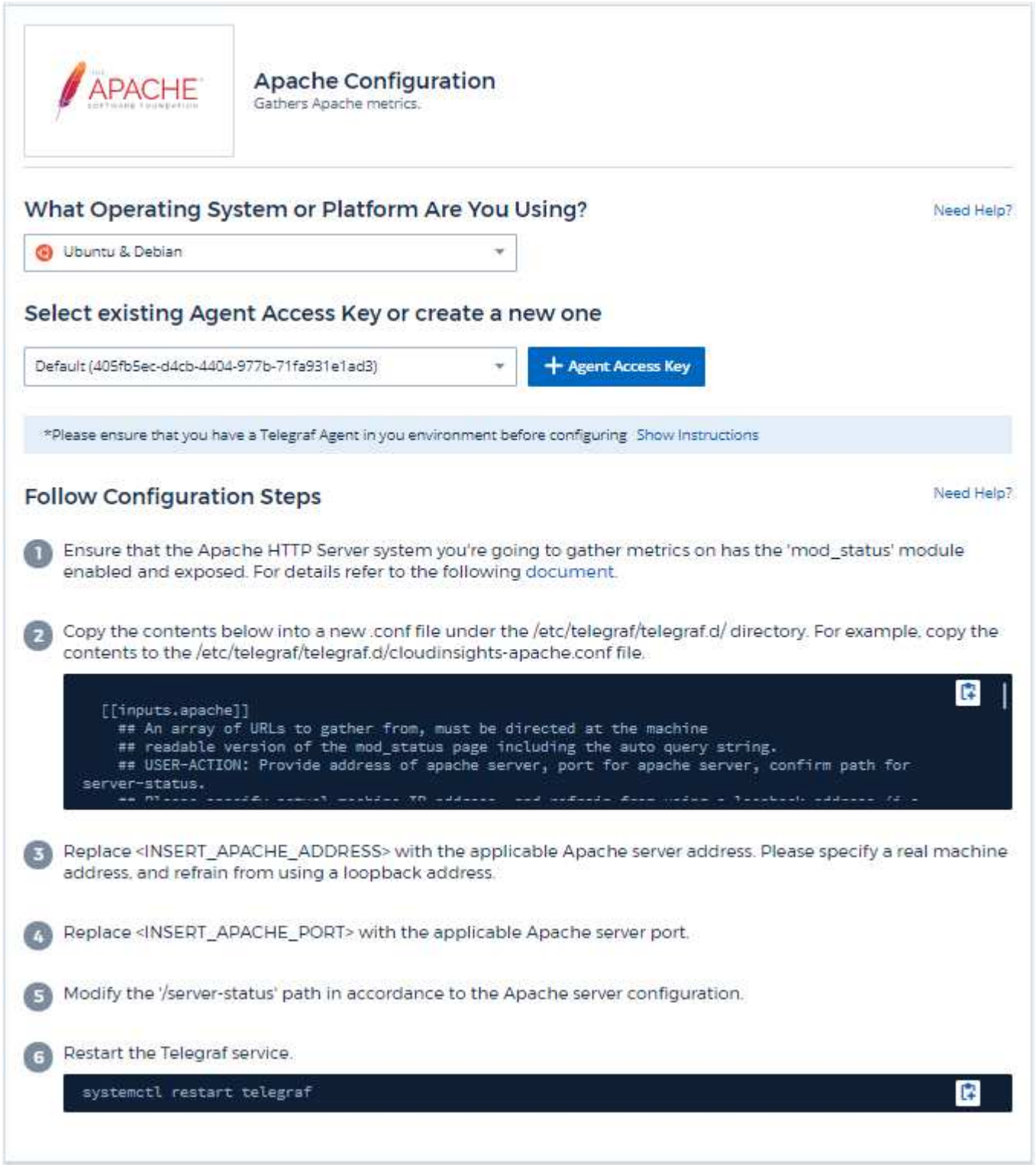
Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie Apache.

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

2. Wenn Sie noch keinen Agenten für die Sammlung installiert haben oder einen Agenten für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das"Agenteninstallation" Anweisungen.

3. Wählen Sie den Agent-Zugriffsschlüssel zur Verwendung mit diesem Datensammler aus. Sie können einen neuen Agentenzugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agentenzugriffsschlüssel** klicken. Best Practice: Verwenden Sie nur dann einen anderen Agent-Zugriffsschlüssel, wenn Sie Datensammler beispielsweise nach Betriebssystem/Plattform gruppieren möchten.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen variieren je nach Art des Betriebssystems oder der Plattform, die Sie zum Sammeln von Daten verwenden.



Aufstellen

Das Plugin von Telegraf für den HTTP-Server von Apache erfordert die Aktivierung des Moduls „mod_status“. Wenn dies aktiviert ist, stellt der HTTP-Server von Apache einen HTML-Endpunkt bereit, der in Ihrem Browser angezeigt oder zum Extrahieren des Status der gesamten HTTP-Serverkonfiguration von Apache verwendet werden kann.

Kompatibilität:

Die Konfiguration wurde für Apaches HTTP-Server Version 2.4.38 entwickelt.

Aktivieren von mod_status:

Das Aktivieren und Freigeben der „mod_status“-Module umfasst zwei Schritte:

- Aktivierungsmodul
- Statistiken aus dem Modul anzeigen

Aktivierungsmodul:

Das Laden der Module wird durch die Konfigurationsdatei unter „/usr/local/apache/conf/httpd.conf“ gesteuert. Bearbeiten Sie die Konfigurationsdatei und entfernen Sie die Kommentarzeichen aus den folgenden Zeilen:

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

Statistiken aus dem Modul anzeigen:

Die Offenlegung von „mod_status“ wird durch die Konfigurationsdatei unter „/usr/local/apache2/conf/extra/httpd-info.conf“ gesteuert. Stellen Sie sicher, dass die Konfigurationsdatei Folgendes enthält (zumindest andere Anweisungen werden dort vorhanden sein):

```
# 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
```

Ausführliche Anweisungen zum Modul „mod_status“ finden Sie im"Apache-Dokumentation"

Objekte und Zähler

Die folgenden Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Merkmale:	Datenpunkte:
Apache	Namespace-Server	Knoten-IP Knotenname Port Übergeordneter Server Konfigurationsgenerierung Übergeordneter Server MPM-Generierung Server-Betriebszeit wird gestoppt	Beschäftigte Worker Bytes pro Anfrage Bytes pro Sekunde CPU-Kinder System-CPU-Kinder Benutzer-CPU-Last CPU-System-CPU-Benutzer Asynchrone Verbindungen Schließende asynchrone Verbindungen Asynchrone Keep-Alive-Verbindungen Schreibende Verbindungen Gesamtdauer pro Anfrage Inaktive Worker Durchschnittliche Auslastung (letzte 1 Min.) Durchschnittliche Auslastung (letzte 15 Min.) Durchschnittliche Auslastung (letzte 5 Min.) Prozesse Anfragen pro Sekunde Gesamtzugriffe Gesamtdauer Gesamt-KByte Anzeigetafel Anzeigetafel wird geschlossen Anzeigetafel DNS-Lookups Anzeigetafel wird beendet Anzeigetafel Anzeigetafel Leerlaufbereinigung Anzeigetafel Keep-Alive Anzeigetafel wird protokolliert Anzeigetafel geöffnet Anzeigetafel liest Anzeigetafel sendet Anzeigetafel startet Anzeigetafel wartet

Fehlerbehebung

Weitere Informationen finden Sie in der"Support" Seite.

Konsul-Datensammler

Data Infrastructure Insights verwendet diesen Datensammler, um Metriken von Consul zu sammeln.

Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie Konsul.

   Wenn Sie keinen Agenten für die Sammlung konfiguriert haben, werden Sie aufgefordert,"Installieren eines Agenten" auf Ihrem Mieter.

   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 Consul-Konfigurationsbildschirm, um den Datensammler zu konfigurieren. Die Anweisungen variieren je nach Art des Betriebssystems oder der Plattform, die Sie zum Sammeln von Daten verwenden.

Aufstellen

Informationen finden Sie im"Konsuldokumentation" .

Objekte und Zähler für Konsul

Die folgenden Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Merkmale:	Datenpunkte:
Konsul	Namespace-Check-ID-Dienstknoten	Knoten-IP Knoten-Betriebssystem Knoten-UUID Knotenname Dienstname Name prüfen Dienst-ID Status	Warnung vor kritischem Überholen

Fehlerbehebung

Weitere Informationen finden Sie in der"Support" Seite.

Couchbase-Datensammler

Data Infrastructure Insights verwendet diesen Datensammler, um Metriken von Couchbase zu sammeln.

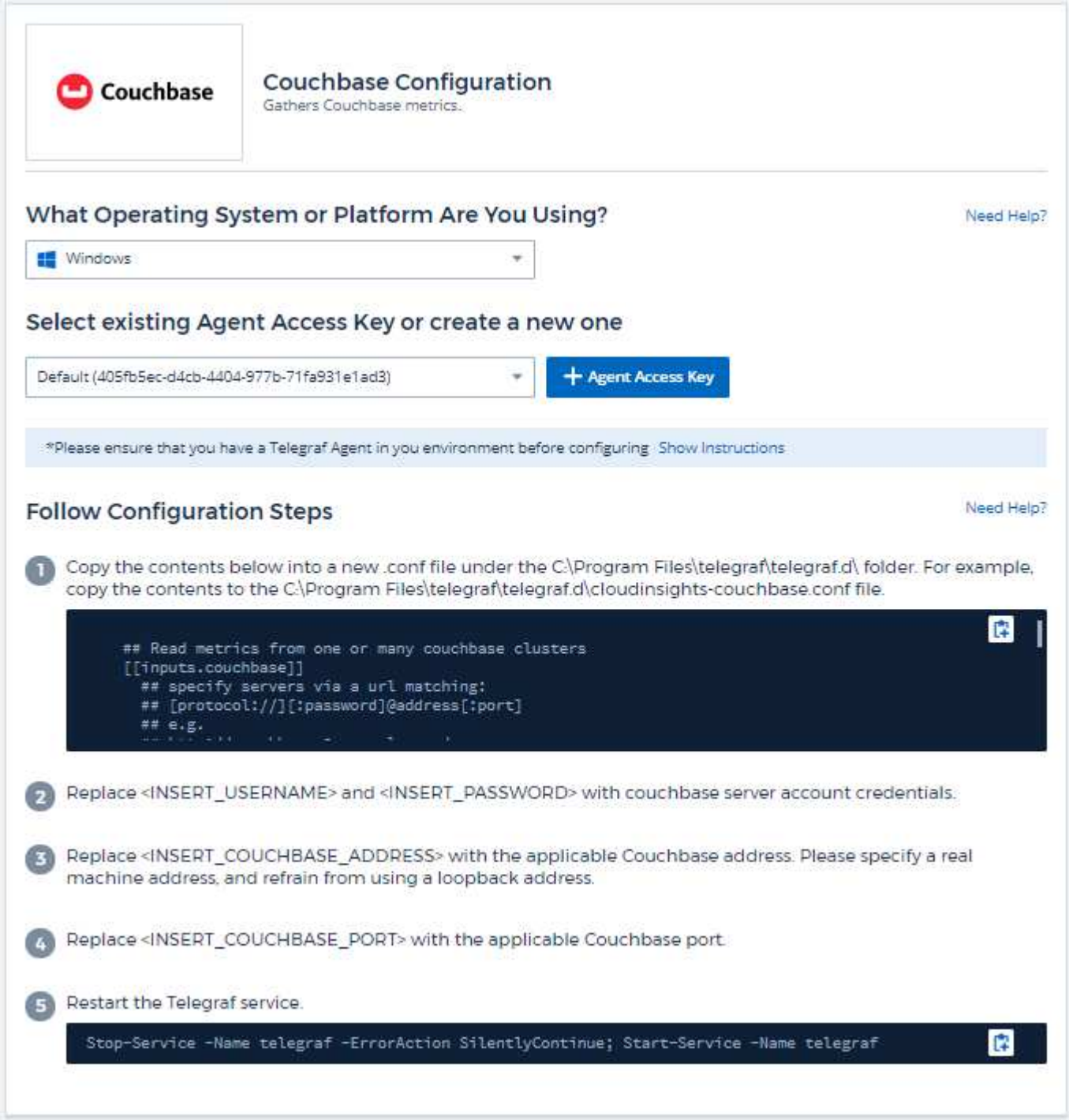
Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie Couchbase.

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

2. Wenn Sie noch keinen Agenten für die Sammlung installiert haben oder einen Agenten für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das"Agenteninstallation" Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel zur Verwendung mit diesem Datensammler aus. Sie können einen neuen Agentenzugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agentenzugriffsschlüssel** klicken. Best Practice: Verwenden Sie nur dann einen anderen Agent-Zugriffsschlüssel, wenn Sie Datensammler beispielsweise nach Betriebssystem/Plattform gruppieren möchten.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen

variieren je nach Art des Betriebssystems oder der Plattform, die Sie zum Sammeln von Daten verwenden.



Aufstellen

Informationen finden Sie im"Couchbase-Dokumentation" .

Objekte und Zähler

Die folgenden Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Merkmale:	Datenpunkte:
Couchbase-Knoten	Namespace-Cluster Couchbase-Knoten-Hostname	Knotenname Knoten-IP	Speicher Freier Speicher Gesamt
Couchbase-Eimer	Namespace-Bucket-Cluster	Knotenname Knoten-IP	Verwendete Daten Datenabrufe Verwendete Festplatte Anzahl der Elemente Verwendeter Speicher Vorgänge pro Sekunde Verwendetes Kontingent

Fehlerbehebung

Weitere Informationen finden Sie in der"Support" Seite.

CouchDB-Datensammler

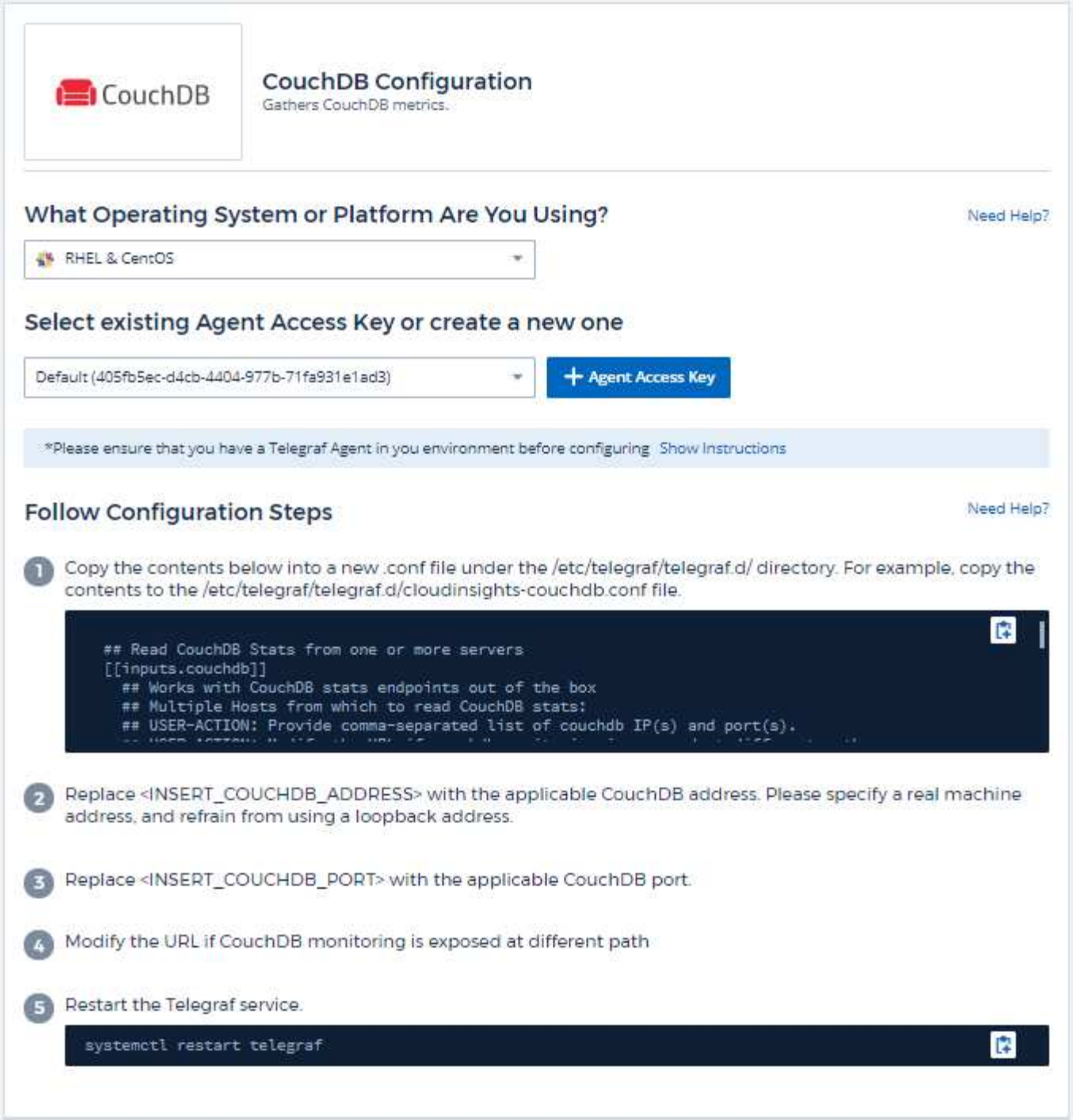
Data Infrastructure Insights verwendet diesen Datensammler, um Metriken von CouchDB zu sammeln.

Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie CouchDB.

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

2. Wenn Sie noch keinen Agenten für die Sammlung installiert haben oder einen Agenten für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das"Agenteninstallation" Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel zur Verwendung mit diesem Datensammler aus. Sie können einen neuen Agentenzugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agentenzugriffsschlüssel** klicken. Best Practice: Verwenden Sie nur dann einen anderen Agent-Zugriffsschlüssel, wenn Sie Datensammler beispielsweise nach Betriebssystem/Plattform gruppieren möchten.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen variieren je nach Art des Betriebssystems oder der Plattform, die Sie zum Sammeln von Daten verwenden.



Aufstellen

Informationen finden Sie im"CouchDB-Dokumentation" .

Objekte und Zähler

Die folgenden Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Merkmale:	Datenpunkte:
CouchDB	Namespace-Server	Knotenname Knoten-IP	Authentifizierungscache-Treffer Authentifizierungscache-Fehler Datenbank-Lesevorgänge Datenbank-Schreibvorgänge Datenbanken öffnen Betriebssystemdateien öffnen Max. Anforderungszeit Min. Anforderungszeit HTTP-Anforderungsmethoden HTTP-Anforderungsmethoden kopieren HTTP-Anforderungsmethoden löschen HTTP-Anforderungsmethoden abrufen HTTP-Anforderungsmethoden headen HTTP-Anforderungsmethoden posten HTTP-Anforderungsmethoden setzen Statuscodes 200 Statuscodes 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 in der"Support" Seite.

Docker-Datensammler

Data Infrastructure Insights verwendet diesen Datensammler, um Metriken von Docker zu sammeln.

Installation

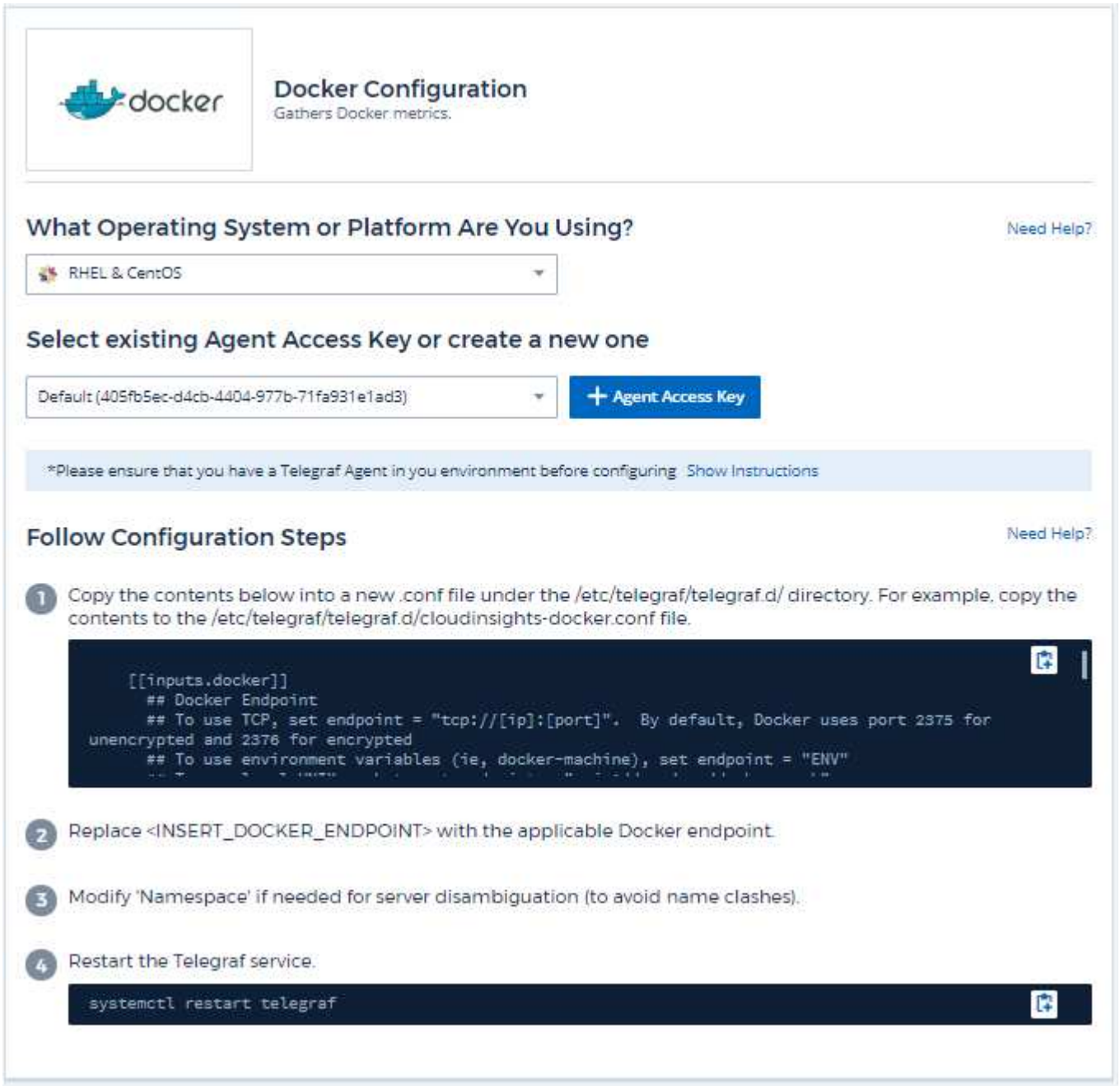
1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie Docker.

   Wenn Sie keinen Agenten für die Sammlung konfiguriert haben, werden Sie aufgefordert,"Installieren eines

Agenten" auf Ihrem Mieter.

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 Docker-Konfigurationsbildschirm, um den Datensammler zu konfigurieren. Die Anweisungen variieren je nach Art des Betriebssystems oder der Plattform, die Sie zum Sammeln von Daten verwenden.



Aufstellen

Das Telegraf-Eingabe-Plugin für Docker sammelt Metriken über einen angegebenen UNIX-Socket oder einen TCP-Endpunkt.

Kompatibilität

Die Konfiguration wurde für Docker Version 1.12.6 entwickelt.

Einrichten

Zugriff auf Docker über einen UNIX-Socket

Wenn der Telegraf-Agent auf Baremetal ausgeführt wird, 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 frei, indem Sie den Socket als Volume in den Pod einbinden und dieses Volume dann in /var/run/docker.sock mounten.  Fügen Sie der PodSpec beispielsweise 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 das für die Kubernetes-Plattform bereitgestellte Data Infrastructure Insights -Installationsprogramm diese Zuordnung automatisch vornimmt.

Zugriff auf Docker über einen TCP-Endpunkt

Standardmäßig verwendet Docker Port 2375 für unverschlüsselten Zugriff und Port 2376 für verschlüsselten Zugriff.

Objekte und Zähler

Die folgenden Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Merkmale:	Datenpunkte:
Docker-Engine	Namespace Docker Engine	Knotenname Knoten-IP Knoten-UUID Knoten-Betriebssystem Kubernetes-Cluster Docker-Version Einheit	Speichercontainer Container Angehaltene Container Laufende Container Gestoppte CPUs Go-Routinen Bilder Listener Verwendete Ereignisse Datei-Deskriptoren Daten Verfügbare Daten Gesamt verwendete Daten Metadaten Verfügbare Metadaten Gesamt verwendete Metadaten Pool-Blockgröße

Objekt:	Kennungen:	Merkmale:	Datenpunkte:
Docker-Container	Namespace Containername Docker Engine	Kubernetes-Container-Hash Kubernetes-Container-Ports Kubernetes-Container-Neustart-Zähler Kubernetes-Container-Beendigungsnachrichtenpfad Kubernetes-Container-Beendigungsnachrichtenrichtlinie Kubernetes-Pod-Beendigungsfrist Container-Image Container-Status Container-Version Knotenname Kubernetes-Container-Protokollpfad Kubernetes-Container-Name Kubernetes-Docker-Typ Kubernetes-Pod-Name Kubernetes-Pod-Namespace Kubernetes-Pod-UID Kubernetes-Sandbox-ID Knoten-IP Knoten-UUID Docker-Version Kubernetes-E/A-Konfiguration gesehen Kubernetes-E/A-Konfigurationsquelle OpenShift-E/A-SCC Kubernetes-Beschreibung Kubernetes-Anzeigename OpenShift-Tags Kompose-Service Pod-Vorlagen-Hash Controller-Revisions-Hash Pod-Vorlagengenerierung Lizenzschema Erstellungsdatum Schema-Lizenz Schemaname Schema-URL Schema-VCS-URL Schemaanbieter Schemaversion Schema Schemaversionsbetreuer Kunde Pod Kubernetes StatefulSet Pod-Name Mandant Webkonsolen-Architektur Autoritative Quell-URL Erstellungsdatum RH-Build-Host RH-Komponente Verteilungsbereich Installation Release-	Aktiver anonymer Speicher Aktiver Dateispeicher Cache-Speicher Hierarchische Grenze Inaktiver anonymer Speicher Inaktive Dateispeichergrenze Zugeordneter Dateispeicher Maximale Speicherauslastung Speicherseitenfehler Schwerwiegender Seitenfehler Eingelagerter Speicher Ausgelagerter Speicher Ausgelagerter Speicher Größe des residenten Satzes Riesiger residenter Satz Größe des residenten Satzes Gesamter aktiver anonymer Speicher Gesamter aktiver Dateispeicher Gesamter Cache-Speicher Gesamter inaktiver anonymer Speicher Gesamter inaktiver Dateispeicher Gesamter zugeordneter Dateispeicher Gesamter Seitenfehler Speicher Gesamter schwerwiegender Seitenfehler Gesamter ausgelagerter Speicher Gesamter ausgelagerter Speicher Gesamte Größe des residenten Satzes Gesamter residenter Satz Größe des residenten Satzes Gesamter nicht auslagerbarer Speicher Nicht auslagerbarer Speichernutzung Speichernutzung in Prozent Exit-Code OOM beendet PID gestartet bei Failing Streak

Objekt:	Kennungen:	Merkmale:	Datenpunkte:
Docker-Container-Block-IO	Namespace Containername Gerät Docker Engine	Kubernetes-Container-Hash Kubernetes-Container-Ports Anzahl der Neustarts von Kubernetes-Containern Pfad der Kubernetes-Container-Beendigungsnachrichten Richtlinie für Kubernetes-Container-Beendigungsnachrichten Karenzzeit für Kubernetes-Pod-Beendigung Container-Image Container-Status Container-Version Knotenname Kubernetes-Container-Protokollpfad Kubernetes-Container-Name Kubernetes-Docker-Typ Kubernetes-Pod-Name Kubernetes-Pod-Namespace Kubernetes-Pod-UID Kubernetes-Sandbox-ID Knoten-IP Knoten-UUID Docker-Version Gesehene Kubernetes-Konfiguration Kubernetes-Konfigurationsquelle OpenShift SCC Kubernetes-Beschreibung Kubernetes-Anzeigename OpenShift-Tags Schema Schemaversion Pod-Vorlagen-Hash Controller-Revisions-Hash Pod-Vorlagengenerierung Kompose-Dienst Schema-Erstellungsdatum Schema-Lizenz Schemaname Schemaanbieter Kunden-Pod Kubernetes-StatefulSet Pod-Name Mandant-Webkonsole Erstellungsdatum Lizenzanbieter Architektur Autoritative Quell-URL RH-Build-Host RH-Komponente Verteilungsbereich Installationsbetreuer Release-Ausführungszusammenfa	IO-Service-Bytes rekursiv Asynchron IO-Service-Bytes rekursiv Lesen IO-Service-Bytes rekursiv Sync IO-Service-Bytes rekursiv gesamt IO-Service-Bytes rekursiv Schreiben IO bedient rekursiv Asynchron IO bedient rekursiv Lesen IO bedient rekursiv Sync IO bedient rekursiv gesamt IO bedient rekursiv Schreiben

Objekt:	Kennungen:	Merkmale:	Datenpunkte:
Docker-Container-Netzwerk	Namespace Containername Netzwerk Docker Engine	Container-Image Container-Status Container-Version Knotenname Knoten-IP Knoten-UUID Knoten-Betriebssystem K8s-Cluster Docker-Version Container-ID	RX Verloren RX Bytes RX Fehler RX Pakete TX Verloren TX Bytes TX Fehler TX Pakete

Objekt:	Kennungen:	Merkmale:	Datenpunkte:
Docker-Container-CPU	Namespace Containername CPU Docker Engine	Kubernetes-Container-Hash Kubernetes-Container-Ports Kubernetes-Container-Neustart-Zähler Kubernetes-Container-Beendigungsnachrichtenpfad Kubernetes-Container-Beendigungsnachrichtenrichtlinie Kubernetes-Pod-Beendigungsfrist Kubernetes-Konfiguration gesehen Kubernetes-Konfigurationsquelle OpenShift SCC-Container-Image Containerstatus Containerversion Knotenname Kubernetes-Container-Protokollpfad Kubernetes-Containername Kubernetes-Docker-Typ Kubernetes-Pod-Name Kubernetes-Pod-Namespace Kubernetes-Pod-UID Kubernetes-Sandbox-ID Knoten-IP Knoten-UUID Knoten-Betriebssystem Kubernetes-Cluster Docker-Version Kubernetes-Beschreibung Kubernetes-Anzeigename OpenShift-Tags Schemaversion Pod-Vorlagen-Hash Controller-Revisions-Hash Pod-Vorlagengenerierung Kompose-Dienst Schema-Erstellungsdatum Schema-Lizenz Schemaname Schemaanbieter Kunden-Pod Kubernetes-StatefulSet Pod-Name Mandant-Webkonsole Erstellungsdatum Lizenzanbieter Architektur Autoritative Quell-URL RH-Build-Host RH-Komponente Verteilungsbereich Installationsbetreuer Release-	Drosselungsperioden Drosselung Drosselungsperioden Drosselungszeit Drosselungszeit Nutzung im Kernelmodus Nutzung im Benutzermodus Nutzung in Prozent Nutzung Systemnutzung gesamt

Fehlerbehebung

Problem:	Versuchen Sie Folgendes:
Ich sehe meine Docker-Metriken nicht in Data Infrastructure Insights, nachdem ich die Anweisungen auf der Konfigurationsseite befolgt habe.	Überprüfen Sie die Protokolle des Telegraf-Agenten, um zu sehen, ob der folgende Fehler gemeldet wird: E! Fehler im Plugin [inputs.docker]: Beim Versuch, eine Verbindung zum Docker-Daemon-Socket herzustellen, wurde die Berechtigung verweigert. Wenn dies der Fall ist, ergreifen Sie die erforderlichen Maßnahmen, um dem Telegraf-Agenten Zugriff auf den Docker-Unix-Socket zu gewähren, wie oben angegeben.

Weitere Informationen finden Sie in der"Support" Seite.

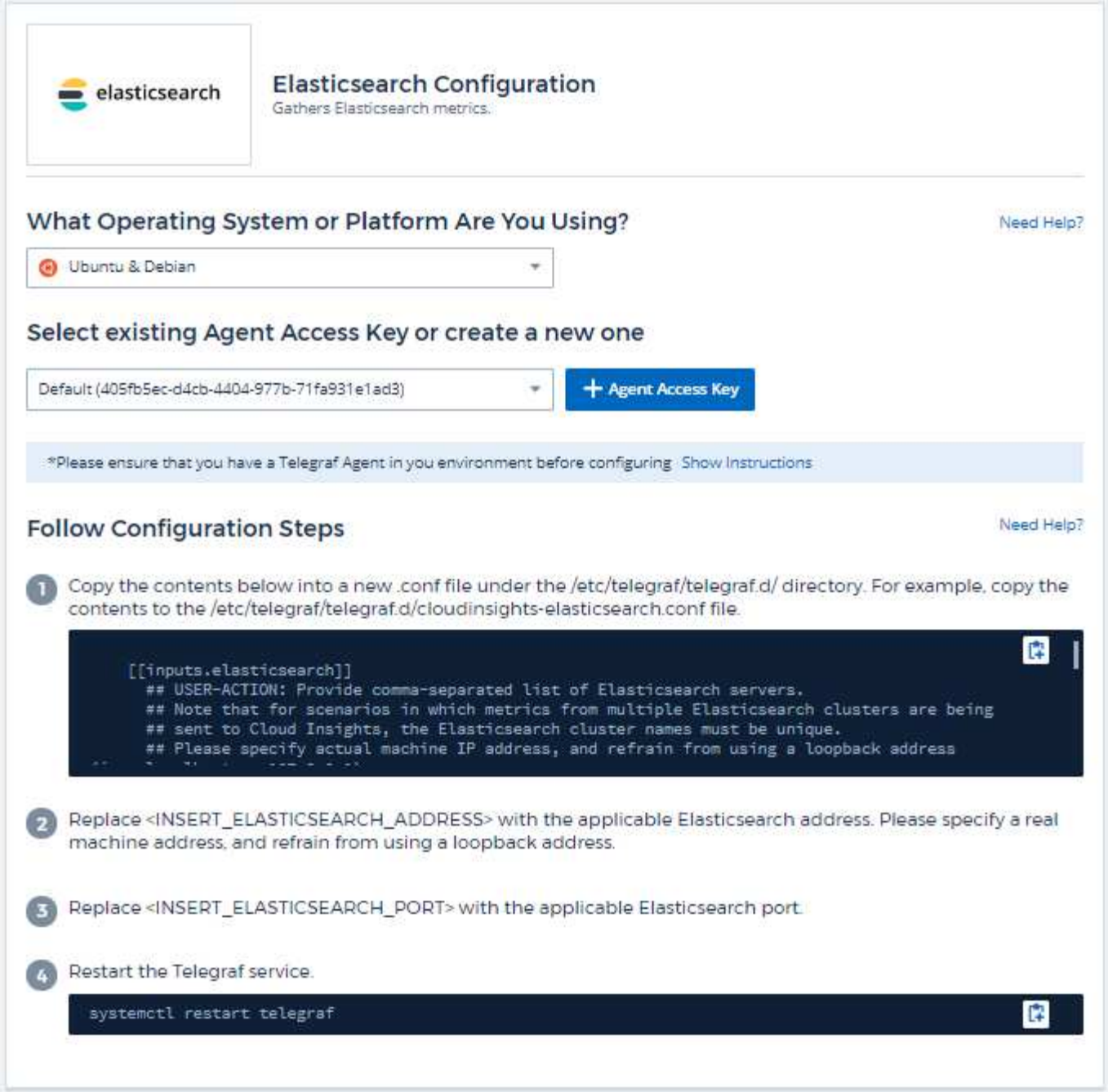
Elasticsearch-Datensammler

Data Infrastructure Insights verwendet diesen Datensammler, um Metriken von Elasticsearch zu sammeln.

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie Elasticsearch.

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

2. Wenn Sie noch keinen Agenten für die Sammlung installiert haben oder einen Agenten für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das"Agenteninstallation" Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel zur Verwendung mit diesem Datensammler aus. Sie können einen neuen Agentenzugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agentenzugriffsschlüssel** klicken. Best Practice: Verwenden Sie nur dann einen anderen Agent-Zugriffsschlüssel, wenn Sie Datensammler beispielsweise nach Betriebssystem/Plattform gruppieren möchten.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen variieren je nach Art des Betriebssystems oder der Plattform, die Sie zum Sammeln von Daten verwenden.



Aufstellen

Informationen finden Sie im"Elasticsearch-Dokumentation" .

Objekte und Zähler

Die folgenden Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Merkmale:
Elasticsearch-Cluster	Namespace-Cluster	Knoten-IP Knotenname Clusterstatus
Elasticsearch-Knoten	Namespace-Cluster ES-Knoten-ID ES-Knoten-IP ES-Knoten	Zonen-ID

Fehlerbehebung

Weitere Informationen finden Sie in der"Support" Seite.

Flink-Datensammler

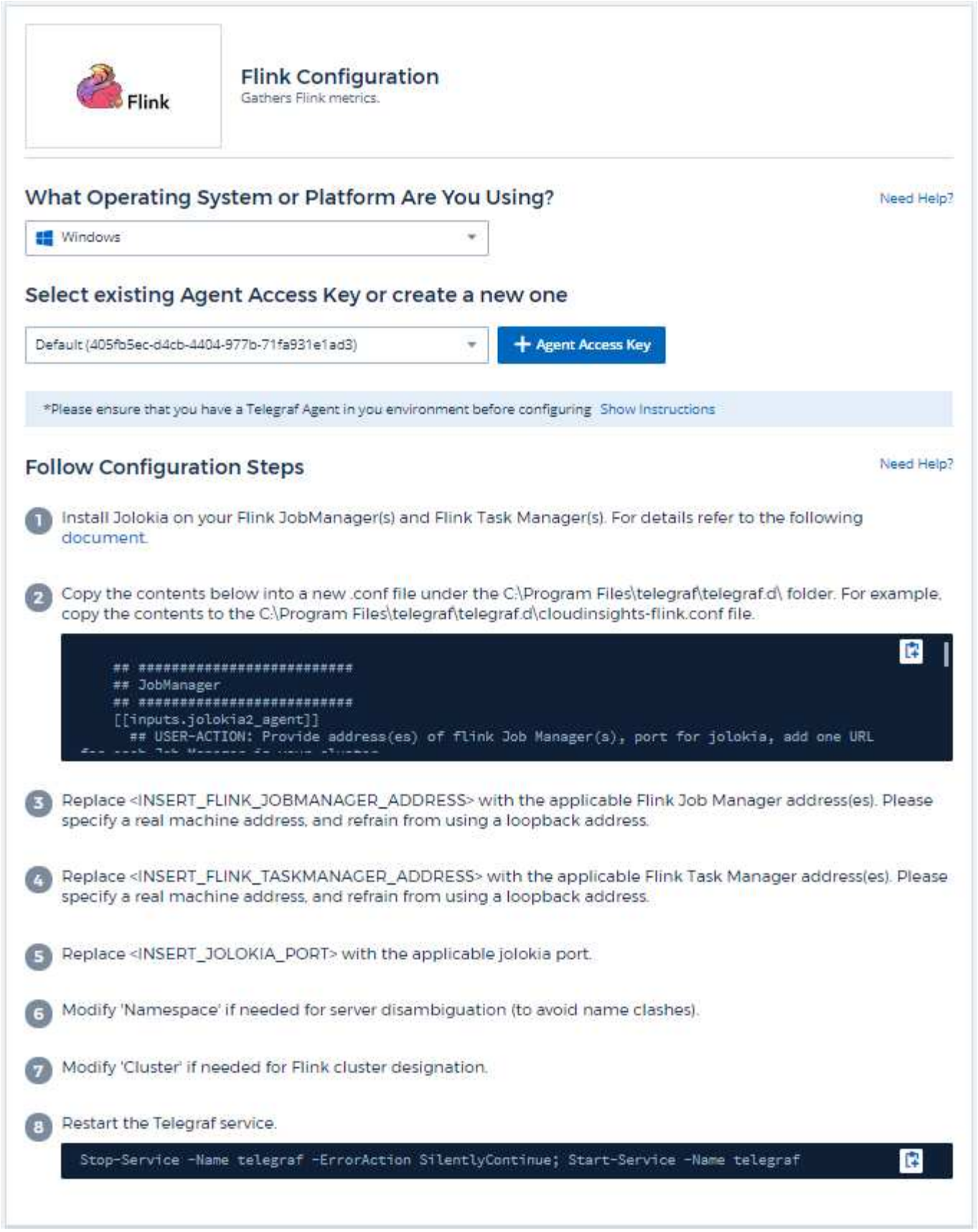
Data Infrastructure Insights verwendet diesen Datensammler, um Metriken von Flink zu sammeln.

Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie Flink.

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

2. Wenn Sie noch keinen Agenten für die Sammlung installiert haben oder einen Agenten für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das"Agenteninstallation" Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel zur Verwendung mit diesem Datensammler aus. Sie können einen neuen Agentenzugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agentenzugriffsschlüssel** klicken. Best Practice: Verwenden Sie nur dann einen anderen Agent-Zugriffsschlüssel, wenn Sie Datensammler beispielsweise nach Betriebssystem/Plattform gruppieren möchten.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen variieren je nach Art des Betriebssystems oder der Plattform, die Sie zum Sammeln von Daten verwenden.



Aufstellen

Eine vollständige Flink-Bereitstellung umfasst die folgenden Komponenten:

JobManager: Das Flink-Primärsystem. Koordiniert eine Reihe von TaskManagern. In einer Hochverfügbarkeitskonfiguration verfügt das System über mehr als einen JobManager. TaskManager: Hier werden Flink-Operatoren ausgeführt. Das Flink-Plugin basiert auf dem Jolokia-Plugin von Telegraf. Um beispielsweise Informationen von allen Flink-Komponenten zu sammeln, muss JMX auf allen Komponenten konfiguriert und über Jolokia verfügbar gemacht werden.

Kompatibilität

Die Konfiguration wurde für Flink Version 1.7.0 entwickelt.

Einrichten

Jolokia Agent Jar

Für alle Einzelkomponenten muss eine Version der Jolokia-Agent-JAR-Datei heruntergeladen werden. Die getestete Version war"Jolokia-Agent 1.6.0" .

Die folgenden Anweisungen gehen davon aus, dass die heruntergeladene JAR-Datei (jolokia-jvm-1.6.0-agent.jar) am Speicherort „/opt/flink/lib/“ abgelegt ist.

JobManager

Um JobManager so zu konfigurieren, dass die Jolokia-API verfügbar gemacht 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 für Jolokia einen anderen Port (8778) wählen.  Wenn Sie eine
interne IP haben, auf die Sie Jolokia sperren möchten, können Sie die
„Catch-All“-IP 0.0.0.0 durch Ihre eigene IP ersetzen.  Beachten Sie, dass
diese IP vom Telegraf-Plugin aus zugänglich sein muss.
```

Task-Manager

Um TaskManager so zu konfigurieren, dass sie die Jolokia-API verfügbar machen, 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 für Jolokia einen anderen Port (8778) wählen.  Wenn Sie eine
interne IP haben, auf die Sie Jolokia sperren möchten, können Sie die
„Catch-All“-IP 0.0.0.0 durch Ihre eigene IP ersetzen.  Beachten Sie, dass
diese IP vom Telegraf-Plugin aus zugänglich sein muss.
```

Objekte und Zähler

Die folgenden Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Merkmale:	Datenpunkte:
Flink Task-Manager	Cluster-Namespace-Server	Knotenname Task-Manager-ID Knoten-IP	Verfügbare Netzwerkspeichersegmente Netzwerkspeichersegmente gesamt Garbage Collection PS MarkSweep-Anzahl Garbage Collection PS MarkSweep-Zeit Garbage Collection PS Scavenge-Anzahl Garbage Collection PS Scavenge-Zeit Heap-Speicher zugesichert Heap-Speicher initialisieren Heap-Speicher max. Verwendeter Heap-Speicher Thread-Anzahl Daemon-Threads Spitzen-Thread-Anzahl Thread-Anzahl insgesamt gestartet
Flink Job	Job-ID des Cluster-Namespace-Servers	Knotenname Jobname Knoten-IP Letzter Prüfpunkt Externer Pfad Neustartzeit	Ausfallzeit Vollständige Neustarts Ausrichtung des letzten Prüfpunkts Gepuffert Dauer des letzten Prüfpunkts Größe des letzten Prüfpunkts Anzahl abgeschlossener Prüfpunkte Anzahl fehlgeschlagener Prüfpunkte Anzahl laufender Prüfpunkte Anzahl Prüfpunkte Betriebszeit

Objekt:	Kennungen:	Merkmale:	Datenpunkte:
Flink Job Manager	Cluster-Namespace-Server	Knotenname Knoten-IP	Garbage Collection PS MarkSweep-Anzahl Garbage Collection PS MarkSweep-Zeit Garbage Collection PS Scavenge-Anzahl Garbage Collection PS Scavenge-Zeit Heap-Speicher zugesichert Heap-Speicher initialisieren Heap-Speicher max. verwendeter Heap-Speicher Anzahl registrierter Task-Manager Anzahl laufender Jobs Verfügbare Task-Slots Gesamt-Thread-Anzahl Daemon-Thread-Anzahl Spitzen-Thread-Anzahl Threads insgesamt gestartet

Objekt:	Kennungen:	Merkmale:	Datenpunkte:
Flink-Aufgabe	Cluster-Namespace Job-ID Aufgaben-ID	Serverknotenname Jobname Sub-Task-Index Task-Versuchs-ID Task-Versuchsnummer Taskname Task-Manager-ID Knoten-IP Aktuelles Eingabewasserzeichen	Puffer im Pool, Nutzung, Puffer in Warteschlangenlänge, Puffer aus, Pool, Nutzung, Puffer aus, Warteschlangenlänge, Anzahl, Puffer lokal, Anzahl, Puffer lokal pro Sekunde, Anzahl, Puffer lokal pro Sekunde, Rate, Anzahl, Puffer extern, Anzahl, Puffer extern pro Sekunde, Anzahl, Puffer extern pro Sekunde, Anzahl, Puffer extern pro Sekunde, Rate, Anzahl, Puffer extern, Anzahl, Puffer extern pro Sekunde, Anzahl, Puffer extern pro Sekunde, Rate, Anzahl, Bytes lokal, Anzahl, Bytes lokal pro Sekunde, Anzahl, Bytes lokal pro Sekunde, Rate, Anzahl, Bytes lokal pro Sekunde, Rate, Anzahl, Bytes extern, Anzahl, Bytes extern pro Sekunde, Anzahl, Bytes extern pro Sekunde, Rate, Anzahl, Bytes extern pro Sekunde, Anzahl, Bytes extern pro Sekunde, Rate, Anzahl, Datensätze extern, Anzahl, Datensätze extern pro Sekunde, Rate, Anzahl, Datensätze extern, Anzahl, Datensätze extern pro Sekunde, Rate, Anzahl, Datensätze extern pro Sekunde

Objekt:	Kennungen:	Merkmale:	Datenpunkte:
Flink-Task-Operator	Cluster-Namespace Job-ID Operator-ID Aufgaben-ID	Serverknotenname Jobname Operatorname Sub-Task-Index Task-Versuchs-ID Task-Versuchsnummer Taskname Task-Manager-ID Knoten-IP	Aktuelles Eingabe-Wasserzeichen Aktuelles Ausgabe-Wasserzeichen Anzahl Datensätze (ein) Anzahl Datensätze (ein) pro Sekunde Anzahl Datensätze (ein) pro Sekunde Rate Anzahl Datensätze (aus) Anzahl Datensätze (aus) pro Sekunde Anzahl Datensätze (aus) pro Sekunde Rate Anzahl verspätet gelöschte Datensätze Zugewiesene Partitionen Verbrauchte Byte-Rate Commit-Latenz (Durchschnitt) Commit-Latenz (Maximal) Commit-Rate Fehlgeschlagene Commits Erfolgreiche Commits Verbindungsabschlussrate Anzahl Verbindungen Anzahl Verbindungserstellungsrate Anzahl Abruflatenz (Durchschnitt) Max. Abruflatenz Abrufrate (Durchschnitt) Abrufgröße (Maximal) Abrufgröße (Maximal) Abrufdrosselzeit (Durchschnitt) Max. Abrufdrosselzeit Heartbeat-Rate Eingehende Byte-Rate IO-Verhältnis IO-Zeit (Durchschnitt) (ns) IO-Warteverhältnis IO-Wartezeit (Durchschnitt) Join-Rate durchschnittliche Join-Zeit vor dem letzten Heartbeat Netzwerk-IO-Rate Ausgehende Byte-Rate Verbrauchte Datensätze Rate der Datensätze Verzögerung (Maximal) Datensätze pro Anfrage durchschnittliche Anfragerate Anfragegröße durchschnittliche Anfragegröße (Maximal) Antwortrate Auswahlrate

Fehlerbehebung

Weitere Informationen finden Sie in der"Support" Seite.

Hadoop-Datensammler

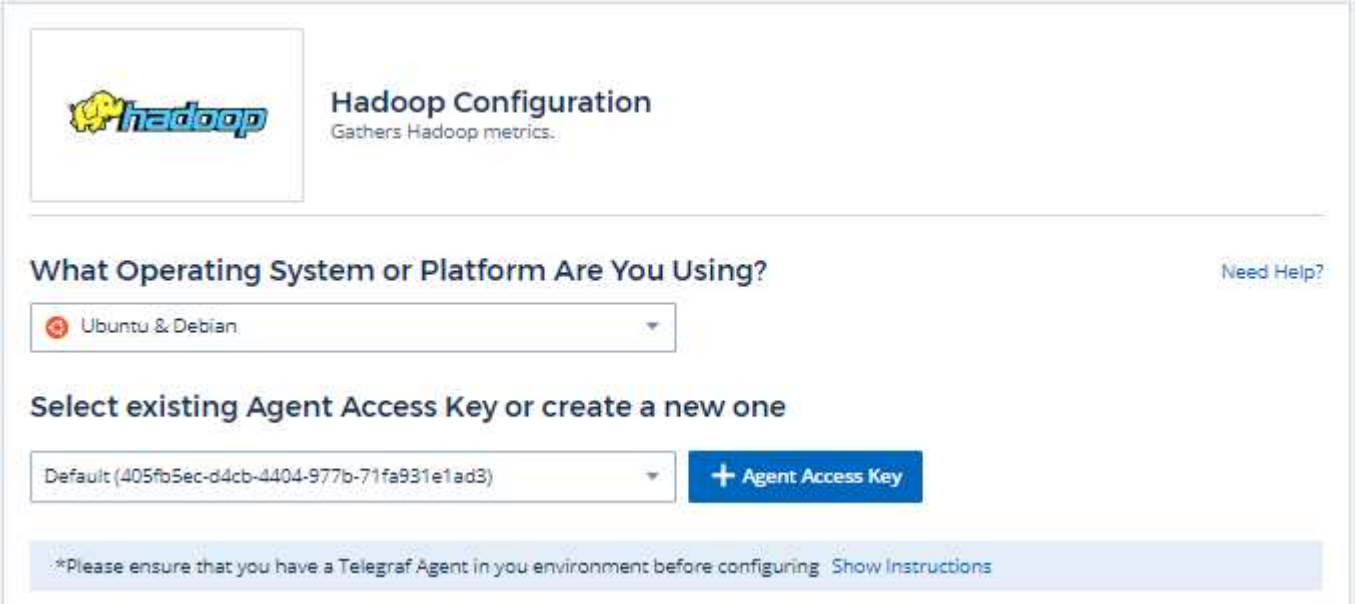
Data Infrastructure Insights verwendet diesen Datensammler, um Metriken von Hadoop zu sammeln.

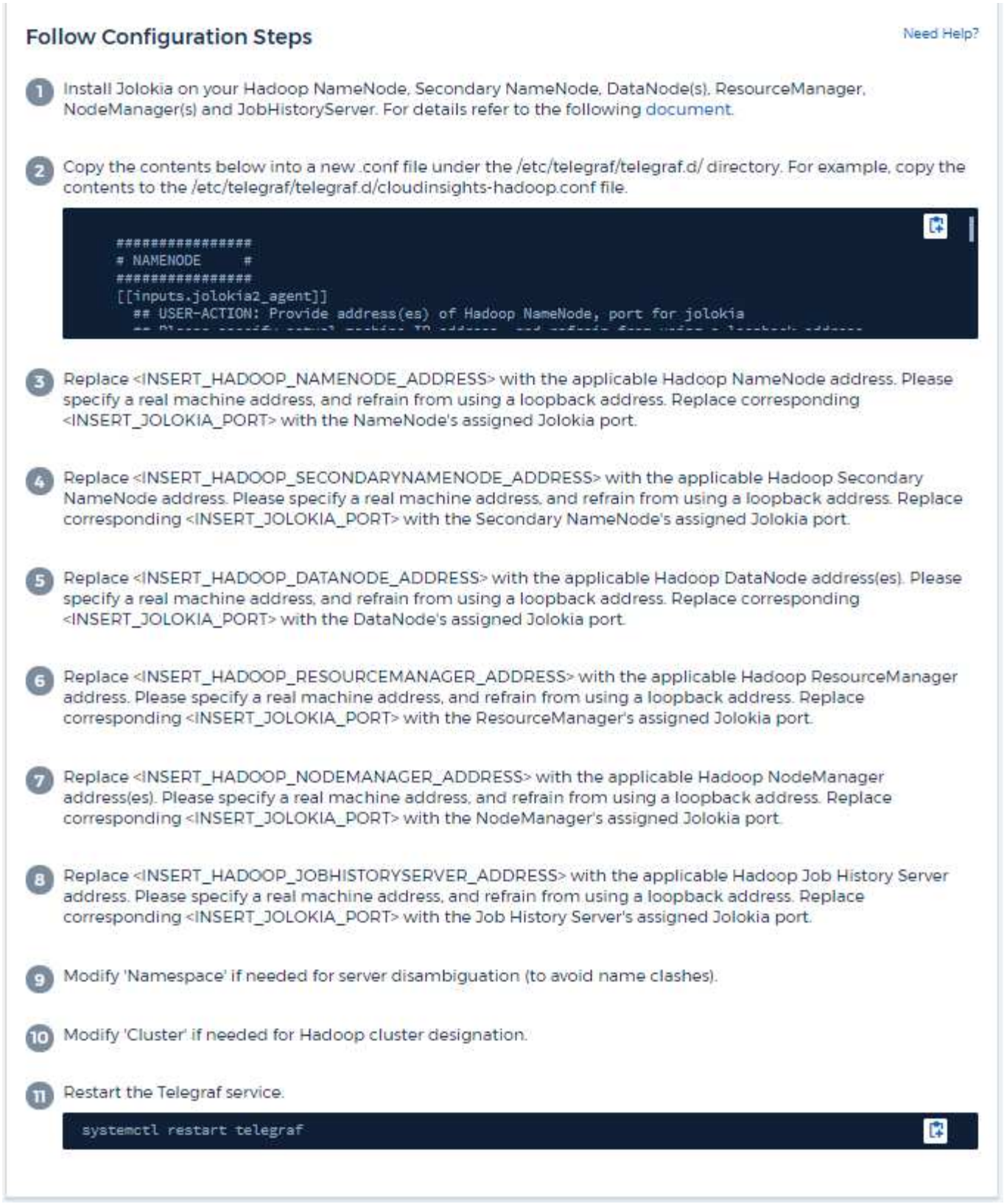
Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie Hadoop.

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

2. Wenn Sie noch keinen Agenten für die Sammlung installiert haben oder einen Agenten für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das"Agenteninstallation" Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel zur Verwendung mit diesem Datensammler aus. Sie können einen neuen Agentenzugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agentenzugriffsschlüssel** klicken. Best Practice: Verwenden Sie nur dann einen anderen Agent-Zugriffsschlüssel, wenn Sie Datensammler beispielsweise nach Betriebssystem/Plattform gruppieren möchten.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen variieren je nach Art des Betriebssystems oder der Plattform, die Sie zum Sammeln von Daten verwenden.





Aufstellen

Eine vollständige Hadoop-Bereitstellung umfasst die folgenden Komponenten:

- NameNode: Das primäre System des Hadoop Distributed File System (HDFS). Koordiniert eine Reihe von DataNodes.

- Sekundärer NameNode: ein Warm-Failover für den Haupt-NameNode. In Hadoop erfolgt die Beförderung zum NameNode nicht automatisch. Der sekundäre NameNode sammelt Informationen vom NameNode, um bei Bedarf für die Beförderung bereit zu sein.
- DataNode: Tatsächlicher Eigentümer der Daten.
- ResourceManager: Das primäre Rechensystem (Yarn). Koordiniert eine Reihe von NodeManagern.
- NodeManager: Die Ressource für die Berechnung. Tatsächlicher Speicherort für die Ausführung von Anwendungen.
- JobHistoryServer: Verantwortlich für die Bearbeitung aller Anfragen zum Jobverlauf.

Das Hadoop-Plugin basiert auf dem Jolokia-Plugin von Telegraf. Um beispielsweise Informationen von allen Hadoop-Komponenten zu sammeln, muss JMX auf allen Komponenten konfiguriert und über Jolokia verfügbar gemacht werden.

Kompatibilität

Die Konfiguration wurde für Hadoop Version 2.9.2 entwickelt.

Einrichten

Jolokia Agent Jar

Für alle Einzelkomponenten muss eine Version der Jolokia-Agent-JAR-Datei heruntergeladen werden. Die getestete Version war"Jolokia-Agent 1.6.0" .

Die folgenden Anweisungen gehen davon aus, dass die heruntergeladene JAR-Datei (jolokia-jvm-1.6.0-agent.jar) am Speicherort „/opt/hadoop/lib/“ abgelegt ist.

NameNode

Um NameNode für die Bereitstellung der Jolokia-API zu konfigurieren, können Sie Folgendes in <HADOOP_HOME>/etc/hadoop/hadoop-env.sh 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 für die Bereitstellung der Jolokia-API zu konfigurieren, 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.
```

Datenknoten

Um die DataNodes so zu konfigurieren, dass sie die Jolokia-API verfügbar machen, 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.
```

Ressourcenmanager

Um den ResourceManager für die Bereitstellung der Jolokia-API zu konfigurieren, 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.
```

Knotenmanager

Um die NodeManager so zu konfigurieren, dass sie die Jolokia-API verfügbar machen, 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.
```

JobHistoryServer

Um den JobHistoryServer für die Bereitstellung der Jolokia-API zu konfigurieren, 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

Die folgenden Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Merkmale:
Sekundärer NameNode von Hadoop	Cluster-Namespace-Server	Knotenname Knoten-IP Kompilierungsinformationen Version
Hadoop NodeManager	Cluster-Namespace-Server	Knotenname Knoten-IP
Hadoop-Ressourcenmanager	Cluster-Namespace-Server	Knotenname Knoten-IP
Hadoop-Datenknoten	Cluster-Namespace-Server	Knotenname Knoten-IP Cluster-ID Version
Hadoop-Namensknoten	Cluster-Namespace-Server	Knotenname Knoten-IP Transaktions-ID Zuletzt geschrieben Zeit seit dem letzten Laden Bearbeitungen HA-Status Dateisystemstatus Blockpool-ID Cluster-ID Kompilierungsinformationen Eindeutige Versionsanzahl Version
Hadoop JobHistoryServer	Cluster-Namespace-Server	Knotenname Knoten-IP

Fehlerbehebung

Weitere Informationen finden Sie in der"Support" Seite.

HAProxy-Datensammler

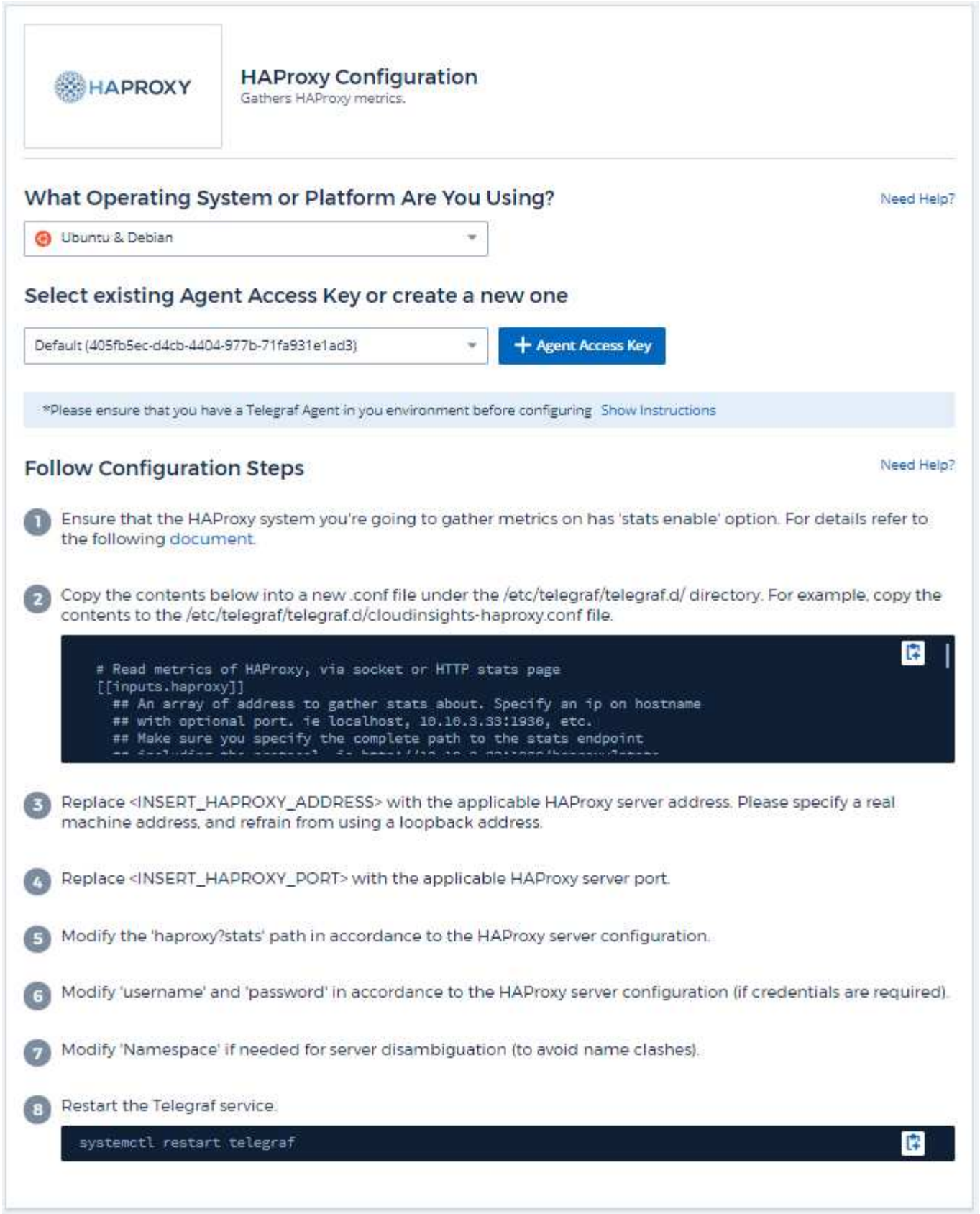
Data Infrastructure Insights verwendet diesen Datensammler, um Metriken von HAProxy zu sammeln.

Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie HAProxy.

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

2. Wenn Sie noch keinen Agenten für die Sammlung installiert haben oder einen Agenten für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das"Agenteninstallation" Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel zur Verwendung mit diesem Datensammler aus. Sie können einen neuen Agentenzugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agentenzugriffsschlüssel** klicken. Best Practice: Verwenden Sie nur dann einen anderen Agent-Zugriffsschlüssel, wenn Sie Datensammler beispielsweise nach Betriebssystem/Plattform gruppieren möchten.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen variieren je nach Art des Betriebssystems oder der Plattform, die Sie zum Sammeln von Daten verwenden.



Aufstellen

Das Plugin von Telegraf für HAProxy basiert auf der Aktivierung von HAProxy Stats. Dies ist eine in HAProxy integrierte Konfiguration, die jedoch nicht standardmäßig aktiviert ist. Wenn aktiviert, stellt HAProxy einen

HTML-Endpunkt bereit, der in Ihrem Browser angezeigt oder zum Extrahieren des Status aller HAProxy-Konfigurationen abgerufen werden kann.

Kompatibilität:

Die Konfiguration wurde für HAProxy Version 1.9.4 entwickelt.

Einrichten:

Um Statistiken zu aktivieren, bearbeiten Sie Ihre Haproxy-Konfigurationsdatei und fügen Sie nach dem Abschnitt „Standardeinstellungen“ die folgenden Zeilen hinzu. Verwenden Sie dabei Ihren eigenen Benutzer/Ihr eigenes Passwort und/oder Ihre Haproxy-URL:

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

Nachfolgend sehen Sie eine vereinfachte Beispielkonfigurationsdatei 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

Die folgenden Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Merkmale:	Datenpunkte:
HAProxy Frontend	Namespace-Adressproxy	Knoten-IP Knotenname Proxy-ID Modus Prozess-ID Sitzungsratenbegrenzung Server-ID Sitzungsbegrenzungsstatus	Bytes Eingehend Bytes Ausgehend Cache-Treffer Cache-Suchen Komprimierung Bytes Umgangene Komprimierung Bytes Eingehend Komprimierung Bytes Ausgehend Komprimierung Antworten Verbindungsrate Verbindungsrate Max. Verbindungen Gesamt Durch Verbindungsregel abgelehnte Anfragen Durch Sicherheitsbedenken abgelehnte Anfragen Antworten Durch Sicherheitsbedenken abgelehnte Anfragen Durch Sitzungsregel abgelehnte Anfragen Fehler bei Anfragen Antworten 1xx Antworten 2xx Antworten 3xx Antworten 4xx Antworten 5xx Antworten Andere Anfragen Abgefangene Anfragen Sitzungsrate Sitzungsrate Max. Anfragen Rate Anfragen Rate Max. Anfragen Gesamtanzahl Sitzungen Sitzungen Max. Sitzungen Gesamtanzahl Anfragen Neuschreibungen

Objekt:	Kennungen:	Merkmale:	Datenpunkte:
HAProxy Server	Namespace-Adress-Proxy-Server	Knoten-IP Knotenname Zeit bis zum Abschluss der Prüfung Fallkonfiguration prüfen Gesundheitswert prüfen Anstiegskonfiguration prüfen Status prüfen Proxy-ID Zeit der letzten Änderung Zeit der letzten Sitzung Modus Prozess-ID Server-ID Status Gewicht	Aktive Server Backup-Server Bytes rein Bytes raus Check-Downs Check-Fehlschläge Client-Abbrüche Verbindungen Durchschnittliche Verbindungsdauer Ausfallzeit Gesamt abgelehnte Antworten Verbindungsfehler Antwortfehler Antworten 1xx Antworten 2xx Antworten 3xx Antworten 4xx Antworten 5xx Antworten Andere ausgewählte Server Gesamtwarteschlange Aktuelle Warteschlange Max. Durchschnittliche Warteschlangendauer Sitzungen pro Sekunde Sitzungen pro Sekunde Max. Verbindungswiederverwendung Antwortzeit Durchschnittliche Sitzungen Sitzungen Max. Server-Übertragungsabbrüche Sitzungen Gesamtsitzungen Gesamtzeit Durchschnittliche Anfragen Neuzuweisungen Anfragen Wiederholungsversuche Anfragen Neuschreibungen

Objekt:	Kennungen:	Merkmale:	Datenpunkte:
HAProxy-Backend	Namespace-Adressproxy	Knoten-IP Knotenname Proxy-ID Letzte Änderung Zeit der letzten Sitzung Modus Prozess-ID Server-ID Sitzungslimit Status Gewicht	Aktive Server Backup-Server Bytes In Bytes Out Cache-Treffer Cache-Lookups Check-Downs Client-Abbrüche Komprimierung Bytes Umgangene Komprimierung Bytes In Komprimierung Bytes Out Komprimierung Antworten Verbindungen Durchschnittliche Verbindungsausfallzeit Anfragen insgesamt aufgrund von Sicherheitsbedenken abgelehnt Antworten aufgrund von Sicherheitsbedenken abgelehnt Verbindungsfehler Antwortfehler Antworten 1xx Antworten 2xx Antworten 3xx Antworten 4xx Antworten 5xx Antworten Andere ausgewählte Server Gesamtwarteschlange Aktuelle Warteschlange Max. Durchschnittliche Warteschlangenzeit Sitzungen pro Sekunde Sitzungen pro Sekunde Max. Anfragen Gesamte Verbindungswiederverwendung Antwortzeit Durchschnittliche Sitzungen Sitzungen Max. Serverübertragungsabbrüche Sitzungen Gesamtsitzungen Gesamtzeit Durchschnittliche Anfragen Neuzuweisungen Anfragen Wiederholungsversuche Anfragen Neuschreibungen

Fehlerbehebung

Weitere Informationen finden Sie in der"Support" Seite.

JVM-Datensammler

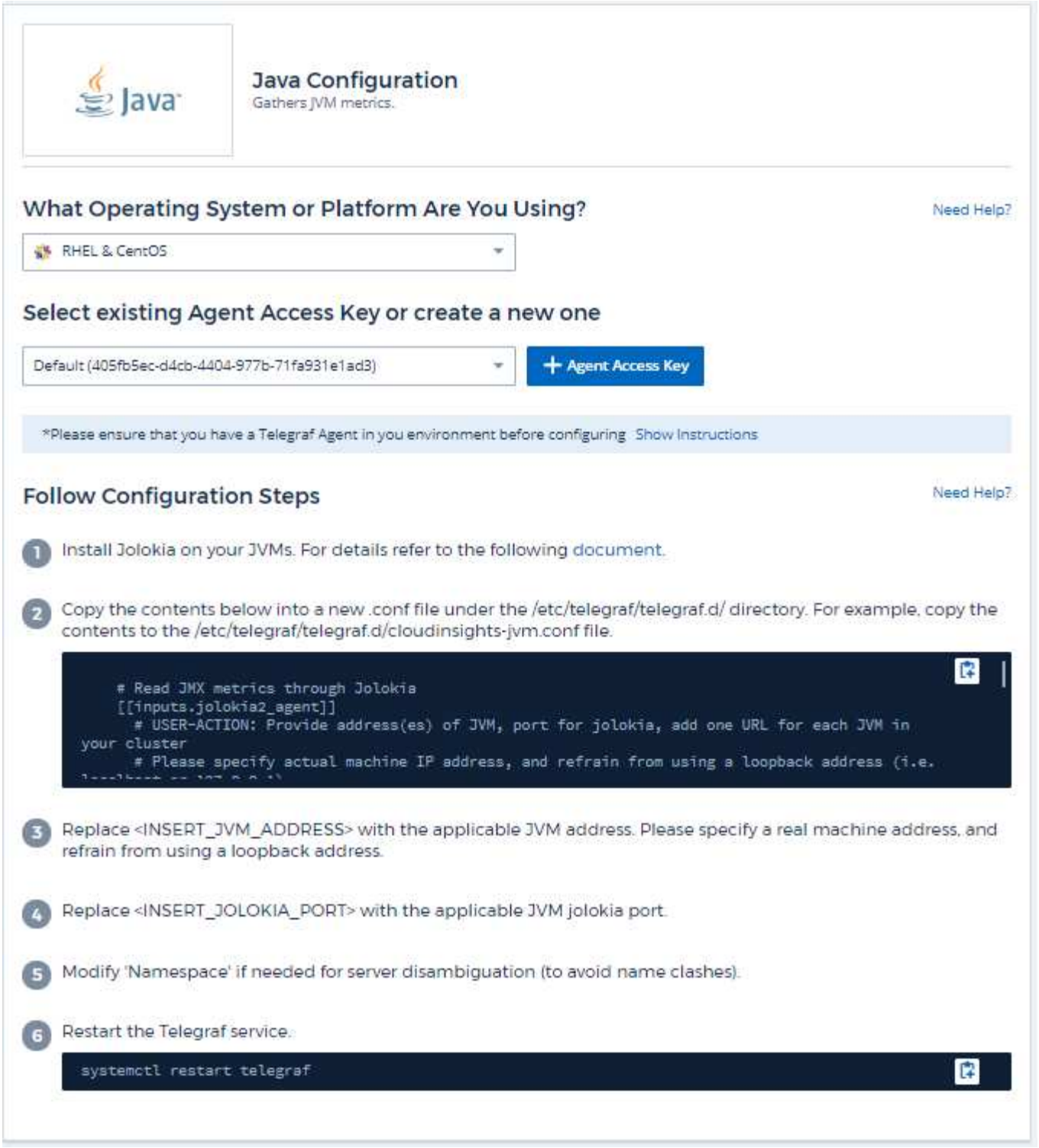
Data Infrastructure Insights verwendet diesen Datensammler, um Metriken von JVM zu sammeln.

Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie JVM.

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

2. Wenn Sie noch keinen Agenten für die Sammlung installiert haben oder einen Agenten für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das"Agenteninstallation" Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel zur Verwendung mit diesem Datensammler aus. Sie können einen neuen Agentenzugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agentenzugriffsschlüssel** klicken. Best Practice: Verwenden Sie nur dann einen anderen Agent-Zugriffsschlüssel, wenn Sie Datensammler beispielsweise nach Betriebssystem/Plattform gruppieren möchten.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen variieren je nach Art des Betriebssystems oder der Plattform, die Sie zum Sammeln von Daten verwenden.



Aufstellen

Informationen finden Sie in"JVM-Dokumentation" .

Objekte und Zähler

Die folgenden Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Merkmale:	Datenpunkte:
JVM	Namespace JVM	Betriebssystemarchitektur Betriebssystemname Betriebssystemversion Laufzeitspezifikation Laufzeitspezifikationsanbieter Laufzeitspezifikationsversion Betriebszeit Laufzeit-VM-Name Laufzeit-VM-Anbieter Laufzeit-VM-Version Knotenname Knoten-IP	Geladene Klasse, geladene Klasse, gesamt, entladene Klasse, Speicher-Heap, festgeschriebener Speicher, Heap-Init-Speicher, verwendeter Heap, max. Speicher, verwendeter Heap, nicht festgeschriebener Speicher, nicht festgeschriebener Speicher, nicht festgeschriebener Speicher, nicht festgeschriebener Speicher, nicht festgeschriebener Speicher, max. nicht festgeschriebener Speicher, verwendeter Speicher, ausstehende Finalisierung, verfügbare OS-Prozessoren, Größe des virtuellen OS-Speichers, Größe des freien OS-physischen Speichers, Größe des freien OS-Swap-Speichers, maximale OS-Dateideskriptoranzahl, Anzahl der geöffneten OS-Dateideskriptoren, CPU-Auslastung des OS-Prozessors, CPU-Zeit des OS-Prozessors, CPU-Auslastung des OS-Systems, durchschnittliche OS-Systemauslastung, gesamt physische OS-Speichergröße, Größe des OS-Swap-Speichers insgesamt, Anzahl der Thread-Daemons, Anzahl der Thread-Spitzen, Anzahl der Threads, Anzahl der gestarteten Threads, Anzahl der Garbage Collector-Kopien, Zeit der Garbage Collector-Kopien, Anzahl der Garbage Collector-

Fehlerbehebung

Weitere Informationen finden Sie in der"Support" Seite.

Kafka-Datensammler

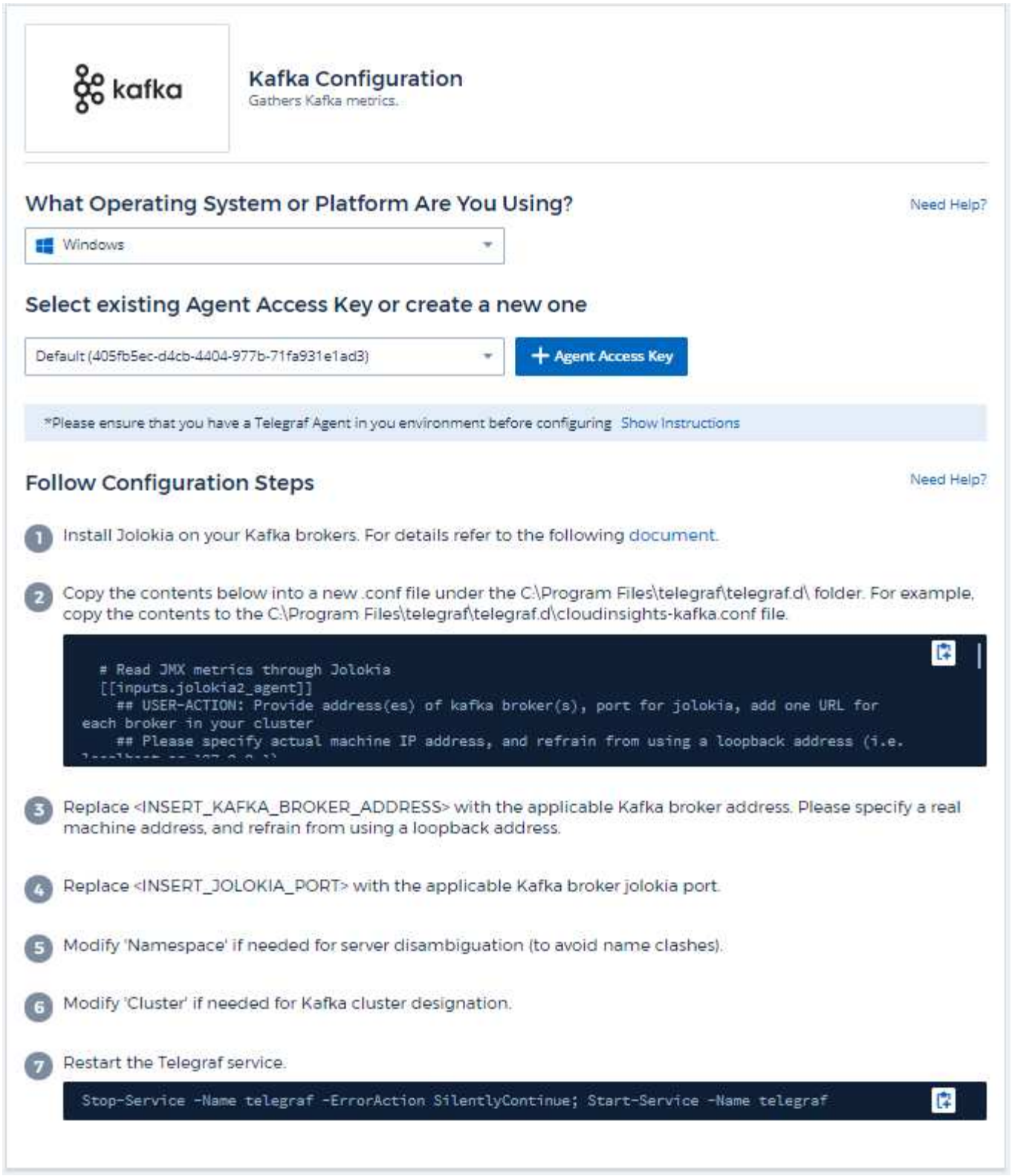
Data Infrastructure Insights verwendet diesen Datensammler, um Metriken von Kafka zu sammeln.

Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie Kafka.

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

2. Wenn Sie noch keinen Agenten für die Sammlung installiert haben oder einen Agenten für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das"Agenteninstallation" Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel zur Verwendung mit diesem Datensammler aus. Sie können einen neuen Agentenzugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agentenzugriffsschlüssel** klicken. Best Practice: Verwenden Sie nur dann einen anderen Agent-Zugriffsschlüssel, wenn Sie Datensammler beispielsweise nach Betriebssystem/Plattform gruppieren möchten.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen variieren je nach Art des Betriebssystems oder der Plattform, die Sie zum Sammeln von Daten verwenden.



Aufstellen

Das Kafka-Plugin basiert auf dem Jolokia-Plugin von Telegraf. Um beispielsweise Informationen von allen Kafka-Brokern zu sammeln, muss JMX auf allen Komponenten konfiguriert und über Jolokia verfügbar gemacht werden.

Kompatibilität

Die Konfiguration wurde für Kafka Version 0.11.0.2 entwickelt.

Einrichten

Bei allen folgenden Anweisungen wird davon ausgegangen, dass Ihr Installationsort für Kafka „/opt/kafka“ ist. Sie können die folgenden Anweisungen an Ihren Installationsort anpassen.

Jolokia Agent Jar

Eine Version, die die Jolokia-Agent-JAR-Datei haben muss"heruntergeladen" . Die getestete Version war Jolokia Agent 1.6.0.

Die folgenden Anweisungen gehen davon aus, dass die heruntergeladene JAR-Datei (jolokia-jvm-1.6.0-agent.jar) am Speicherort „/opt/kafka/libs/“ abgelegt ist.

Kafka-Broker

Um Kafka Brokers so zu konfigurieren, dass die Jolokia-API verfügbar gemacht wird, können Sie Folgendes in <KAFKA_HOME>/bin/kafka-server-start.sh direkt vor dem Aufruf von „kafka-run-class.sh“ 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 im obigen Beispiel „hostname -I“ verwendet wird, um die Umgebungsvariable „RMI_HOSTNAME“ einzurichten. Bei Maschinen mit mehreren IP-Adressen muss dies angepasst werden, um die IP-Adresse zu erfassen, die für RMI-Verbindungen von Bedeutung ist.

Sie können für JMX (9999 oben) und Jolokia (8778) einen anderen Port wählen. Wenn Sie eine interne IP haben, auf die Sie Jolokia sperren möchten, können Sie die „Catch-All“-IP 0.0.0.0 durch Ihre eigene IP ersetzen. Beachten Sie, dass diese IP vom Telegraf-Plugin aus zugänglich sein muss. Sie können die Option „-Dcom.sun.management.jmxremote.authenticate=false“ verwenden, wenn Sie keine Authentifizierung wünschen. Die Nutzung erfolgt auf eigene Gefahr.

Objekte und Zähler

Die folgenden Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Merkmale:
Kafka Broker	Cluster-Namespace-Broker	Knotenname Knoten-IP

Fehlerbehebung

Weitere Informationen finden Sie in der"Support" Seite.

Kibana-Datensammler

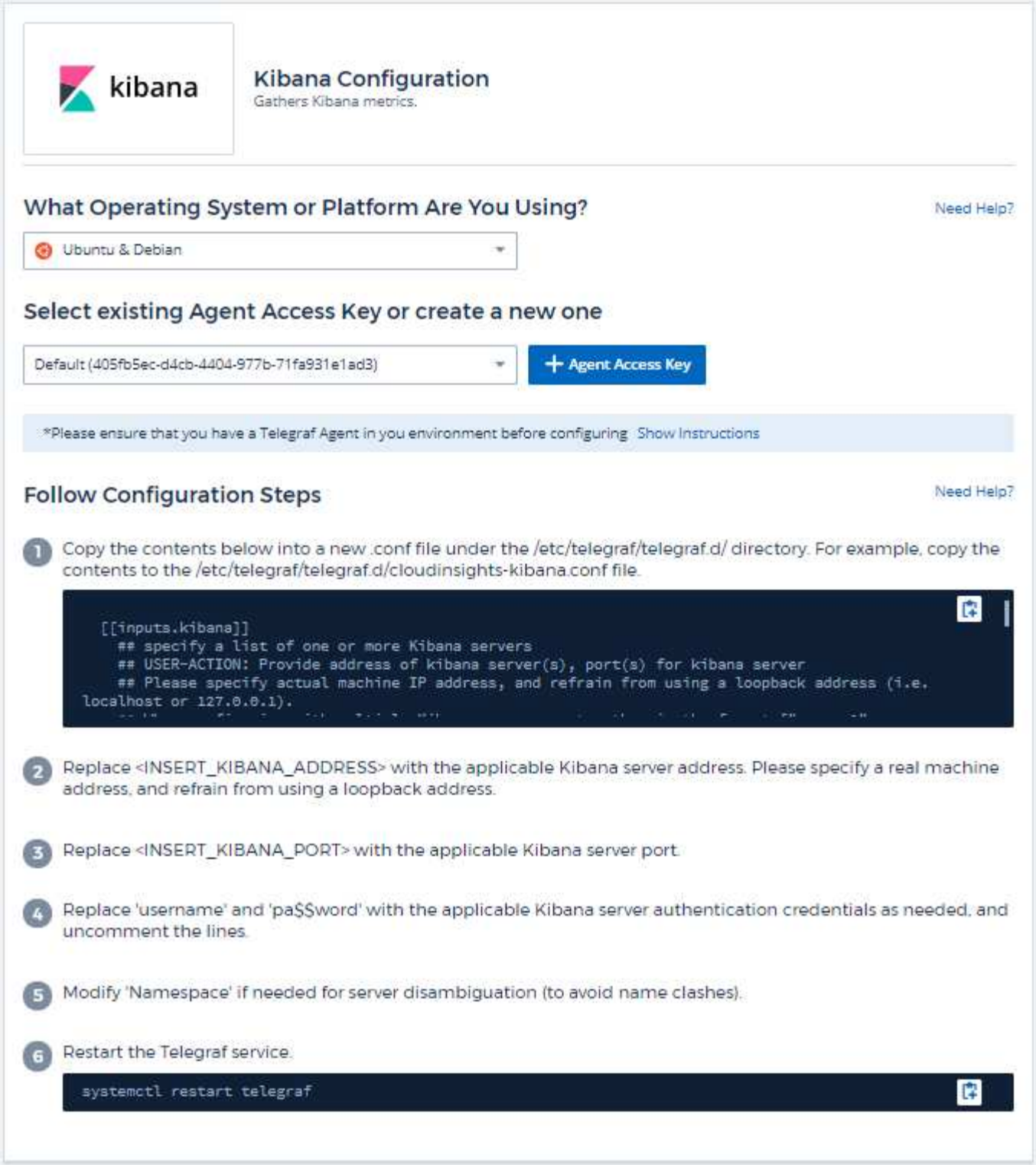
Data Infrastructure Insights verwendet diesen Datensammler, um Metriken von Kibana zu sammeln.

Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie Kibana.

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

2. Wenn Sie noch keinen Agenten für die Sammlung installiert haben oder einen Agenten für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das"Agenteninstallation" Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel zur Verwendung mit diesem Datensammler aus. Sie können einen neuen Agentenzugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agentenzugriffsschlüssel** klicken. Best Practice: Verwenden Sie nur dann einen anderen Agent-Zugriffsschlüssel, wenn Sie Datensammler beispielsweise nach Betriebssystem/Plattform gruppieren möchten.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen variieren je nach Art des Betriebssystems oder der Plattform, die Sie zum Sammeln von Daten verwenden.



Aufstellen

Informationen finden Sie im"Kibana-Dokumentation" .

Objekte und Zähler

Die folgenden Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Merkmale:	Datenpunkte:
Kibana	Namespace-Adresse	Knoten-IP Knotenname Version Status	Gleichzeitige Verbindungen Heap Max Verwendeter Heap Anfragen pro Sekunde Antwortzeit Durchschnittliche Antwortzeit Max. Betriebszeit

Fehlerbehebung

Weitere Informationen finden Sie in der"Support" Seite.

Installation und Konfiguration des Kubernetes Monitoring Operators

Data Infrastructure Insights bietet den **Kubernetes Monitoring Operator** für die Kubernetes-Sammlung. Navigieren Sie zu **Kubernetes > Collectors > +Kubernetes Collector**, um einen neuen Operator bereitzustellen.

Vor der Installation des Kubernetes Monitoring Operator

Siehe die"Voraussetzungen" Dokumentation, bevor Sie den Kubernetes Monitoring Operator installieren oder aktualisieren.

Installieren des Kubernetes Monitoring Operators

kubernetes

Kubernetes

Deploy NetApp Monitoring Operator

Quickly install and configure a Kubernetes Operator to send cluster information to Cloud Insights.

Select existing API Access Token or create a new one

KEY2024 (...vw6NdM) | + API Access Token | Production Best Practices

Installation Instructions

Need Help?

Please review the pre-requisites for installing the NetApp Kubernetes Monitoring Operator.
To update an existing operator installation please follow these steps.

1 Define Kubernetes cluster name and namespace

Provide the Kubernetes cluster name and specify a namespace for deploying the monitoring components.

Cluster	Namespace
clustername	netapp-monitoring

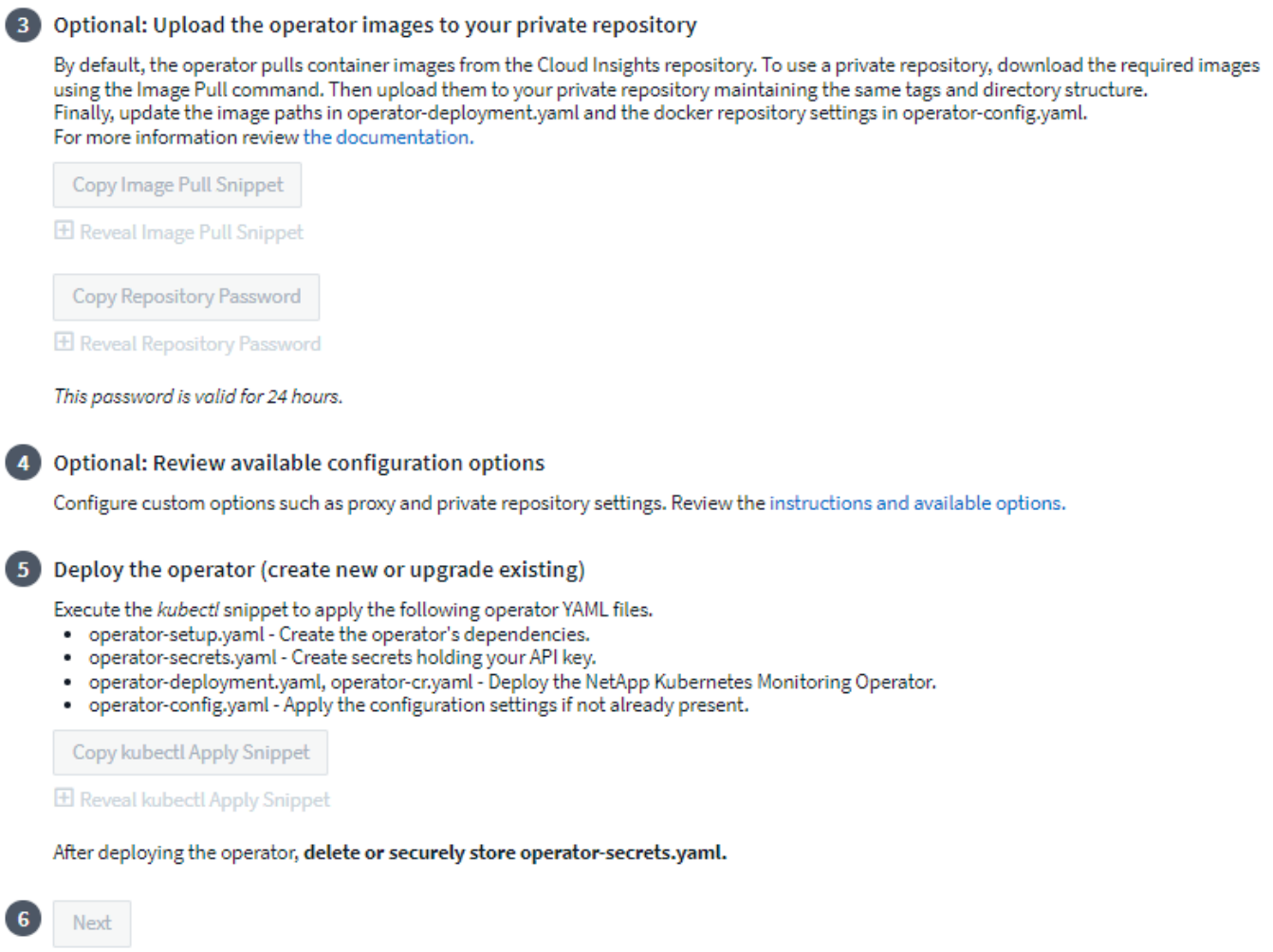
2 Download the operator YAML files

Execute the following download command in a *bash* prompt.

Copy Download Command Snippet

Reveal Download Command Snippet

This snippet includes a unique access key that is valid for 24 hours.



Schritte zum Installieren des Kubernetes Monitoring Operator-Agenten auf Kubernetes:

1. Geben Sie einen eindeutigen Clusternamen und Namespace ein. Wenn SieUpgrade von einem vorherigen Kubernetes-Operator, verwenden Sie denselben Clusternamen und Namespace.
2. Sobald diese eingegeben sind, können Sie den Download-Befehlsausschnitt in die Zwischenablage kopieren.
3. Fügen Sie den Snippet in ein *Bash*-Fenster ein und führen Sie ihn aus. Die Operator-Installationsdateien werden heruntergeladen. Beachten Sie, dass das Snippet einen eindeutigen Schlüssel hat und 24 Stunden gültig ist.
4. Wenn Sie ein benutzerdefiniertes oder privates Repository haben, kopieren Sie den optionalen Image Pull-Ausschnitt, fügen Sie ihn in eine *Bash*-Shell ein und führen Sie ihn aus. Sobald die Bilder abgerufen wurden, kopieren Sie sie in Ihr privates Repository. Achten Sie darauf, dieselben Tags und dieselbe Ordnerstruktur beizubehalten. Aktualisieren Sie die Pfade in *operator-deployment.yaml* sowie die Docker-Repository-Einstellungen in *operator-config.yaml*.
5. Überprüfen Sie bei Bedarf die verfügbaren Konfigurationsoptionen wie Proxy- oder private Repository-Einstellungen. Weitere Informationen finden Sie unter"Konfigurationsoptionen" .
6. Wenn Sie bereit sind, stellen Sie den Operator bereit, indem Sie das kubectl Apply-Snippet kopieren, herunterladen und ausführen.
7. Die Installation erfolgt automatisch. Wenn der Vorgang abgeschlossen ist, klicken Sie auf die Schaltfläche *Weiter*.

8. Wenn die Installation abgeschlossen ist, klicken Sie auf die Schaltfläche *Weiter*. Denken Sie daran, auch die Datei *operator-secrets.yaml* zu löschen oder sicher zu speichern.

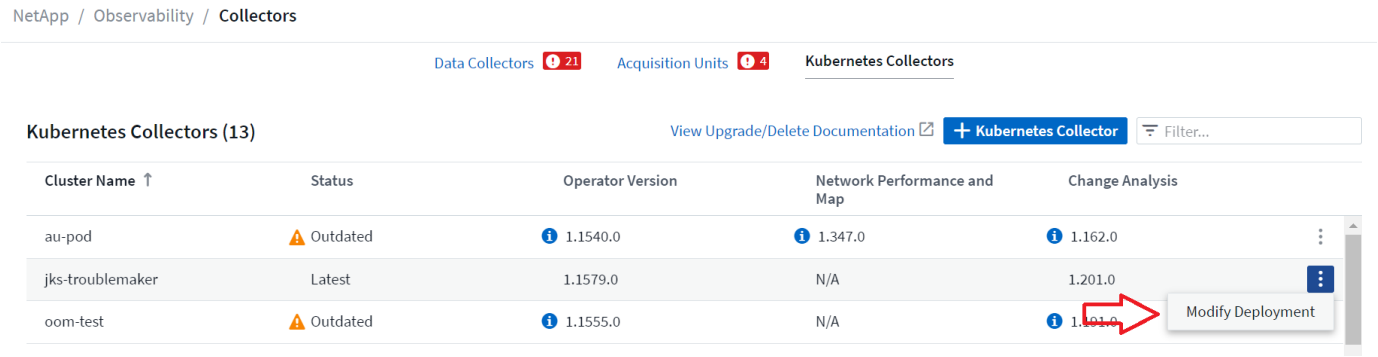
Wenn Sie ein benutzerdefiniertes Repository haben, lesen Sie überVerwenden eines benutzerdefinierten/privaten Docker-Repositorys .

Kubernetes-Überwachungskomponenten

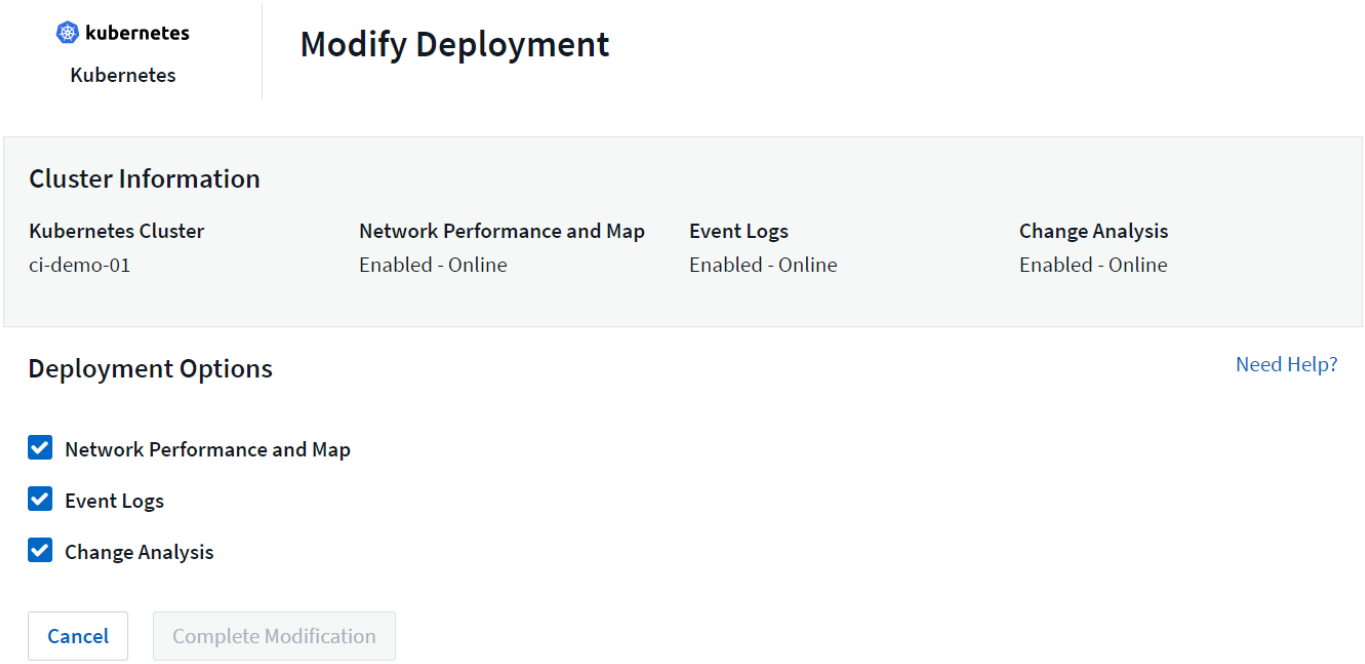
Data Infrastructure Insights Kubernetes Monitoring besteht aus vier Überwachungskomponenten:

- Clustermetriken
- Netzwerkleistung und Karte (optional)
- Ereignisprotokolle (optional)
- Änderungsanalyse (optional)

Die oben genannten optionalen Komponenten sind standardmäßig für jeden Kubernetes-Collector aktiviert. Wenn Sie entscheiden, dass Sie eine Komponente für einen bestimmten Collector nicht benötigen, können Sie sie deaktivieren, indem Sie zu **Kubernetes > Collectors** navigieren und im Drei-Punkte-Menü des Collectors auf der rechten Bildschirmseite *Bereitstellung ändern* auswählen.



Der Bildschirm zeigt den aktuellen Status jeder Komponente an und ermöglicht Ihnen, Komponenten für diesen Collector nach Bedarf zu deaktivieren oder zu aktivieren.



Upgrade auf den neuesten Kubernetes Monitoring Operator

DII-Druckknopf-Upgrades

Sie können den Kubernetes Monitoring Operator über die DII Kubernetes Collectors-Seite aktualisieren. Klicken Sie auf das Menü neben dem Cluster, den Sie aktualisieren möchten, und wählen Sie *Upgrade*. Der Betreiber überprüft die Bildsignaturen, erstellt einen Snapshot Ihrer aktuellen Installation und führt das Upgrade durch. Innerhalb weniger Minuten sollte der Status des Operators von „Upgrade läuft“ bis „Neueste“ fortschreiten. Wenn ein Fehler auftritt, können Sie für weitere Einzelheiten den Fehlerstatus auswählen und die Tabelle zur Fehlerbehebung bei Push-Button-Upgrades weiter unten zu Rate ziehen.

Push-Button-Upgrades mit privaten Repositories

Wenn Ihr Operator für die Verwendung eines privaten Repositorys konfiguriert ist, stellen Sie bitte sicher, dass alle zum Ausführen des Operators erforderlichen Bilder und deren Signaturen in Ihrem Repository verfügbar sind. Wenn während des Upgrade-Vorgangs ein Fehler aufgrund fehlender Bilder auftritt, fügen Sie diese einfach zu Ihrem Repository hinzu und versuchen Sie das Upgrade erneut. Um die Bildsignaturen in Ihr Repository hochzuladen, verwenden Sie bitte das Cosign-Tool wie folgt und stellen Sie sicher, dass Sie Signaturen für alle unter 3 angegebenen Bilder hochladen. Optional: Laden Sie die Operatorbilder in Ihr privates Repository hoch > Image Pull Snippet

```
cosign copy example.com/src:v1 example.com/dest:v1
#Example
cosign copy <DII container registry>/netapp-monitoring:<image version>
<private repository>/netapp-monitoring:<image version>
```

Rollback auf eine zuvor ausgeführte Version

Wenn Sie das Upgrade mithilfe der Funktion „Upgrade per Knopfdruck“ durchgeführt haben und innerhalb von sieben Tagen nach dem Upgrade Probleme mit der aktuellen Version des Operators auftreten, können Sie mithilfe des während des Upgrade-Vorgangs erstellten Snapshots ein Downgrade auf die zuvor ausgeführte

Version durchführen. Klicken Sie auf das Menü neben dem Cluster, für den Sie ein Rollback durchführen möchten, und wählen Sie *Rollback* aus.

Manuelle Upgrades

Stellen Sie fest, ob eine Agentenkonfiguration mit dem vorhandenen Operator vorhanden ist (wenn Ihr Namespace nicht der Standardnamespace *netapp-monitoring* ist, ersetzen Sie ihn durch den entsprechenden Namespace):

```
 kubectl -n netapp-monitoring get agentconfiguration netapp-ci-monitoring-
configuration
Wenn eine Agentenkonfiguration vorhanden ist:
```

- Installierender neueste Operator über den vorhandenen Operator.
  - Stellen Sie sicher, dass SieAbrufen der neuesten Container-Images wenn Sie ein benutzerdefiniertes Repository verwenden.

Wenn die Agentenkonfiguration nicht vorhanden ist:

- Notieren Sie sich den von Data Infrastructure Insights erkannten Clusternamen (wenn Ihr Namespace nicht der Standardnamespace „netapp-monitoring“ ist, ersetzen Sie ihn durch den entsprechenden Namespace):

```
 kubectl -n netapp-monitoring get agent -o
jsonpath='{.items[0].spec.cluster-name}'
* Erstellen Sie eine Sicherungskopie des vorhandenen Operators (wenn Ihr
Namespace nicht der Standard-Netapp-Monitoring-Namespace ist, ersetzen
Sie ihn durch den entsprechenden Namespace):
```

```
 kubectl -n netapp-monitoring get agent -o yaml > agent_backup.yaml
* <<to-remove-the-kubernetes-monitoring-operator,Deinstallieren>>der
bestehende Betreiber.
* <<installing-the-kubernetes-monitoring-operator,Installieren>>der
neueste Operator.
```

  - Verwenden Sie denselben Clusternamen.
  - Nachdem Sie die neuesten Operator-YAML-Dateien heruntergeladen haben, portieren Sie vor der Bereitstellung alle in agent_backup.yaml gefundenen Anpassungen in die heruntergeladene operator-config.yaml.
  - Stellen Sie sicher, dass SieAbrufen der neuesten Container-Images wenn Sie ein benutzerdefiniertes Repository verwenden.

Stoppen und Starten des Kubernetes-Überwachungsoperators

So stoppen Sie den Kubernetes Monitoring Operator:

```
 kubectl -n netapp-monitoring scale deploy monitoring-operator
--replicas=0
So starten Sie den Kubernetes Monitoring Operator:
```

```
kubectl -n netapp-monitoring scale deploy monitoring-operator --replicas=1
```

Deinstallation

So entfernen Sie den Kubernetes Monitoring Operator

Beachten Sie, dass der Standardnamespace für den Kubernetes Monitoring Operator „netapp-monitoring“ ist. Wenn Sie Ihren eigenen Namespace festgelegt haben, ersetzen Sie diesen Namespace in diesen und allen nachfolgenden Befehlen und Dateien.

Neuere Versionen des Monitoring-Operators können mit den folgenden Befehlen deinstalliert werden:

```
kubectl -n <NAMESPACE> delete agent -l installed-by=nkmo-<NAMESPACE>
kubectl -n <NAMESPACE> delete
clusterrole,clusterrolebinding,crd,svc,deploy,role,rolebinding,secret,sa
-l installed-by=nkmo-<NAMESPACE>
```

Wenn der Überwachungsoperator in seinem eigenen dedizierten Namespace bereitgestellt wurde, löschen Sie den Namespace:

```
 kubectl delete ns <NAMESPACE>
Hinweis: Wenn der erste Befehl „Keine Ressourcen gefunden“ zurückgibt,
befolgen Sie die folgenden Anweisungen, um ältere Versionen des
Überwachungsoperators zu deinstallieren.
```

Führen Sie die folgenden Befehle der Reihe nach aus. Abhängig von Ihrer aktuellen Installation können einige dieser Befehle die Meldung „Objekt nicht gefunden“ zurückgeben. Diese Nachrichten können bedenkenlos ignoriert werden.

```
kubectl -n <NAMESPACE> delete agent agent-monitoring-netapp
kubectl delete crd agents.monitoring.netapp.com
kubectl -n <NAMESPACE> delete role agent-leader-election-role
kubectl delete clusterrole agent-manager-role agent-proxy-role agent-
metrics-reader <NAMESPACE>-agent-manager-role <NAMESPACE>-agent-proxy-role
<NAMESPACE>-cluster-role-privileged
kubectl delete clusterrolebinding agent-manager-rolebinding agent-proxy-
rolebinding agent-cluster-admin-rolebinding <NAMESPACE>-agent-manager-
rolebinding <NAMESPACE>-agent-proxy-rolebinding <NAMESPACE>-cluster-role-
binding-privileged
kubectl delete <NAMESPACE>-psp-nkmo
kubectl delete ns <NAMESPACE>
```

Wenn zuvor eine Sicherheitskontextbeschränkung erstellt wurde:

```
kubectl delete scc telegraf-hostaccess
```

Über Kube-State-Metrics

Der NetApp Kubernetes Monitoring Operator installiert seine eigenen Kube-State-Metriken, um Konflikte mit anderen Instanzen zu vermeiden.

Informationen zu Kube-State-Metrics finden Sie unter"diese Seite" .

Konfigurieren/Anpassen des Operators

Diese Abschnitte enthalten Informationen zum Anpassen Ihrer Operatorkonfiguration, zum Arbeiten mit Proxy, zum Verwenden eines benutzerdefinierten oder privaten Docker-Repositorys oder zum Arbeiten mit OpenShift.

Konfigurationsoptionen

Die am häufigsten geänderten Einstellungen können in der benutzerdefinierten Ressource *AgentConfiguration* konfiguriert werden. Sie können diese Ressource vor der Bereitstellung des Operators bearbeiten, indem Sie die Datei *operator-config.yaml* bearbeiten. Diese Datei enthält auskommentierte Beispiele für Einstellungen. Siehe die Liste der"Verfügbare Einstellungen" für die neueste Version des Operators.

Sie können diese Ressource auch bearbeiten, nachdem der Operator bereitgestellt wurde, indem Sie den folgenden Befehl verwenden:

```
 kubectl -n netapp-monitoring edit AgentConfiguration
Um festzustellen, ob Ihre bereitgestellte Version des Operators
AgentConfiguration unterstützt, führen Sie den folgenden Befehl aus:
```

```
 kubectl get crd agentconfigurations.monitoring.netapp.com
Wenn die Meldung „Fehler vom Server (Nicht gefunden)“ angezeigt wird, muss
Ihr Operator aktualisiert werden, bevor Sie die Agentenkonfiguration
verwenden können.
```

Konfigurieren der Proxy-Unterstützung

Es gibt zwei Stellen, an denen Sie einen Proxy auf Ihrem Mandanten verwenden können, um den Kubernetes Monitoring Operator zu installieren. Dabei kann es sich um dasselbe oder um separate Proxy-Systeme handeln:

- Proxy, der während der Ausführung des Installationscode-Snippets (mit „curl“) benötigt wird, um das System, auf dem das Snippet ausgeführt wird, mit Ihrer Data Infrastructure Insights -Umgebung zu verbinden
- Proxy, der vom Ziel-Kubernetes-Cluster zur Kommunikation mit Ihrer Data Infrastructure Insights -Umgebung benötigt wird

Wenn Sie für einen oder beide einen Proxy verwenden, müssen Sie zur Installation des Kubernetes Operating Monitor zunächst sicherstellen, dass Ihr Proxy so konfiguriert ist, dass eine gute Kommunikation mit Ihrer Data Infrastructure Insights Umgebung möglich ist. Wenn Sie über einen Proxy verfügen und von dem Server/der VM, von dem/der Sie den Operator installieren möchten, auf Data Infrastructure Insights zugreifen können, ist Ihr Proxy wahrscheinlich richtig konfiguriert.

Legen Sie für den Proxy, der zur Installation des Kubernetes Operating Monitor verwendet wird, vor der Installation des Operators die Umgebungsvariablen *http_proxy/https_proxy* fest. Für einige Proxy-Umgebungen müssen Sie möglicherweise auch die Umgebungsvariable *no_proxy* festlegen.

Um die Variable(n) festzulegen, führen Sie **vor** der Installation des Kubernetes Monitoring Operator die folgenden Schritte auf Ihrem System aus:

1. Legen Sie die Umgebungsvariable(n) *https_proxy* und/oder *http_proxy* für den aktuellen Benutzer fest:
   a. Wenn der einzurichtende Proxy keine Authentifizierung (Benutzername/Passwort) hat, führen Sie den folgenden Befehl aus:

      ```
       export https_proxy=<proxy_server>:<proxy_port>
      .. Wenn der einzurichtende Proxy über eine Authentifizierung
      (Benutzername/Passwort) verfügt, führen Sie diesen Befehl aus:
      ```

      ```
      export
      http_proxy=<proxy_username>:<proxy_password>@<proxy_server>:<proxy_po
      rt>
      ```

Damit der für Ihren Kubernetes-Cluster verwendete Proxy mit Ihrer Data Infrastructure Insights -Umgebung kommunizieren kann, installieren Sie nach dem Lesen aller dieser Anweisungen den Kubernetes Monitoring Operator.

Konfigurieren Sie den Proxy-Abschnitt der AgentConfiguration in operator-config.yaml, bevor Sie den

Kubernetes Monitoring Operator bereitstellen.

```
agent:
  ...
  proxy:
    server: <server for proxy>
    port: <port for proxy>
    username: <username for proxy>
    password: <password for proxy>

    # In the noproxy section, enter a comma-separated list of
    # IP addresses and/or resolvable hostnames that should bypass
    # the proxy
    noproxy: <comma separated list>

    isTelegrafProxyEnabled: true
    isFluentbitProxyEnabled: <true or false> # true if Events Log enabled
    isCollectorsProxyEnabled: <true or false> # true if Network
Performance and Map enabled
    isAuProxyEnabled: <true or false> # true if AU enabled
  ...
...
```

Verwenden eines benutzerdefinierten oder privaten Docker-Repositorys

Standardmäßig ruft der Kubernetes Monitoring Operator Container-Images aus dem Data Infrastructure Insights Repository ab. Wenn Sie einen Kubernetes-Cluster als Ziel für die Überwachung verwenden und dieser Cluster so konfiguriert ist, dass er nur Container-Images aus einem benutzerdefinierten oder privaten Docker-Repository oder Container-Register abruft, müssen Sie den Zugriff auf die vom Kubernetes Monitoring Operator benötigten Container konfigurieren.

Führen Sie das „Image Pull Snippet“ aus der Installationskachel des NetApp Monitoring Operator aus. Mit diesem Befehl melden Sie sich beim Data Infrastructure Insights -Repository an, rufen alle Bildabhängigkeiten für den Operator ab und melden sich vom Data Infrastructure Insights -Repository ab. Geben Sie bei der entsprechenden Aufforderung das bereitgestellte temporäre Repository-Passwort ein. Dieser Befehl lädt alle vom Bediener verwendeten Bilder herunter, auch für optionale Funktionen. Unten sehen Sie, für welche Funktionen diese Bilder verwendet werden.

Kernoperator-Funktionalität und Kubernetes-Überwachung

- NetApp-Überwachung
- ci-kube-rbac-proxy
- ci-ksm
- ci-telegraf
- Distroless-Root-Benutzer

Ereignisprotokoll

- ci-fluent-bit
- ci-kubernetes-event-exporter

Netzwerkleistung und Karte

- ci-net-observer

Übertragen Sie das Operator-Docker-Image gemäß Ihren Unternehmensrichtlinien in Ihr privates/lokales/Unternehmens-Docker-Repository. Stellen Sie sicher, dass die Bild-Tags und Verzeichnispfade zu diesen Bildern in Ihrem Repository mit denen im Data Infrastructure Insights -Repository übereinstimmen.

Bearbeiten Sie die Bereitstellung des Überwachungsoperators in operator-deployment.yaml und ändern Sie alle Bildreferenzen, um Ihr privates Docker-Repository zu verwenden.

```
image: <docker repo of the enterprise/corp docker repo>/ci-kube-rbac-
proxy:<ci-kube-rbac-proxy version>
image: <docker repo of the enterprise/corp docker repo>/netapp-
monitoring:<version>
```

Bearbeiten Sie die AgentConfiguration in operator-config.yaml, um den neuen Speicherort des Docker-Repositorys widerzuspiegeln. Erstellen Sie ein neues imagePullSecret für Ihr privates Repository. Weitere Informationen finden Sie unter *https://kubernetes.io/docs/tasks/configure-pod-container/pull-image-private-registry/*

```
agent:
  ...
  # An optional docker registry where you want docker images to be pulled
from as compared to CI's docker registry
  # Please see documentation link here:
xref:{relative_path}task_config_telegraf_agent_k8s.html#using-a-custom-or-
private-docker-repository
  dockerRepo: your.docker.repo/long/path/to/test
  # Optional: A docker image pull secret that maybe needed for your
private docker registry
  dockerImagePullSecret: docker-secret-name
```

OpenShift-Anweisungen

Wenn Sie OpenShift 4.6 oder höher verwenden, müssen Sie die AgentConfiguration in *operator-config.yaml* bearbeiten, um die Einstellung *runPrivileged* zu aktivieren:

```
# Set runPrivileged to true SELinux is enabled on your kubernetes nodes
runPrivileged: true
```

Openshift implementiert möglicherweise eine zusätzliche Sicherheitsebene, die den Zugriff auf einige Kubernetes-Komponenten blockieren kann.

Toleranzen und Makel

Die DaemonSets *netapp-ci-telegraf-ds*, *netapp-ci-fluent-bit-ds* und *netapp-ci-net-observer-l4-ds* müssen auf jedem Knoten in Ihrem Cluster einen Pod planen, um Daten auf allen Knoten korrekt zu erfassen. Der Operator wurde so konfiguriert, dass er einige bekannte **Verunreinigungen** toleriert. Wenn Sie benutzerdefinierte Taints auf Ihren Knoten konfiguriert haben und dadurch verhindern, dass Pods auf jedem Knoten ausgeführt werden, können Sie eine **Toleranz** für diese Taints erstellen."in der *AgentConfiguration*" . Wenn Sie benutzerdefinierte Taints auf alle Knoten in Ihrem Cluster angewendet haben, müssen Sie der Operatorbereitstellung auch die erforderlichen Toleranzen hinzufügen, damit der Operator-Pod geplant und ausgeführt werden kann.

Mehr über Kubernetes erfahren"Makel und Duldungen" .

Zurück zum"* Seite „NetApp Kubernetes Monitoring Operator Installation“*"

Eine Anmerkung zu Geheimnissen

Um dem Kubernetes Monitoring Operator die Berechtigung zum Anzeigen von Geheimnissen im gesamten Cluster zu entziehen, löschen Sie vor der Installation die folgenden Ressourcen aus der Datei *operator-setup.yaml*:

```
 ClusterRole/netapp-ci<namespace>-agent-secret
 ClusterRoleBinding/netapp-ci<namespace>-agent-secret
```

Wenn es sich um ein Upgrade handelt, löschen Sie auch die Ressourcen aus Ihrem Cluster:

```
 kubectl delete ClusterRole/netapp-ci-<namespace>-agent-secret-clusterrole
 kubectl delete ClusterRoleBinding/netapp-ci-<namespace>-agent-secret-
clusterrolebinding
```

Wenn die Änderungsanalyse aktiviert ist, ändern Sie die Datei *AgentConfiguration* oder *operator-config.yaml*, um den Abschnitt zur Änderungsverwaltung zu kommentieren und *kindsToIgnoreFromWatch: '"secrets"'* in den Abschnitt zur Änderungsverwaltung aufzunehmen. Beachten Sie das Vorhandensein und die Position von einfachen und doppelten Anführungszeichen in dieser Zeile.

```
change-management:
  ...
  # # A comma separated list of kinds to ignore from watching from the
default set of kinds watched by the collector
  # # Each kind will have to be prefixed by its apigroup
  # # Example: '"networking.k8s.io.networkpolicies,batch.jobs",
"authorization.k8s.io.subjectaccessreviews"'
  kindsToIgnoreFromWatch: '"secrets"'
  ...
```

Überprüfen der Bildsignaturen des Kubernetes-Überwachungsoperators

Das Image für den Operator und alle zugehörigen Images, die er bereitstellt, sind von NetApp signiert. Sie können die Images vor der Installation manuell mit dem Cosign-Tool überprüfen oder einen Kubernetes-Zulassungscontroller konfigurieren. Weitere Einzelheiten finden Sie in der"Kubernetes-Dokumentation" .

Der öffentliche Schlüssel, der zum Überprüfen der Bildsignaturen verwendet wird, ist in der Installationskachel des Überwachungsoperators unter *Optional: Laden Sie die Operatorbilder in Ihr privates Repository hoch > Öffentlicher Schlüssel der Bildsignatur* verfügbar.

Um eine Bildsignatur manuell zu überprüfen, führen Sie die folgenden Schritte aus:

1. Kopieren und führen Sie das Image Pull Snippet aus
2. Kopieren Sie das Repository-Passwort und geben Sie es ein, wenn Sie dazu aufgefordert werden.
3. Speichern Sie den öffentlichen Schlüssel der Bildsignatur (dii-image-signing.pub im Beispiel).
4. Überprüfen Sie die Bilder mit Cosign. Siehe das folgende Beispiel für die Verwendung von Cosign

```
$ cosign verify --key dii-image-signing.pub --insecure-ignore-sct
--insecure-ignore-tlog <repository>/<image>:<tag>
Verification for <repository>/<image>:<tag> --
The following checks were performed on each of these signatures:
  - The cosign claims were validated
  - The signatures were verified against the specified public key
[{"critical":{"identity":{"docker-
reference":"<repository>/<image>"},"image":{"docker-manifest-
digest":"sha256:<hash>"},"type":"cosign container image
signature"},"optional":null}]
```

Fehlerbehebung

Wenn beim Einrichten des Kubernetes Monitoring Operators Probleme auftreten, können Sie Folgendes versuchen:

Problem:	Versuchen Sie Folgendes:
Ich sehe keinen Hyperlink/keine Verbindung zwischen meinem Kubernetes Persistent Volume und dem entsprechenden Back-End-Speichergerät. Mein Kubernetes Persistent Volume wird mit dem Hostnamen des Speicherservers konfiguriert.	Befolgen Sie die Schritte zum Deinstallieren des vorhandenen Telegraf-Agenten und installieren Sie anschließend den neuesten Telegraf-Agenten neu. Sie müssen Telegraf Version 2.0 oder höher verwenden und Ihr Kubernetes-Clusterspeicher muss aktiv von Data Infrastructure Insights überwacht werden.

Problem:	Versuchen Sie Folgendes:
Ich sehe in den Protokollen Meldungen, die den folgenden ähneln: E0901 15:21:39.962145 1 reflector.go:178] k8s.io/kube-state-metrics/internal/store/builder.go:352: *v1.MutatingWebhookConfiguration konnte nicht aufgelistet werden: Der Server konnte die angeforderte Ressource nicht finden. E0901 15:21:43.168161 1 reflector.go:178] k8s.io/kube-state-metrics/internal/store/builder.go:352: *v1.Lease konnte nicht aufgelistet werden: Der Server konnte die angeforderte Ressource nicht finden (get leases.coordination.k8s.io) usw.	Diese Meldungen können auftreten, wenn Sie kube-state-metrics Version 2.0.0 oder höher mit Kubernetes-Versionen unter 1.20 ausführen. So erhalten Sie die Kubernetes-Version: *kubectl version* So erhalten Sie die kube-state-metrics-Version: *kubectl get deploy/kube-state-metrics -o jsonpath='{..image}'* Um diese Meldungen zu verhindern, können Benutzer ihre kube-state-metrics-Bereitstellung ändern, um die folgenden Leases zu deaktivieren: *mutatingwebhookconfigurations validatingwebhookconfigurations volumeattachments resources* Genauer gesagt können sie das folgende CLI-Argument verwenden: resources=certificatesigningrequests,configmaps,cronjobs,daemonsets, deployments,endpoints,horizontalpodautoscalers,ingresses,jobs,limitranges, namespaces,networkpolicies,nodes,persistentvolumeclaims,persistentvolumes, poddisruptionbudgets,pods,replicasets,replicationcontrollers,resourcequotas, secrets,services,statefulsets,storageclasses Die Standardressourcenliste ist: „Zertifikatsignaturanforderungen, Konfigurationszuordnungen, Cronjobs, Daemonsets, Bereitstellungen, Endpunkte, horizontale Pod-Autoskalierer, Ingresses, Jobs, Leases, Grenzwertbereiche, mutierende Webhookkonfigurationen, Namespaces, Netzwerkrichtlinien, Knoten, persistente Volumeansprüche, persistente Volumes, Pod-Unterbrechungsbudgets, Pods, Replikatsets, Replikationscontroller, Ressourcenkontingente, Geheimnisse, Dienste, Statefulsets, Speicherklassen, validierende Webhookkonfigurationen, Volumeanhänge“

Problem:	Versuchen Sie Folgendes:
Ich sehe Fehlermeldungen von Telegraf, die den folgenden ähneln, aber Telegraf wird gestartet und ausgeführt: 11. Okt. 14:23:41 ip-172-31-39-47 systemd[1]: Der Plugin-gesteuerte Server-Agent zum Melden von Metriken in InfluxDB wurde gestartet. 11. Okt. 14:23:41 ip-172-31-39-47 telegraf[1827]: time="2021-10-11T14:23:41Z" level=error msg="Cache-Verzeichnis konnte nicht erstellt werden. /etc/telegraf/.cache/snowflake, err: mkdir /etc/telegraf/.ca che: Zugriff verweigert. Ignoriert\n" func="gosnowflake.(*defaultLogger).Errorf" file="log.go:120" 11. Okt. 14:23:41 ip-172-31-39-47 telegraf[1827]: time="2021-10-11T14:23:41Z" level=error msg="Öffnen fehlgeschlagen. Ignoriert. Öffnen Sie /etc/telegraf/.cache/snowflake/ocsp_response_cache.json: keine solche Datei oder kein solches Verzeichnis\n" func="gosnowflake.(*defaultLogger).Errorf" file="log.go:120" 11. Okt. 14:23:41 ip-172-31-39-47 telegraf[1827]: 2021-10-11T14:23:41Z I! Telegraf 1.19.3 wird gestartet	Dies ist ein bekanntes Problem. Siehe"Dieser GitHub-Artikel" für weitere Details. Solange Telegraf läuft, können Benutzer diese Fehlermeldungen ignorieren.
Auf Kubernetes melden meine Telegraf-Pods den folgenden Fehler: „Fehler beim Verarbeiten der Mountstats-Informationen: Mountstats-Datei konnte nicht geöffnet werden: /hostfs/proc/1/mountstats, Fehler: Öffnen von /hostfs/proc/1/mountstats: Berechtigung verweigert“	Wenn SELinux aktiviert ist und erzwungen wird, verhindert es wahrscheinlich, dass die Telegraf-Pods auf die Datei /proc/1/mountstats auf dem Kubernetes-Knoten zugreifen können. Um diese Einschränkung zu umgehen, bearbeiten Sie die Agentenkonfiguration und aktivieren Sie die Einstellung „runPrivileged“. Weitere Einzelheiten finden Sie in den OpenShift-Anweisungen.
Auf Kubernetes meldet mein Telegraf ReplicaSet-Pod den folgenden Fehler: [inputs.prometheus] Fehler im Plugin: Schlüsselpaar /etc/kubernetes/pki/etcd/server.crt konnte nicht geladen werden:/etc/kubernetes/pki/etcd/server.key: öffne /etc/kubernetes/pki/etcd/server.crt: keine solche Datei oder kein solches Verzeichnis	Der Telegraf ReplicaSet-Pod soll auf einem Knoten ausgeführt werden, der als Master oder für etcd bestimmt ist. Wenn der ReplicaSet-Pod auf einem dieser Knoten nicht ausgeführt wird, werden diese Fehler angezeigt. Überprüfen Sie, ob Ihre Master-/etcd-Knoten Verunreinigungen aufweisen. Wenn dies der Fall ist, fügen Sie die erforderlichen Toleranzen zum Telegraf ReplicaSet, telegraf-rs, hinzu. Bearbeiten Sie beispielsweise das ReplicaSet … kubectl edit rs telegraf-rs … und fügen Sie der Spezifikation die entsprechenden Toleranzen hinzu. Starten Sie dann den ReplicaSet-Pod neu.

Problem:	Versuchen Sie Folgendes:
Ich habe eine PSP/PSA-Umgebung. Betrifft dies meinen Überwachungsbetreiber?	Wenn Ihr Kubernetes-Cluster mit Pod Security Policy (PSP) oder Pod Security Admission (PSA) ausgeführt wird, müssen Sie auf den neuesten Kubernetes Monitoring Operator aktualisieren. Befolgen Sie diese Schritte, um auf den aktuellen Operator mit Unterstützung für PSP/PSA zu aktualisieren: 1. Deinstallieren der vorherige Überwachungsoperator: kubectl delete agent agent-monitoring-netapp -n netapp-monitoring kubectl delete ns netapp-monitoring kubectl delete crd agents.monitoring.netapp.com kubectl delete clusterrole agent-manager-role agent-proxy-role agent-metrics-reader kubectl delete clusterrolebinding agent-manager-rolebinding agent-proxy-rolebinding agent-cluster-admin-rolebinding 2. Installieren die neueste Version des Überwachungsoperators.
Beim Versuch, den Operator bereitzustellen, sind mir Probleme begegnet, und ich verwende PSP/PSA.	1. Bearbeiten Sie den Agenten mit dem folgenden Befehl: kubectl -n <name-space> edit agent 2. Markieren Sie „security-policy-enabled“ als „false“. Dadurch werden die Pod-Sicherheitsrichtlinien und die Pod-Sicherheitszulassung deaktiviert und dem Operator die Bereitstellung ermöglicht. Bestätigen Sie mit den folgenden Befehlen: kubectl get psp (sollte anzeigen, dass die Pod-Sicherheitsrichtlinie entfernt wurde) kubectl get all -n <namespace>
grep -i psp (sollte anzeigen, dass nichts gefunden wurde)	„ImagePullBackoff“-Fehler aufgetreten
Diese Fehler können auftreten, wenn Sie über ein benutzerdefiniertes oder privates Docker-Repository verfügen und den Kubernetes Monitoring Operator noch nicht so konfiguriert haben, dass es ordnungsgemäß erkannt wird. Mehr lesen Informationen zur Konfiguration für benutzerdefinierte/private Repos.	Ich habe ein Problem mit der Bereitstellung meines Überwachungsoperators und die aktuelle Dokumentation hilft mir nicht bei der Lösung.

Problem:	Versuchen Sie Folgendes:

Erfassen oder notieren Sie die Ausgabe der folgenden Befehle und wenden Sie sich an das technische Supportteam.
 	
`kubectl -n netapp-monitoring get all`
`kubectl -n netapp-monitoring describe all`
`kubectl -n netapp-monitoring logs <monitoring-operator-pod> --all -containers=true`
`kubectl -n netapp-monitoring logs <telegraf-pod> --all -containers=true`
	Net-Observer-Pods (Workload Map) im Operator-Namespace befinden sich in CrashLoopBackOff

Diese Pods entsprechen dem Workload Map-Datensammler für die Netzwerkbeobachtung. Versuchen Sie Folgendes: • Überprüfen Sie die Protokolle eines der Pods, um die Mindestkernelversion zu bestätigen. Beispiel: ---- {"ci-tenant-id":"Ihre Mandanten-ID","collector-cluster":"Ihr K8S-Clustername","environment":"prod","level":"error","msg":"Validierung fehlgeschlagen. Grund: Kernelversion 3.10.0 ist niedriger als die Mindestkernelversion 4.18.0","time":"2022-11-09T08:23:08Z"} ---- • Net-Observer-Pods erfordern mindestens die Linux-Kernelversion 4.18.0. Überprüfen Sie die Kernelversion mit dem Befehl „uname -r“ und stellen Sie sicher, dass sie >= 4.18.0 ist	Pods werden im Operator-Namespace ausgeführt (Standard: Netapp-Monitoring), aber in der Benutzeroberfläche werden keine Daten für die Workload-Map oder Kubernetes-Metriken in Abfragen angezeigt.
Überprüfen Sie die Zeiteinstellung auf den Knoten des K8S-Clusters. Für eine genaue Prüfung und Datenberichterstattung wird dringend empfohlen, die Zeit auf dem Agent-Computer mithilfe des Network Time Protocol (NTP) oder Simple Network Time Protocol (SNTP) zu synchronisieren.	Einige der Net-Observer-Pods im Operator-Namespace befinden sich im Status „Ausstehend“
Net-Observer ist ein DaemonSet und führt in jedem Knoten des K8S-Clusters einen Pod aus. • Beachten Sie den Pod, der sich im Status „Ausstehend“ befindet, und prüfen Sie, ob ein Ressourcenproblem für die CPU oder den Speicher vorliegt. Stellen Sie sicher, dass im Knoten genügend Speicher und CPU verfügbar sind.	Unmittelbar nach der Installation des Kubernetes Monitoring Operator wird mir in meinen Protokollen Folgendes angezeigt: [inputs.prometheus] Fehler im Plug-In: Fehler beim Senden der HTTP-Anforderung an http://kube-state-metrics.<namespace>.svc.cluster.local:8080/metrics: Get http://kube-state-metrics.<namespace>.svc.cluster.local:8080/metrics: dial tcp: lookup kube-state-metrics.<namespace>.svc.cluster.local: no such host

Problem:	Versuchen Sie Folgendes:
Diese Meldung wird normalerweise nur angezeigt, wenn ein neuer Operator installiert wird und der *telegraf-rs*-Pod vor dem *ksm*-Pod aktiv ist. Diese Nachrichten sollten aufhören, sobald alle Pods ausgeführt werden.	Ich sehe keine erfassten Metriken für die in meinem Cluster vorhandenen Kubernetes-CronJobs.
Überprüfen Sie Ihre Kubernetes-Version (d. h. `kubectl version`). Wenn es sich um v1.20.x oder niedriger handelt, ist dies eine erwartete Einschränkung. Die mit dem Kubernetes Monitoring Operator bereitgestellte Version von kube-state-metrics unterstützt nur v1.CronJob. Bei Kubernetes 1.20.x und darunter befindet sich die CronJob-Ressource unter v1beta.CronJob. Aus diesem Grund kann kube-state-metrics die CronJob-Ressource nicht finden.	Nach der Installation des Operators treten die Telegraf-DS-Pods in CrashLoopBackOff ein und die Pod-Protokolle zeigen „su: Authentifizierungsfehler“ an.
Bearbeiten Sie den Telegraf-Abschnitt in *AgentConfiguration* und setzen Sie *dockerMetricCollectionEnabled* auf „false“. Weitere Einzelheiten finden Sie in der Betriebsanleitung des Betreibers."Konfigurationsoptionen" . … Spezifikation: … Telegraf: … - Name: Docker-Ausführungsmodus: - DaemonSet-Ersetzungen: - Schlüssel: DOCKER_UNIX_SOCK_PLACEHOLDER-Wert: unix:///run/docker.sock … …	In meinen Telegraf-Protokollen werden immer wieder Fehlermeldungen angezeigt, die den folgenden ähneln: E! [Agent] Fehler beim Schreiben in outputs.http: Post "https://<tenant_url>/rest/v1/lake/ingest/influxdb": Kontextfrist überschritten (Client.Timeout beim Warten auf Header überschritten)
Bearbeiten Sie den Telegraf-Abschnitt in *AgentConfiguration* und erhöhen Sie *outputTimeout* auf 10 s. Weitere Einzelheiten finden Sie in der Betriebsanleitung des Betreibers."Konfigurationsoptionen" .	Mir fehlen *involvedobject*-Daten für einige Ereignisprotokolle.
Stellen Sie sicher, dass Sie die Schritte in der"Berechtigungen" Abschnitt oben.	Warum werden zwei Überwachungsoperator-Pods ausgeführt, einer mit dem Namen netapp-ci-monitoring-operator-<pod> und der andere mit dem Namen monitoring-operator-<pod>?
Ab dem 12. Oktober 2023 hat Data Infrastructure Insights den Operator überarbeitet, um unseren Benutzern einen besseren Service zu bieten. Damit diese Änderungen vollständig übernommen werden können, müssen SieEntfernen Sie den alten Operator Undinstallieren Sie die neue .	Meine Kubernetes-Ereignisse wurden unerwartet nicht mehr an Data Infrastructure Insights gemeldet.
Rufen Sie den Namen des Event-Exporter-Pods ab: `kubectl -n netapp-monitoring get pods`	grep event-exporter

Problem:	Versuchen Sie Folgendes:
awk '{print $1}'	sed 's/event-exporter./event-exporter/'` Es sollte entweder „netapp-ci-event-exporter“ oder „event-exporter“ sein. Bearbeiten Sie als Nächstes den Überwachungsagenten `kubectl -n netapp-monitoring edit agent` und legen Sie den Wert für LOG_FILE so fest, dass er den entsprechenden Event-Exporter-Pod-Namen widerspiegelt, der im vorherigen Schritt gefunden wurde. Genauer gesagt sollte LOG_FILE entweder auf "/var/log/containers/netapp-ci-event-exporter.log" oder "/var/log/containers/event-exporter*.log" gesetzt werden. …. fluent-bit: … - name: event-exporter-ci substitutions: - key: LOG_FILE values: - /var/log/containers/netapp-ci-event-exporter*.log … …. Alternativ kann man auchdeinstallieren UndNeuinstallation der Agent.
Ich sehe, dass vom Kubernetes Monitoring Operator bereitgestellte Pods aufgrund unzureichender Ressourcen abstürzen.	Siehe den Kubernetes Monitoring Operator"Konfigurationsoptionen" um die CPU- und/oder Speichergrenzen nach Bedarf zu erhöhen.
Ein fehlendes Image oder eine ungültige Konfiguration führte dazu, dass die netapp-ci-kube-state-metrics-Pods nicht gestartet werden konnten oder nicht bereit waren. Jetzt steckt das StatefulSet fest und Konfigurationsänderungen werden nicht auf die Netapp-CI-Kube-State-Metrics-Pods angewendet.	Das StatefulSet ist in einem"gebrochen" Zustand. Nachdem Sie alle Konfigurationsprobleme behoben haben, führen Sie einen Bounce der Netapp-CI-Kube-State-Metrics-Pods durch.
netapp-ci-kube-state-metrics-Pods können nach der Ausführung eines Kubernetes Operator-Upgrades nicht gestartet werden und lösen ErrImagePull aus (das Abrufen des Images schlägt fehl).	Versuchen Sie, die Pods manuell zurückzusetzen.
Bei der Protokollanalyse werden für meinen Kubernetes-Cluster Meldungen vom Typ „Ereignis verworfen, da es älter ist als maxEventAgeSeconds“ beobachtet.	Ändern Sie die Operator-Agentenkonfiguration und erhöhen Sie *event-exporter-maxEventAgeSeconds* (z. B. auf 60 s), *event-exporter-kubeQPS* (z. B. auf 100) und *event-exporter-kubeBurst* (z. B. auf 500). Weitere Einzelheiten zu diesen Konfigurationsoptionen finden Sie im"Konfigurationsoptionen" Seite.

Problem:	Versuchen Sie Folgendes:
Telegraf warnt vor unzureichendem sperrbaren Speicher oder stürzt ab.	Versuchen Sie, das Limit des sperrbaren Speichers für Telegraf im zugrunde liegenden Betriebssystem/Knoten zu erhöhen. Wenn eine Erhöhung des Limits keine Option ist, ändern Sie die NKMO-Agentenkonfiguration und setzen Sie *unprotected* auf *true*. Dadurch wird Telegraf angewiesen, keinen Versuch zu unternehmen, gesperrte Speicherseiten zu reservieren. Dies kann zwar ein Sicherheitsrisiko darstellen, da entschlüsselte Geheimnisse möglicherweise auf die Festplatte ausgelagert werden, ermöglicht jedoch die Ausführung in Umgebungen, in denen die Reservierung gesperrten Speichers nicht möglich ist. Weitere Informationen zu den *ungeschützten* Konfigurationsoptionen finden Sie im"Konfigurationsoptionen" Seite.
Ich sehe Warnmeldungen von Telegraf, die etwa wie folgt aussehen: *W! [inputs.diskio] Der Datenträgername für „vdc“ konnte nicht ermittelt werden: Fehler beim Lesen von /dev/vdc: keine solche Datei oder kein solches Verzeichnis*	Für den Kubernetes Monitoring Operator sind diese Warnmeldungen harmlos und können ignoriert werden. Alternativ können Sie den Abschnitt „Telegraf“ in der AgentConfiguration bearbeiten und *runDsPrivileged* auf „true“ setzen. Weitere Einzelheiten finden Sie im"Konfigurationsoptionen des Betreibers" .

Problem:	Versuchen Sie Folgendes:

Mein Fluent-Bit-Pod schlägt mit den folgenden Fehlern fehl: [2024/10/16 14:16:23] [Fehler] [/src/fluent-bit/plugins/in_tail/tail_fs_inotify.c:360 errno=24] Zu viele offene Dateien [2024/10/16 14:16:23] [Fehler] Initialisierung der Eingabe tail.0 fehlgeschlagen [2024/10/16 14:16:23] [Fehler] [Engine] Initialisierung der Eingabe fehlgeschlagen	Versuchen Sie, Ihre *fsnotify*-Einstellungen in Ihrem Cluster zu ändern:
	`sudo sysctl fs.inotify.max_user_instances (take note of setting)`
	`sudo sysctl fs.inotify.max_user_instances=<something larger than current setting>`
	`sudo sysctl fs.inotify.max_user_watches (take note of setting)`
	`sudo sysctl fs.inotify.max_user_watches=<something larger than current setting>`
	Starten Sie Fluent-bit neu.
	Hinweis: Um diese Einstellungen auch nach einem Neustart des Knotens dauerhaft zu halten, müssen Sie die folgenden Zeilen in */etc/sysctl.conf* einfügen.
	`fs.inotify.max_user_instances=<something larger than current setting>`
	`fs.inotify.max_user_watches=<something larger than current setting>`

Problem:	Versuchen Sie Folgendes:
Die Telegraf DS-Pods melden Fehler im Zusammenhang mit dem Kubernetes-Eingabe-Plugin, das keine HTTP-Anfragen stellen kann, da das TLS-Zertifikat nicht validiert werden kann. Zum Beispiel: E! [inputs.kubernetes] Fehler im Plugin: Fehler beim Senden einer HTTP-Anfrage an"<a href="https://<kubelet_IP>:10250/stats/summary": " class="bare">https://<kubelet_IP>:10250/stats/summary": Erhalten"<a href="https://<kubelet_IP>:10250/stats/summary": " class="bare">https://<kubelet_IP>:10250/stats/summary": tls: Zertifikat konnte nicht überprüft werden: x509: Zertifikat für <kubelet_IP> kann nicht validiert werden, da es keine IP-SANs enthält	Dies tritt auf, wenn das Kubelet selbstsignierte Zertifikate verwendet und/oder das angegebene Zertifikat die <kubelet_IP> nicht in der Liste „Subject Alternative Name“ des Zertifikats enthält. Um dieses Problem zu lösen, kann der Benutzer die"Agentenkonfiguration" , und setzen Sie *telegraf:insecureK8sSkipVerify* auf *true*. Dadurch wird das Telegraf-Eingabe-Plugin so konfiguriert, dass die Überprüfung übersprungen wird. Alternativ kann der Benutzer das Kubelet konfigurieren für"serverTLSBootstrap" , wodurch eine Zertifikatsanforderung von der API „certificates.k8s.io“ ausgelöst wird.

Weitere Informationen finden Sie in der"Support" Seite oder in der"Datensammler-Supportmatrix" .

Memcached-Datensammler

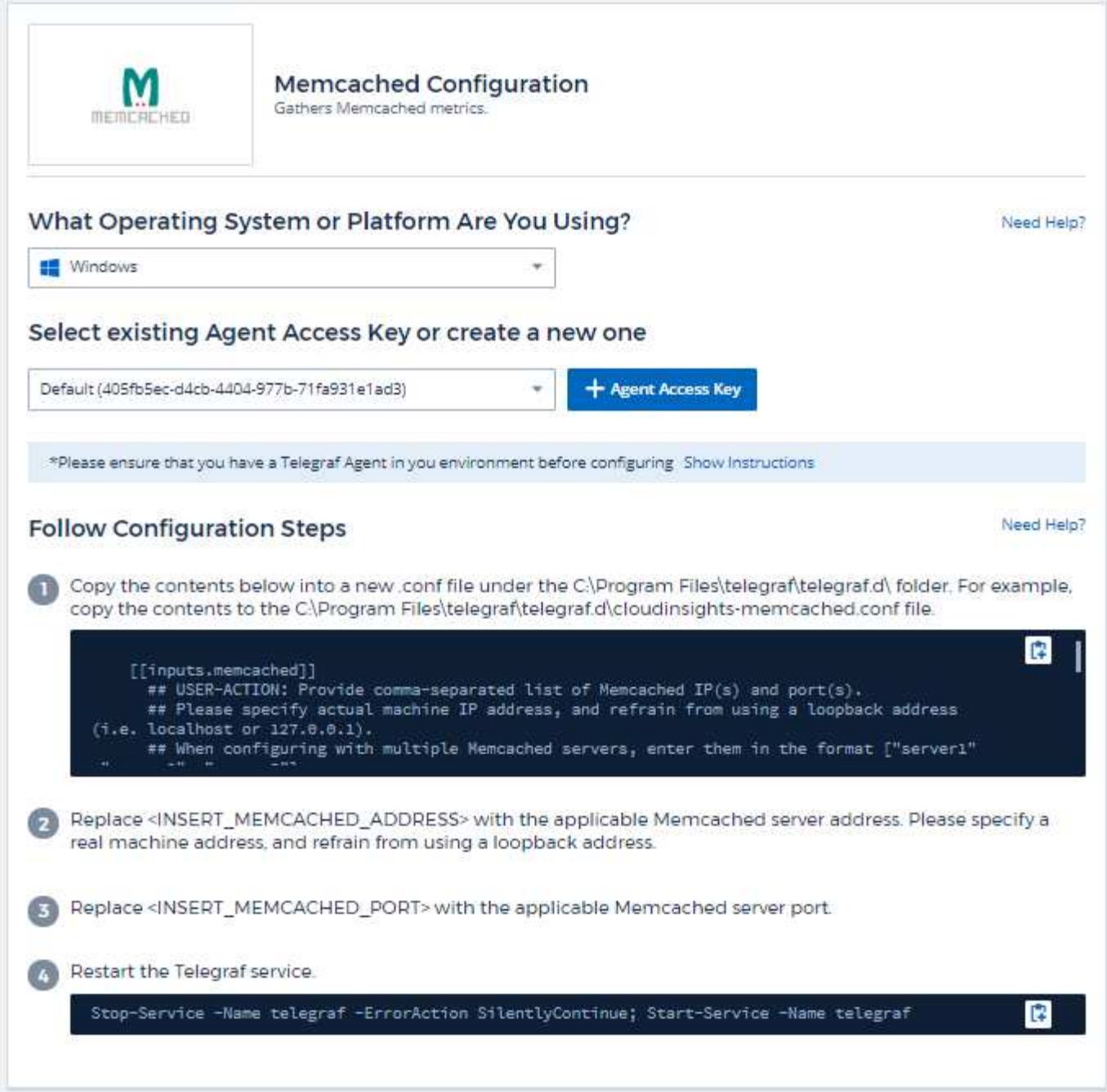
Data Infrastructure Insights verwendet diesen Datensammler, um Metriken von Memcached zu sammeln.

Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie Memcached.

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

2. Wenn Sie noch keinen Agenten für die Sammlung installiert haben oder einen Agenten für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das"Agenteninstallation" Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel zur Verwendung mit diesem Datensammler aus. Sie können einen neuen Agentenzugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agentenzugriffsschlüssel** klicken. Best Practice: Verwenden Sie nur dann einen anderen Agent-Zugriffsschlüssel, wenn Sie Datensammler beispielsweise nach Betriebssystem/Plattform gruppieren möchten.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen variieren je nach Art des Betriebssystems oder der Plattform, die Sie zum Sammeln von Daten verwenden.



Aufstellen

Informationen finden Sie im"Memcached-Wiki" .

Objekte und Zähler

Die folgenden Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Merkmale:	Datenpunkte:
Memcached	Namespace-Server	Knoten-IP Knotenname	Verbindungen annehmen Bearbeitete Authentifizierungsanfragen Fehlgeschlagene Authentifizierungen Verwendete Bytes Gelesene Bytes (pro Sek.) Geschriebene Bytes (pro Sek.) CAS Badval CAS-Treffer CAS-Fehlschläge Flush-Anforderungen (pro Sek.) Get-Anforderungen (pro Sek.) Set-Anforderungen (pro Sek.) Touch-Anforderungen (pro Sek.) Verbindungserträge (pro Sek.) Verbindungsstrukturen Offene Verbindungen Aktuell gespeicherte Elemente Decr-Anforderungen Treffer (pro Sek.) Decr-Anforderungen Fehlschläge (pro Sek.) Löschanforderungen Treffer (pro Sek.) Löschanforderungen Fehlschläge (pro Sek.) Ausgewiesene Elemente Gültige Ausweisungen Abgelaufene Elemente Get-Treffer (pro Sek.) Get-Fehlschläge (pro Sek.) Verwendete Hash-Bytes Hash wird erweitert Hash-Leistungsstufe Incr-Anforderungen Treffer (pro Sek.) Incr-Anforderungen Fehlschläge (pro Sek.) Server Max. Bytes Listen Deaktiviert Anzahl zurückgeforderte Worker-Threads Anzahl insgesamt geöffnete Verbindungen

Fehlerbehebung

Weitere Informationen finden Sie in der"Support" Seite.

MongoDB-Datensammler

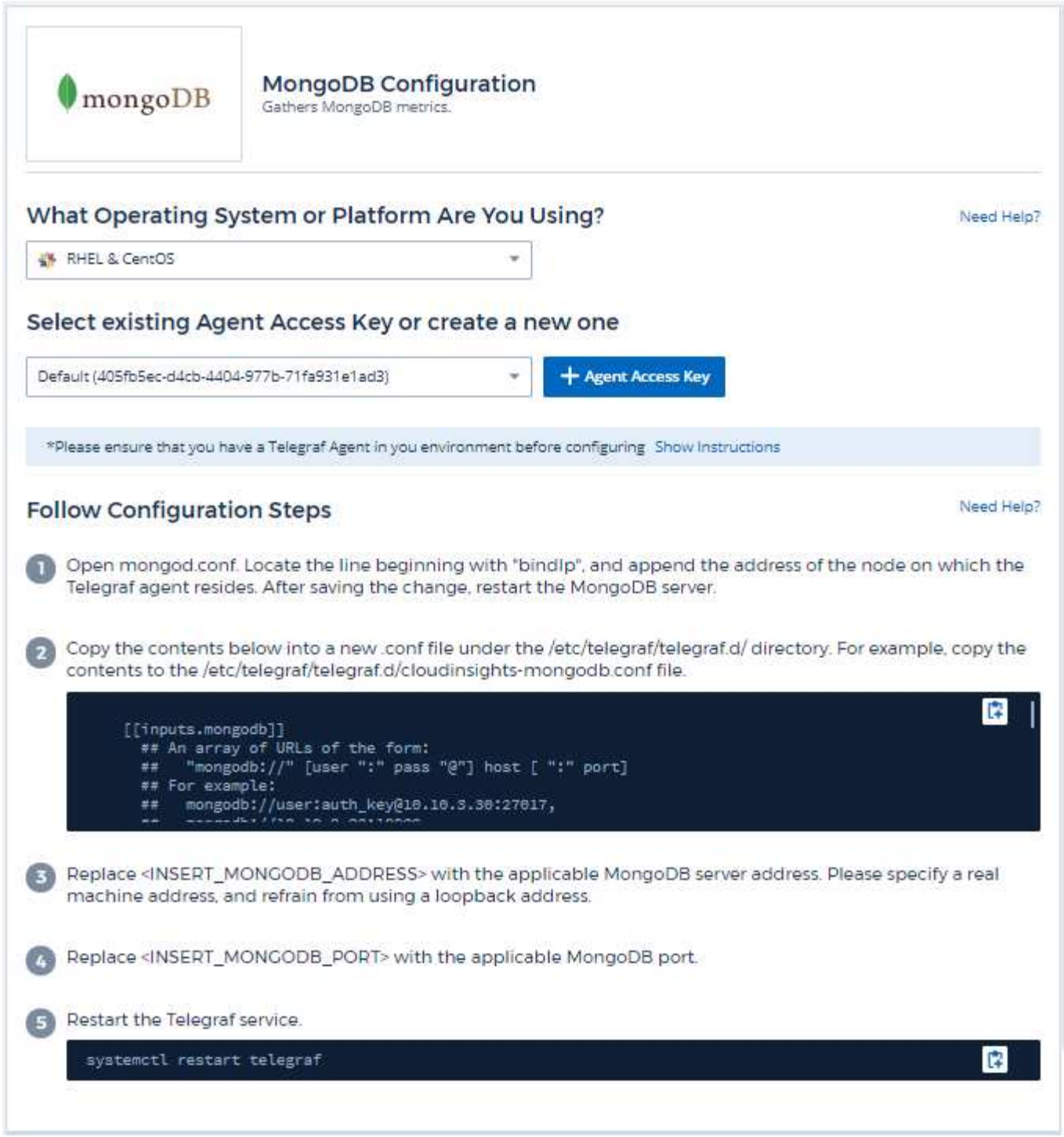
Data Infrastructure Insights verwendet diesen Datensammler, um Metriken von MongoDB zu sammeln.

Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie MongoDB.

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

2. Wenn Sie noch keinen Agenten für die Sammlung installiert haben oder einen Agenten für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das"Agenteninstallation" Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel zur Verwendung mit diesem Datensammler aus. Sie können einen neuen Agentenzugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agentenzugriffsschlüssel** klicken. Best Practice: Verwenden Sie nur dann einen anderen Agent-Zugriffsschlüssel, wenn Sie Datensammler beispielsweise nach Betriebssystem/Plattform gruppieren möchten.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen variieren je nach Art des Betriebssystems oder der Plattform, die Sie zum Sammeln von Daten verwenden.



Aufstellen

Informationen finden Sie im"MongoDB-Dokumentation" .

Objekte und Zähler

Die folgenden Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Merkmale:	Datenpunkte:
MongoDB	Namespace-Hostname		

Objekt:	Kennungen:	Merkmale:	Datenpunkte:
MongoDB-Datenbank	Namespace Hostname Datenbankname		

Fehlerbehebung

Informationen finden Sie im"Support" Seite.

MySQL-Datensammler

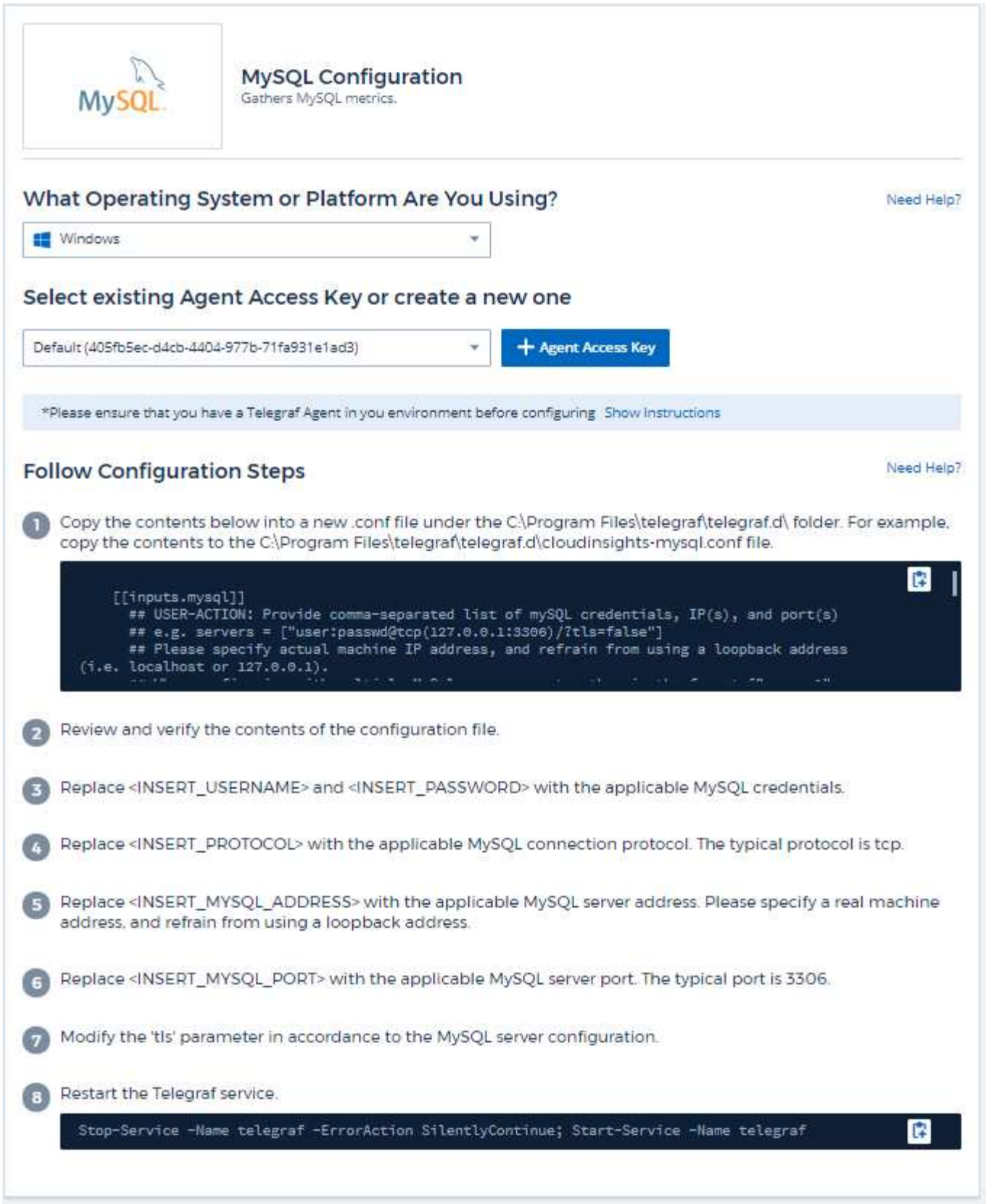
Data Infrastructure Insights verwendet diesen Datensammler, um Metriken aus MySQL zu sammeln.

Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie MySQL.

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

2. Wenn Sie noch keinen Agenten für die Sammlung installiert haben oder einen Agenten für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das"Agenteninstallation" Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel zur Verwendung mit diesem Datensammler aus. Sie können einen neuen Agentenzugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agentenzugriffsschlüssel** klicken. Best Practice: Verwenden Sie nur dann einen anderen Agent-Zugriffsschlüssel, wenn Sie Datensammler beispielsweise nach Betriebssystem/Plattform gruppieren möchten.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen variieren je nach Art des Betriebssystems oder der Plattform, die Sie zum Sammeln von Daten verwenden.



Aufstellen

Informationen finden Sie im"MySQL-Dokumentation" .

Objekte und Zähler

Die folgenden Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Merkmale:	Datenpunkte:
MySQL	Namespace MySQL-Server	Knoten-IP Knotenname	Abgebrochene Clients (pro Sek.) Abgebrochene Verbindungen (pro Sek.) RX-Bytes (pro Sek.) TX-Bytes (pro Sek.) Befehle Admin (pro Sek.) Befehle Ereignis ändern Befehle Funktion ändern Befehle Instanz ändern Befehle Prozedur ändern Befehle Server ändern Befehle Tabelle ändern Befehle Tablespace ändern Befehle Benutzer ändern Befehle Analysieren Befehle Zu Keycache zuweisen Befehle Beginnen Befehle Binlog Befehle Prozedur aufrufen Befehle DB ändern Befehle Master ändern Befehle Repl ändern Filterbefehle Prüfen Befehle Prüfsummenbefehle Commit Befehle DB erstellen Befehle Ereignis erstellen Befehle Funktion erstellen Befehle Index erstellen Befehle Prozedur erstellen Befehle Server erstellen Befehle Tabelle erstellen Befehle Trigger erstellen Befehle UDF erstellen Befehle Benutzer erstellen Befehle Ansicht erstellen Befehle Dealloc SQL-Verbindungsfehler Akzeptieren Erstellte temporäre Datenträgertabellen Verzögerte Fehler Befehle leeren Handler Commit InnoDB-Pufferpool Bytes Daten Schlüsselblöcke nicht geleert Schlüsselleseanforderungen Schlüsselschreibanforderungen Schlüsselschreibvorgänge Max. Ausführungszeit überschritten Max. verwendete Verbindungen Geöffnete Dateien

Fehlerbehebung

Weitere Informationen finden Sie in der"Support" Seite.

Netstat-Datensammler

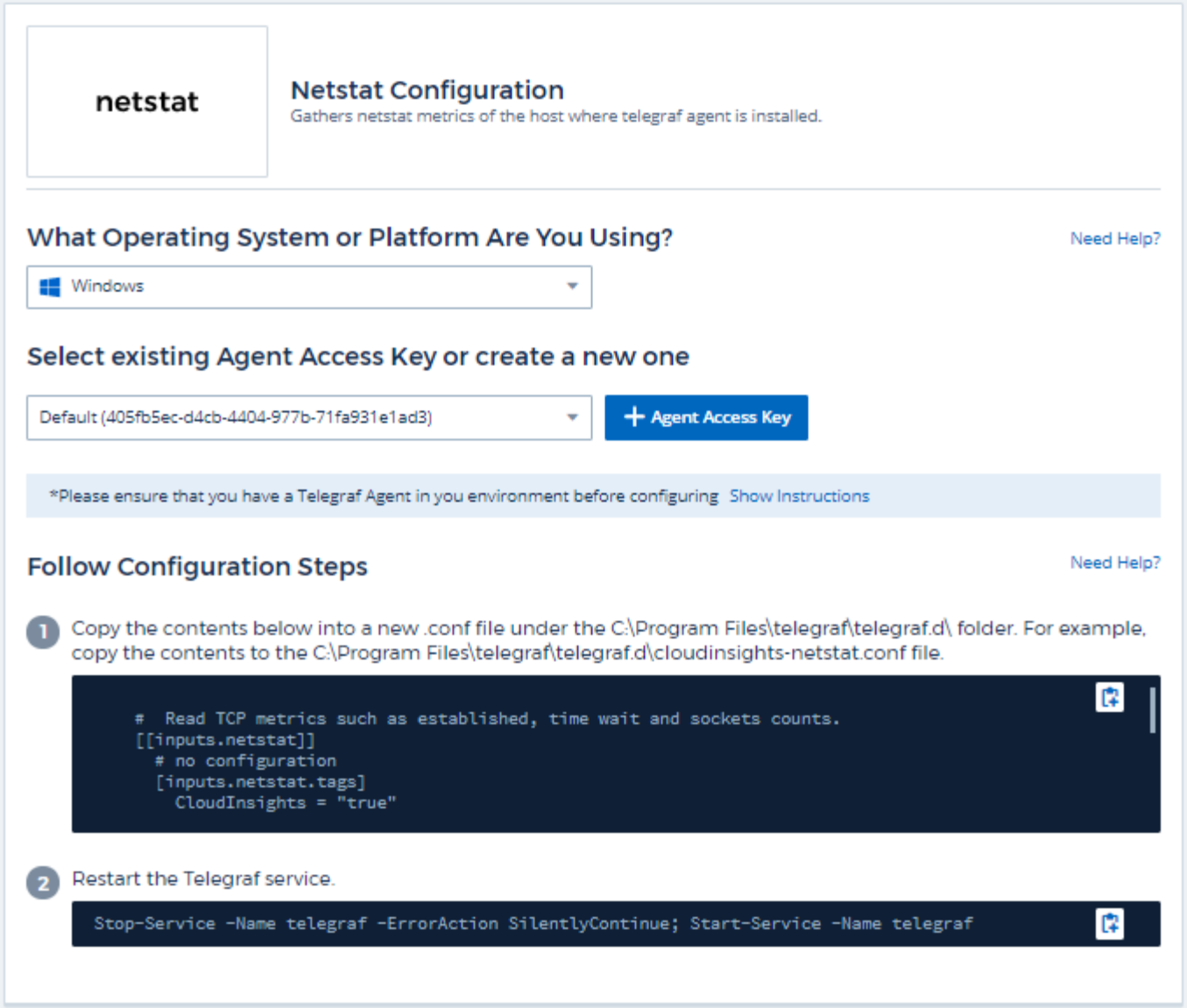
Data Infrastructure Insights verwendet diesen Datensammler, um Netstat-Metriken zu erfassen.

Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie Netstat.

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

2. Wenn Sie noch keinen Agenten für die Sammlung installiert haben oder einen Agenten für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das"Agenteninstallation" Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel zur Verwendung mit diesem Datensammler aus. Sie können einen neuen Agentenzugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agentenzugriffsschlüssel** klicken. Best Practice: Verwenden Sie nur dann einen anderen Agent-Zugriffsschlüssel, wenn Sie Datensammler beispielsweise nach Betriebssystem/Plattform gruppieren möchten.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen variieren je nach Art des Betriebssystems oder der Plattform, die Sie zum Sammeln von Daten verwenden.



Aufstellen

Objekte und Zähler

Die folgenden Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Merkmale:	Datenpunkte:
Netstat	Knoten-UUID	Knoten-IP Knotenname	

Fehlerbehebung

Weitere Informationen finden Sie in der"Support" Seite.

Nginx-Datensammler

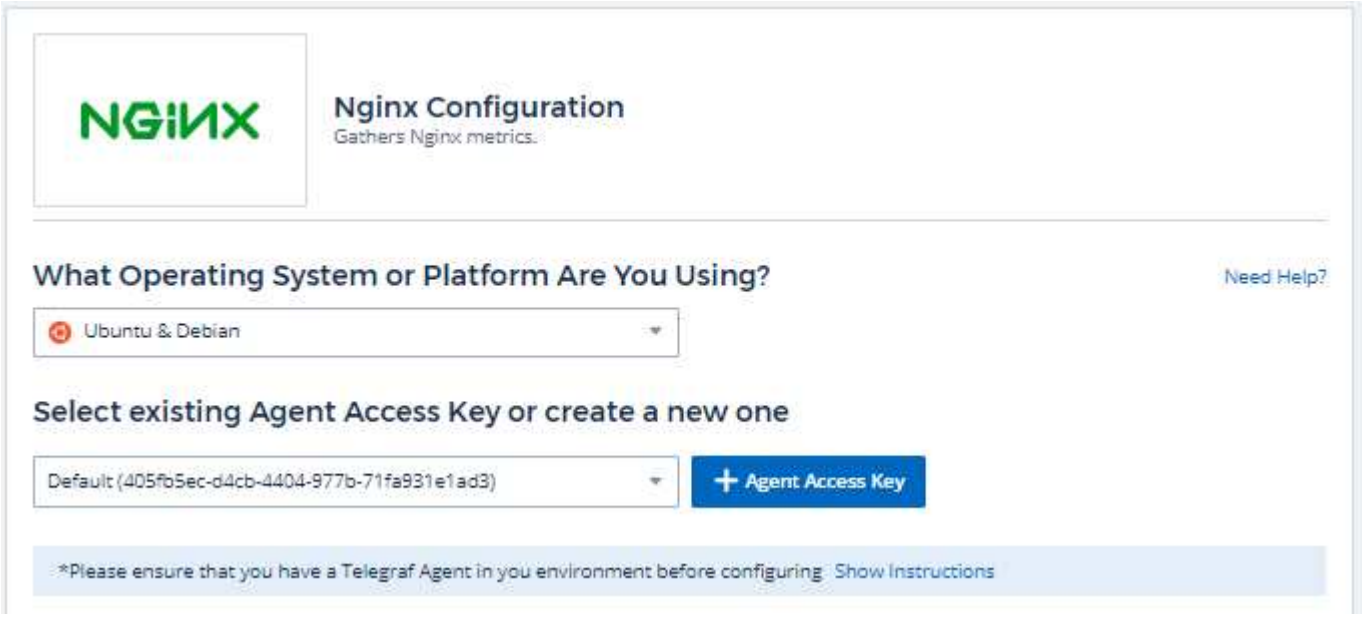
Data Infrastructure Insights verwendet diesen Datensammler, um Metriken von Nginx zu sammeln.

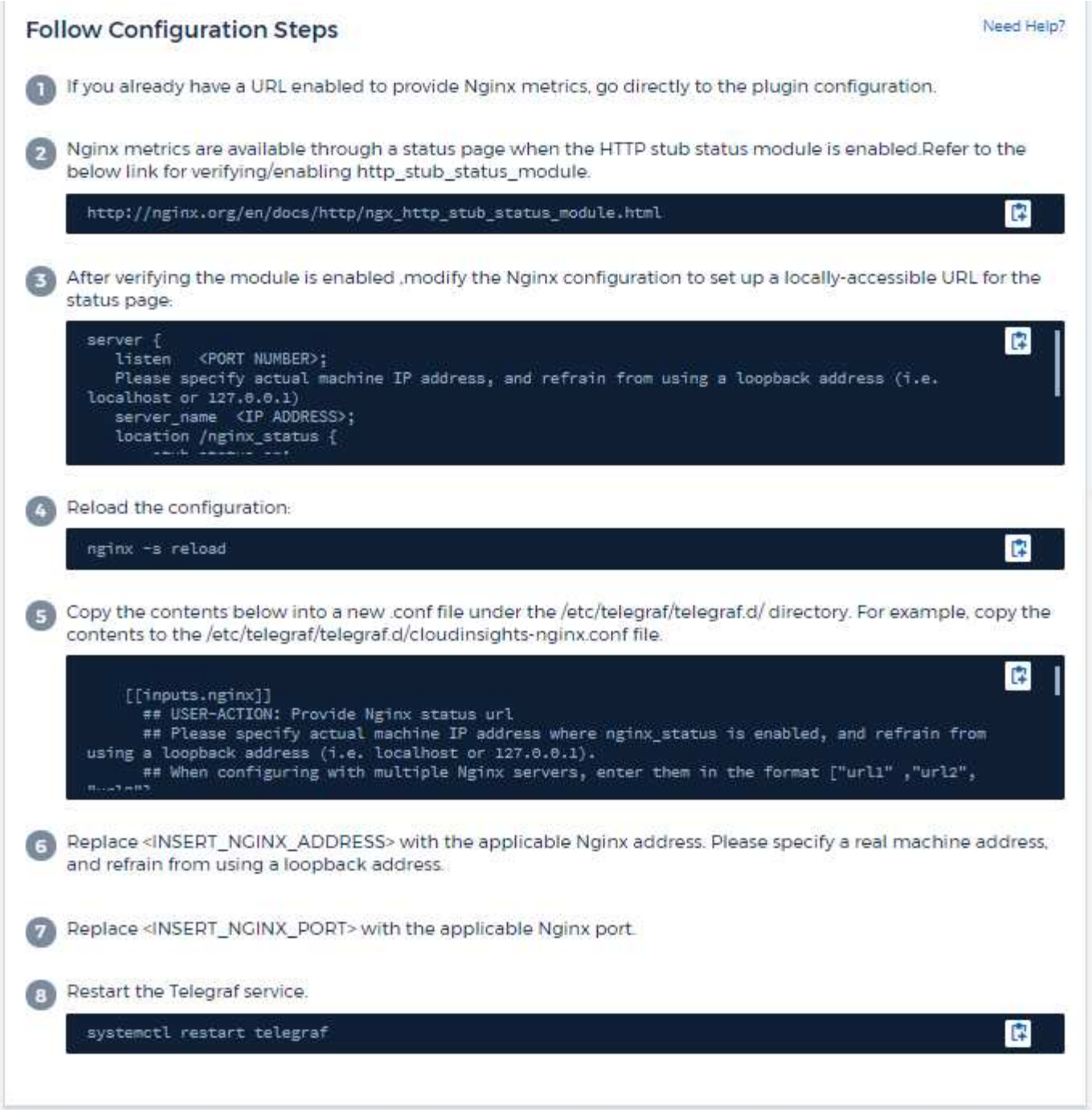
Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie Nginx.

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

2. Wenn Sie noch keinen Agenten für die Sammlung installiert haben oder einen Agenten für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das"Agenteninstallation" Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel zur Verwendung mit diesem Datensammler aus. Sie können einen neuen Agentenzugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agentenzugriffsschlüssel** klicken. Best Practice: Verwenden Sie nur dann einen anderen Agent-Zugriffsschlüssel, wenn Sie Datensammler beispielsweise nach Betriebssystem/Plattform gruppieren möchten.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen variieren je nach Art des Betriebssystems oder der Plattform, die Sie zum Sammeln von Daten verwenden.





Aufstellen

Die Nginx-Metriksammlung erfordert, dass Nginx"http_stub_status_module" aktiviert werden.

Weitere Informationen finden Sie in der"Nginx-Dokumentation" .

Objekte und Zähler

Die folgenden Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Merkmale:	Datenpunkte:
Nginx	Namespace-Server	Knoten-IP Knotenname Port	Akzeptiert Aktive bearbeitete Leseanfragen Wartende Schreibanfragen

Fehlerbehebung

Weitere Informationen finden Sie in der"Support" Seite.

PostgreSQL-Datensammler

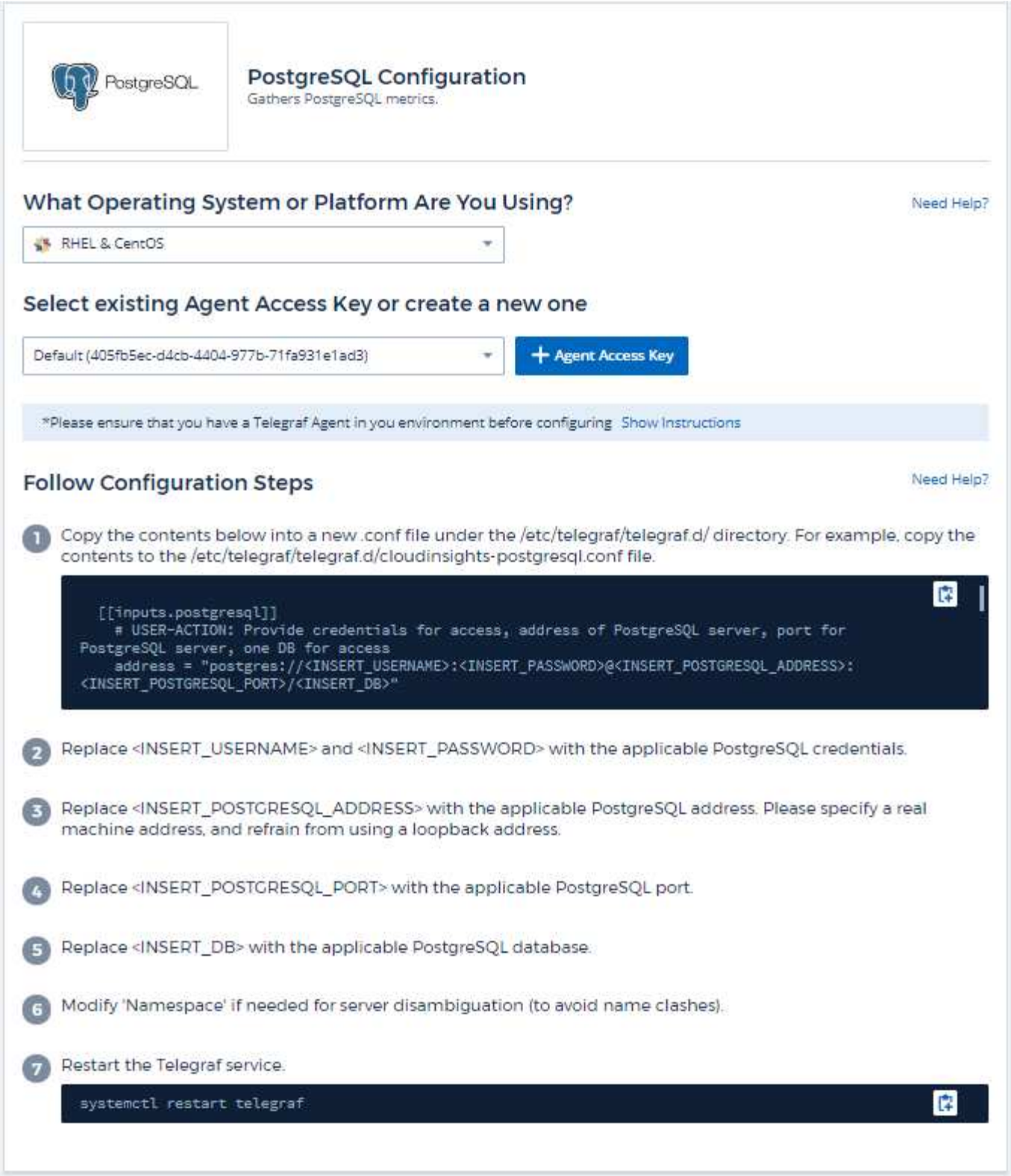
Data Infrastructure Insights verwendet diesen Datensammler, um Metriken von PostgreSQL zu sammeln.

Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie PostgreSQL.

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

2. Wenn Sie noch keinen Agenten für die Sammlung installiert haben oder einen Agenten für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das"Agenteninstallation" Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel zur Verwendung mit diesem Datensammler aus. Sie können einen neuen Agentenzugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agentenzugriffsschlüssel** klicken. Best Practice: Verwenden Sie nur dann einen anderen Agent-Zugriffsschlüssel, wenn Sie Datensammler beispielsweise nach Betriebssystem/Plattform gruppieren möchten.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen variieren je nach Art des Betriebssystems oder der Plattform, die Sie zum Sammeln von Daten verwenden.



Aufstellen

Informationen finden Sie im"PostgreSQL-Dokumentation" .

Objekte und Zähler

Die folgenden Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Merkmale:	Datenpunkte:
PostgreSQL-Server	Namespace-Datenbankserver	Knotenname Knoten-IP	Puffer Zugewiesene Puffer Backend-Puffer Backend-Dateisynchronisierungspuffer Checkpoint-Puffer Saubere Checkpoints Synchronisierungszeit Checkpoints Schreibzeit Checkpoints Anfragen Checkpoints Zeitlich begrenzt Max Geschrieben Sauber
PostgreSQL-Datenbank	Namespace-Datenbankserver	Datenbank-OID Knotenname Knoten-IP	Blöcke Lesezeit Blöcke Schreibzeit Blöcke Treffer Blöcke Lesevorgänge Konflikte Deadlocks Client Anzahl Temp. Dateien Bytes Temp. Dateien Anzahl Zeilen Gelöschte Zeilen Abgerufene Zeilen Eingefügte Zeilen Zurückgegebene Zeilen Aktualisierte Transaktionen Festgeschriebene Transaktionen Zurückgesetzte Transaktionen

Fehlerbehebung

Weitere Informationen finden Sie in der"Support" Seite.

Puppet Agent-Datensammler

Data Infrastructure Insights verwendet diesen Datensammler, um Metriken von Puppet Agent zu sammeln.

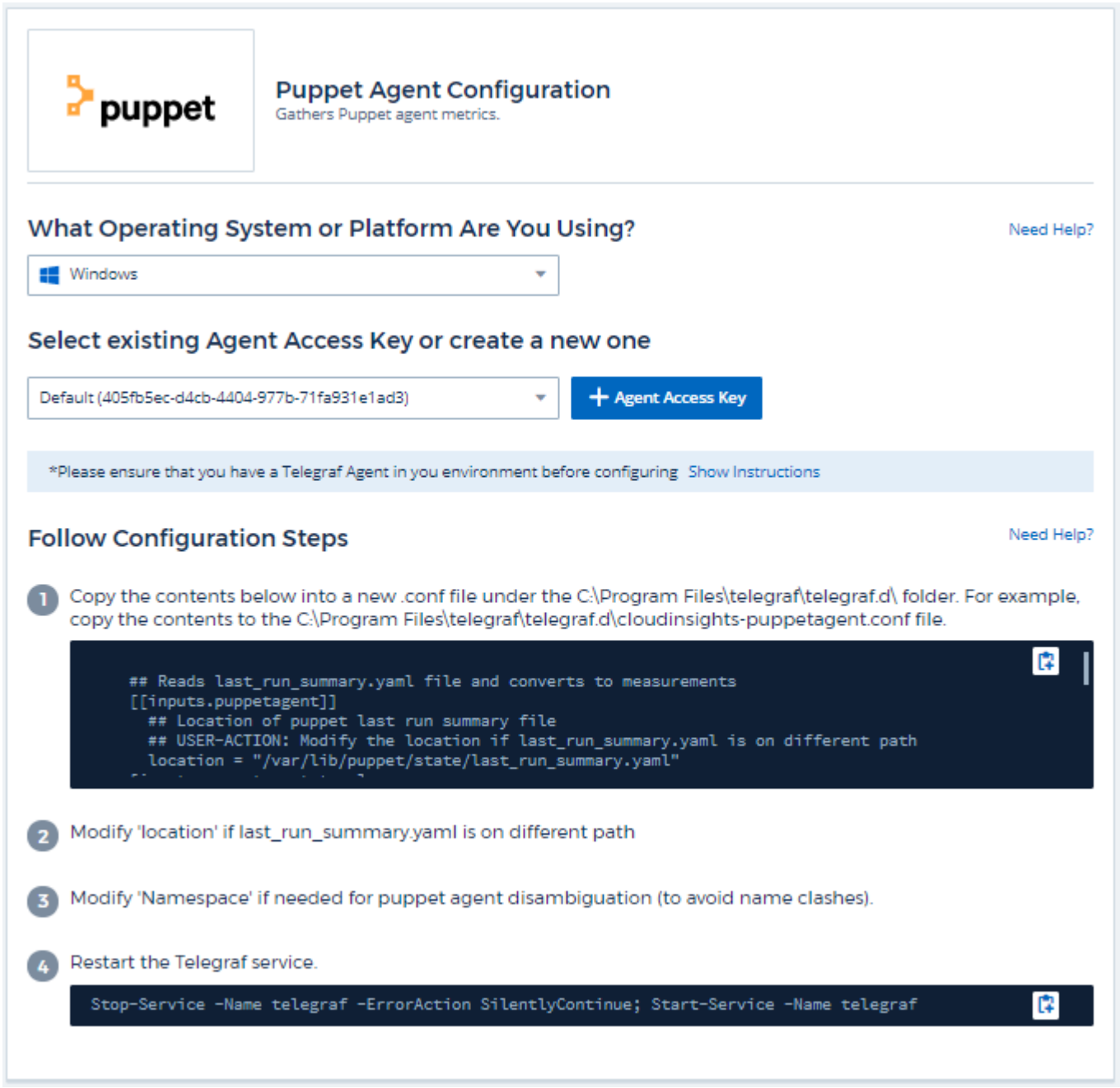
Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie Puppet.

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

2. Wenn Sie noch keinen Agenten für die Sammlung installiert haben oder einen Agenten für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das"Agenteninstallation" Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel zur Verwendung mit diesem Datensammler aus. Sie können einen neuen Agentenzugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agentenzugriffsschlüssel** klicken. Best Practice: Verwenden Sie nur dann einen anderen Agent-Zugriffsschlüssel, wenn Sie Datensammler beispielsweise nach Betriebssystem/Plattform gruppieren möchten.

4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen variieren je nach Art des Betriebssystems oder der Plattform, die Sie zum Sammeln von Daten verwenden.



Aufstellen

Informationen finden Sie im "Puppet-Dokumentation"

Objekte und Zähler

Die folgenden Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Merkmale:	Datenpunkte:

Puppenagent	Namespace-Knoten-UUID	Knotenname Standort Knoten-IP-Version Konfigurationszeichenfolge-Version Puppet	Änderungen Gesamtereignisse Fehlerereignisse Erfolgsereignisse Gesamtressourcen Geänderte Ressourcen Fehlgeschlagene Ressourcen Neustart fehlgeschlagene Ressourcen Nicht synchronisierte Ressourcen Neu gestartete Ressourcen Geplante Ressourcen Übersprungene Ressourcen Gesamtzeit Ankerzeit Konfigurationsabrufzeit Cron-Zeit Ausführungszeit Dateizeit Filebucket-Zeit Lastrun-Zeit Paketzeit Zeitplanzeit Servicezeit Sshauthorizedkey-Zeit Gesamtzeit Benutzer

Fehlerbehebung

Weitere Informationen finden Sie in der"Support" Seite.

Redis-Datensammler

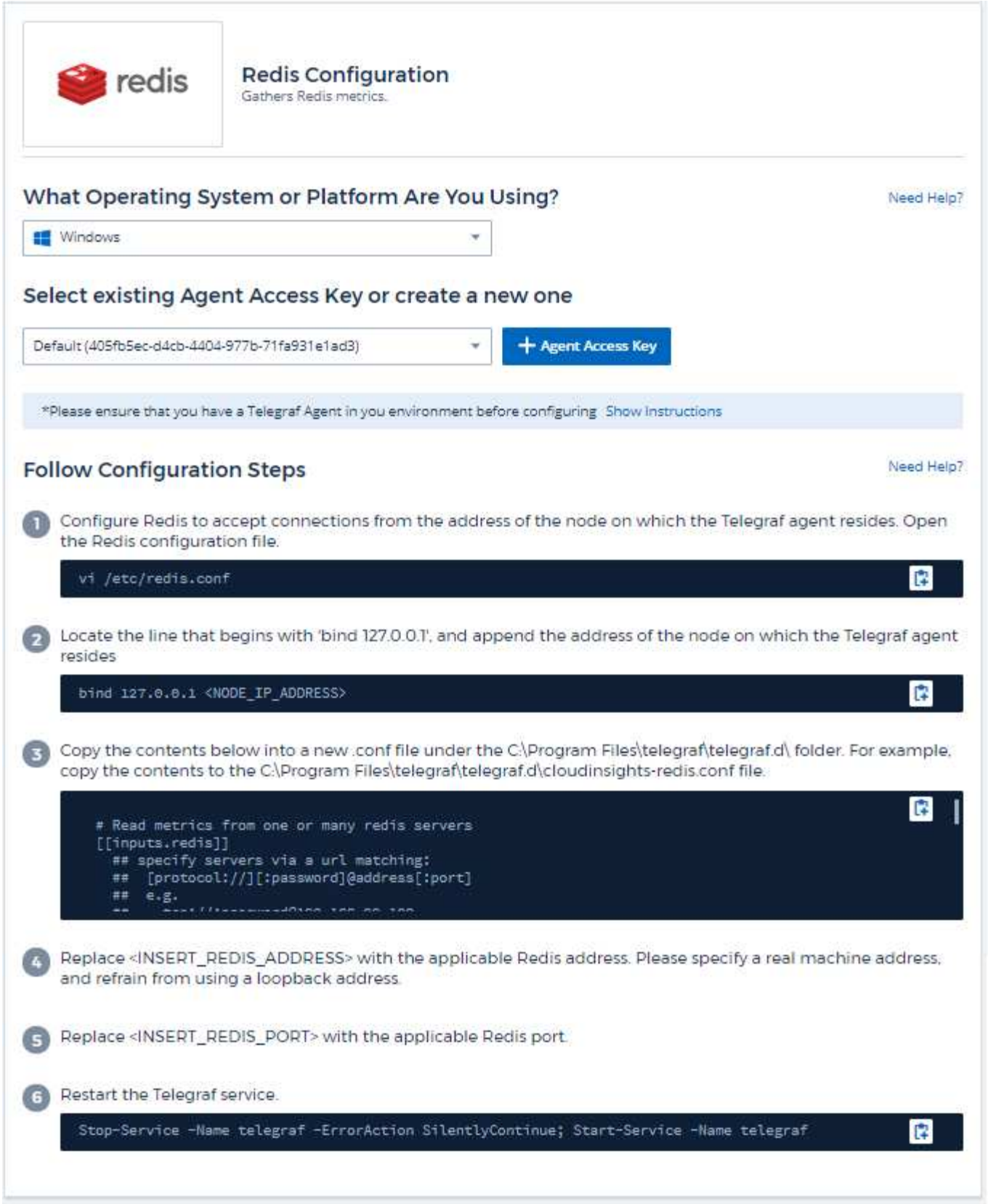
Data Infrastructure Insights verwendet diesen Datensammler, um Metriken von Redis zu sammeln. Redis ist ein Open-Source-Datenstrukturspeicher im Arbeitsspeicher, der als Datenbank, Cache und Nachrichtenbroker verwendet wird und die folgenden Datenstrukturen unterstützt: Zeichenfolgen, Hashes, Listen, Sets und mehr.

Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie Redis.

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

2. Wenn Sie noch keinen Agenten für die Sammlung installiert haben oder einen Agenten für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das"Agenteninstallation" Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel zur Verwendung mit diesem Datensammler aus. Sie können einen neuen Agentenzugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agentenzugriffsschlüssel** klicken. Best Practice: Verwenden Sie nur dann einen anderen Agent-Zugriffsschlüssel, wenn Sie Datensammler beispielsweise nach Betriebssystem/Plattform gruppieren möchten.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen variieren je nach Art des Betriebssystems oder der Plattform, die Sie zum Sammeln von Daten verwenden.



Aufstellen

Informationen finden Sie im"Redis-Dokumentation" .

Objekte und Zähler

Die folgenden Objekte und ihre Zähler werden gesammelt:

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

Fehlerbehebung

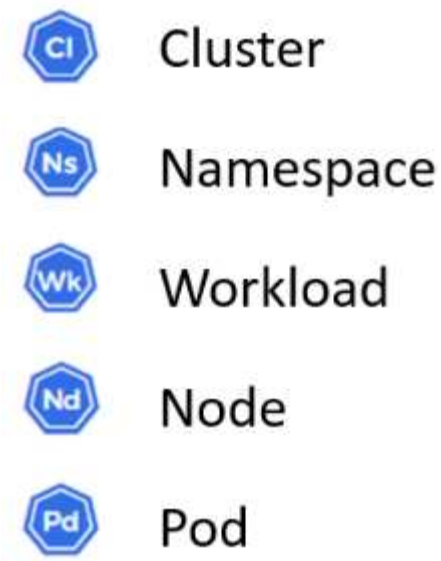
Weitere Informationen finden Sie in der"Support" Seite.

Objektsymbolreferenz

In Data Infrastructure Insights verwendete Objektsymbole.

Infrastruktursymbole:

Kubernetes-Symbole:



Überwachung der Netzwerkleistung von Kubernetes und Kartensymbole:

Rechtliche Hinweise

Rechtliche Hinweise bieten Zugriff auf Urheberrechtserklärungen, Marken, Patente und mehr.

Copyright

"https://www.netapp.com/company/legal/copyright/"

Marken

NETAPP, das NETAPP-Logo und die auf der NetApp -Markenseite aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen- und Produktnamen können Marken ihrer jeweiligen Eigentümer sein.

"https://www.netapp.com/company/legal/trademarks/"

Patente

Eine aktuelle Liste der Patente im Besitz von NetApp finden Sie unter:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Datenschutzrichtlinie

"https://www.netapp.com/company/legal/privacy-policy/"

Open Source

Hinweisdateien enthalten Informationen zu Urheberrechten und Lizenzen Dritter, die in der NetApp -Software verwendet werden.

"Hinweis zu Data Infrastructure Insights (ehemals Cloud Insights)"

"Hinweis zur Workload-Sicherheit (früher Cloud Secure)"

Copyright-Informationen

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers 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, BEISPIELHAFTE 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 IRGENDEINER 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.