



Documentação do Data Infrastructure Insights

Data Infrastructure Insights

NetApp
December 19, 2024

Índice

Documentação do Data Infrastructure Insights	1
O que o Data Infrastructure Insights pode fazer por mim?	1
Como começar	1
Novidades do Data Infrastructure Insights	2
Dezembro de 2024	2
Novembro de 2024	4
Outubro de 2024	5
Setembro de 2024	8
Agosto de 2024	8
Julho de 2024	10
Junho de 2024	11
Maio de 2024	11
Abril de 2024	12
Março de 2024	13
Fevereiro de 2024	14
Janeiro de 2024	17
Dezembro de 2023	18
Novembro de 2023	21
Outubro de 2023	22
Setembro de 2023	24
Agosto de 2023	27
Julho de 2023	30
Junho de 2023	33
Maio de 2023	34
Abril de 2023	35
Março de 2023	38
Janeiro de 2023	39
Dezembro de 2022	39
Novembro de 2022	41
Outubro de 2022	41
Setembro de 2022	42
Agosto de 2022	43
Junho de 2022	48
Maio de 2022	51
Abril de 2022	53
Março de 2022	55
Fevereiro de 2022	56
Dezembro de 2021	57
Novembro de 2021	59
Outubro de 2021	61
Setembro de 2021	62
Agosto de 2021	63
Junho de 2021	64

Maio de 2021	67
Abril de 2021	68
Fevereiro de 2021	71
Janeiro de 2021	72
Dezembro de 2020	75
Novembro de 2020	75
Outubro de 2020	76
Setembro de 2020	76
Agosto de 2020	78
Julho de 2020	79
Junho de 2020	87
Maio de 2020	88
Abril de 2020	91
Fevereiro de 2020	93
Janeiro de 2020	94
Dezembro de 2019	96
Novembro de 2019	96
Outubro de 2019	96
Setembro de 2019	97
Agosto de 2019	99
Julho de 2019	99
Junho de 2019	99
Maio de 2019	100
Abril de 2019	101
Março de 2019	101
Fevereiro de 2019	102
Janeiro de 2019	102
Dezembro de 2018	102
Novembro de 2018	103
Integração do Data Infrastructure Insights	104
Criando sua conta do NetApp BlueXP	104
Iniciando a avaliação gratuita do Data Infrastructure Insights	104
Inicie sessão e vá	105
Terminar sessão	105
Segurança	106
Segurança do Insights da infraestrutura de dados	106
Informação e região	108
Ferramenta SecurityAdmin	110
Como começar	119
Tutoriais de recursos	119
Coleta de dados	120
Importar a partir da Galeria do Dashboard	147
Contas de usuário e funções	147
Lista de coletores de dados do Insights de infraestrutura de dados	157
Subscrever o Data Infrastructure Insights	161

Edição de avaliação	161
E se a minha subscrição tiver expirado?	162
E se a minha subscrição tiver expirado?	162
Avaliação do módulo	163
Opções de subscrição	164
Como faço para me inscrever?	166
Veja o status da assinatura	167
Veja o seu Gerenciamento de uso	168
Inscreva-se diretamente e pule a avaliação	169
Adicionando um ID de direito	169
Observabilidade	170
Criando painéis	170
Trabalhando com consultas	212
Insights	227
Monitores e alertas	235
Trabalhando com Anotações	332
Trabalhar com aplicações	341
Resolução automática do dispositivo	343
Informações da página de ativos	360
Relatórios	376
Kubernetes	455
Visão geral do cluster do Kubernetes	455
Antes de instalar ou atualizar o Operador de Monitoramento do Kubernetes do NetApp	456
Instalação e configuração do operador de monitoramento Kubernetes	460
Opções de configuração do operador de monitoramento Kubernetes	477
Página de detalhes do cluster do Kubernetes	490
Monitoramento e mapa de desempenho de rede do Kubernetes	494
Kubernetes Change Analytics	502
Essenciais de ONTAP	507
Visão geral	507
Proteção de dados	508
Segurança	509
Alertas	513
Infraestrutura	514
Rede	515
Workloads	515
Admin e outras tarefas	517
API do Data Infrastructure Insights	517
Monitoramento do seu ambiente	528
Segurança da carga de trabalho	534
Sobre o Storage Workload Security	534
Como começar	534
Alertas	569
Forense	575
Políticas de resposta automatizadas	587

Políticas de tipos de ficheiros permitidos	589
Integração com a proteção autônoma contra ransomware do ONTAP	590
Integração com o ONTAP Access negada	593
Bloquear o acesso do utilizador	595
Segurança da carga de trabalho: Simulando um ataque	600
Configurar notificações de e-mail para alertas, avisos e integridade do coletor de agente/fonte de dados	603
API de segurança de carga de trabalho	604
Solução de problemas	607
Solução de problemas gerais do Data Infrastructure Insights	607
Solução de problemas da Unidade de aquisição no Linux	609
Solução de problemas da Unidade de aquisição no Windows	612
Pesquisando um coletor de dados com falha	615
Matriz de suporte do Data Infrastructure Insights Data Collector	616
Armazenamento HP Enterprise 3PAR/Alletra 9000/Primera StoreServ	616
Amazon AWS EC2	632
Amazon AWS S3	638
Microsoft Azure NetApp Files	642
Switches Fibre Channel Brocade	651
Consultor de rede Brocade	659
Brocade FOS REST	665
Switches de malha Cisco MDS e Nexus	671
Cohesity	677
EMC Celerra (SSH)	687
EMC CLARiiON (Navicli)	697
EMC Data Domain (SSH)	711
EMC ECS	719
Dell EMC Isilon e PowerScale REST	727
Dell EMC Isilon / PowerScale (CLI)	744
EMC PowerStore REST	759
EMC RecoverPoint (HTTP)	773
EMC ScaleIO e PowerFlex REST	776
CLI do EMC Symmetrix	784
Dell Unisphere REST	802
EMC VNX (SSH)	812
EMC VNXe e Unity Unisphere (CLI)	828
EMC VPLEX	842
EMC XtremIO (HTTP)	852
NetApp e-Series	864
Google Cloud Compute	878
HDS HCP (HTTPS)	884
Gerenciador de dispositivos HiCommand	890
Hitachi Ops Center	907
HDS HNAS (CLI)	918
Armazenamento HPE Nimble / Alletra 6000	927
Huawei OceanStor (REST/HTTPS)	939

IBM Cleversafe	954
IBM DS 8K (DSCLI)	959
IBM PowerVM (SSH)	969
IBM SVC (CLI)	972
IBM XIV E A9000 (XIVCLI)	986
Infinidat Infinibox (HTTP)	998
Computação do Microsoft Azure	1007
Microsoft Hyper-V	1012
Modo NetApp 7	1022
NetApp Cloud Volumes Service	1045
Amazon FSX para NetApp ONTAP	1051
NetApp Clustered Data ONTAP 8.1,1 mais	1068
NetApp SolidFire 8,1 mais	1099
NetApp StorageGRID (HTTPS)	1113
Armazenamento Nutanix (RESTO)	1122
OPENSTACK (API REST / SSH)	1136
Oracle ZFS (HTTPS)	1142
Pure Storage FlashArray (HTTP)	1157
Red Hat RHV (RESTO)	1169
Rubrik Storage	1173
Centro Virtual da NetApp HCI	1183
VMware Cloud na AWS	1192
VMware vSphere (Web Services)	1200
Referência e suporte	1214
Solicitação de suporte	1214
Referência do coletor de dados - infraestrutura	1219
Referência do coletor de dados - Serviços	1338
Referência do ícone do objeto	1412
Avisos legais	1414
Direitos de autor	1414
Marcas comerciais	1414
Patentes	1414
Política de privacidade	1414
Código aberto	1414

Documentação do Data Infrastructure Insights

O NetApp Data Infrastructure Insights (anteriormente conhecido como Cloud Insights) é uma ferramenta de monitoramento de infraestrutura de nuvem que oferece visibilidade de toda a sua infraestrutura. Com o Data Infrastructure Insights, você pode monitorar, solucionar problemas e otimizar todos os recursos, incluindo suas nuvens públicas e seus data centers privados.

O que o Data Infrastructure Insights pode fazer por mim?

O Data Infrastructure Insights oferece monitoramento de multcloud híbrida, com uma observabilidade de toda a stack de infraestrutura e workloads.

- Coletores de dados para infraestrutura e workloads heterogêneos, incluindo Kubernetes
- Open Telegraf Collector e APIs abertas para fácil integração
- Alertas e notificações abrangentes
- Aprendizado de máquina para insights inteligentes
- Otimizar a utilização de recursos
- Painéis integrados ou personalizáveis com filtros avançados para minimizar o ruído de exibição para responder a perguntas
- Descubra a integridade das operações de storage da ONTAP
- Proteja seu ativo comercial mais valioso: Os dados, contra ransomware ou ataque de destruição de dados

Como começar

- Como faço "[comece já](#)" com o Data Infrastructure Insights?
- Estou inscrito. Agora, o que eu faço? "[A adquirir dados](#)" "[Configurando usuários](#)"
- Incrível! O que se segue? "[Preparar ativos: Anotar](#)" "[Encontrando os ativos que você quer: Consultando](#)" "[Ver os dados que você deseja: Painéis](#)" "[Monitoramento e alertas](#)" "[Proteção de dados](#)"
- Isso é ótimo! Estou pronto para "[subscribe](#)".

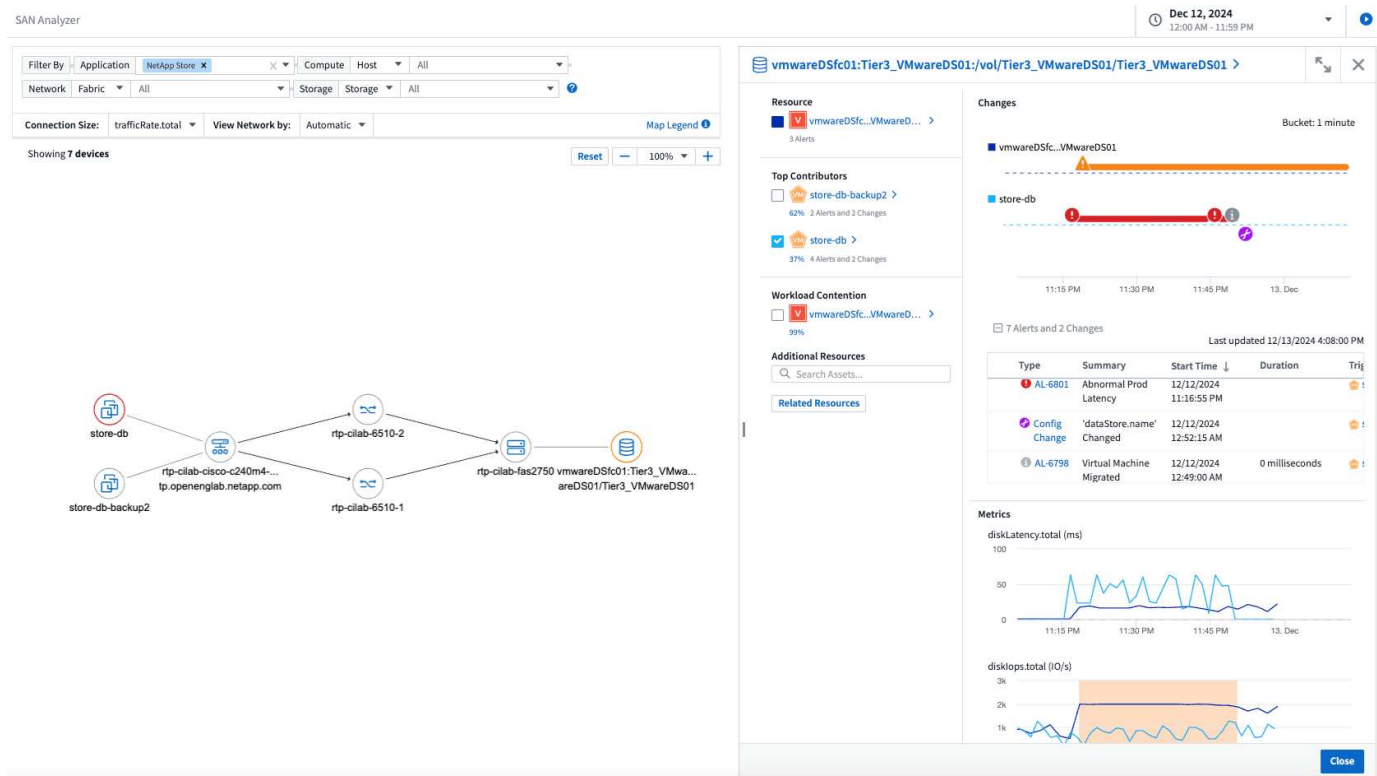
Novidades do Data Infrastructure Insights

A NetApp está continuamente melhorando e aprimorando seus produtos e serviços. Aqui estão alguns dos recursos e funcionalidades mais recentes disponíveis no Insights de infraestrutura de dados (anteriormente Cloud Insights).

Dezembro de 2024

Apresentamos o SAN Analyzer: Visibilidade aprimorada para workloads de bloco

A SAN desempenha um papel crucial no tratamento de workloads vitais, mas sua complexidade pode resultar em interrupções significativas e interrupções dos clientes. Com o **SAN Analyzer** da DII, o gerenciamento de SAN torna-se mais simples e eficiente. Essa poderosa ferramenta oferece visibilidade completa, mapeando dependências de VM/host para rede, LUN e armazenamento. Ao fornecer um mapa de topologia interativo, o SAN Analyzer permite identificar problemas, entender alterações e melhorar a compreensão do fluxo de dados. Otimize o gerenciamento de SAN em AMBIENTES DE TI complexos com o SAN Analyzer e aumente a visibilidade dos workloads de bloco.



Otimize os custos de VM com desativação de host inteligente e recuperação de VM

O Data Infrastructure Insights ajuda a gerenciar os custos de infraestrutura e licenciamento, analisando o comportamento histórico do ambiente e estabelecendo previsões de curto e longo prazo, gerando recomendações detalhadas para desativação de host e recuperação de VMs desativadas e ociosas. Essas recomendações ajudam você a garantir a estabilidade do desempenho, liberar a capacidade não utilizada e reduzir a alocação de memória e CPU.

Filter By Data Center All Virtual Center IP All Cluster All

Summary Hypervisor Decommissioning VM Reclamation

Save 2,228 cores by decommissioning 58 hypervisors
Decommissioning these Hypervisors will reduce your consumption of cores by 27.9%

Top 10 clusters by cores savings opportunities

Cluster	hosts.cpu.savings (cores)
RTP/HOSTING013_PROD	~480
BOS/HOSTING023_PROD	~400
NYC/HOSTING007_ENG	~380
SF/HOSTING003_PROD	~250
BOS/HOSTING005_ENG	~200
MUN/HOSTING001_PROD	~150
LON/HOSTING023_ENG	~120
RTP/HOSTING031_PROD	~100
NYC/HOSTING015_PROD	~80
BOS/HOSTING008_PROD	~70

Memory Savings (TiB)
38.9
26.8% savings

[View All Hypervisor Decommissions](#)

Save 72.0 TiB by reclaiming 336 virtual machines
Reclaiming these VMs will reduce your allocated capacity by 8.2%

Underutilized capacity (TiB)

Powered Off: ~58 TiB
Idle: ~10 TiB

vCPU Savings: **2,755** (9.0% savings)
Memory Savings (TiB): **8.5** (7.9% savings)

[View All VM Reclamations](#)

Descubra insights de log com suporte a gráficos de tempo e widget de tabela

Agora você pode aproveitar os gráficos de tempo (barra, linha, área) para identificar tendências e padrões nos dados de log, como erros recorrentes ou picos de atividade, fornecendo informações valiosas sobre o comportamento do sistema ao longo do tempo. Além disso, com tabelas, agora você pode incluir mensagens de log diretamente no painel, permitindo uma visualização mais abrangente dos detalhes do log.

Count logs.netapp.ems by severity

Severity	Count	Percentage
informational	8,181	55.02%
notice	4,571	30.74%
error	1,704	11.46%
alert	401	2.70%
emergency	12	0.08%
Total	14,869	

Count of Emergency and Error events by storage_name

Emergency and Error

1,716 items found

timestamp	severity	source	message
12/16/2024 11:32:36 AM	error	rtp-sa-cl07	waf.mirror.access.denied: Access to SnapMirror volume 'leafy_demo01_cv_dst' was denied because SnapMirror initialization was not complete (exported Snapshot copy identifier '0' is invalid).
12/16/2024 11:32:33 AM	error	jamaica	scsitar.get.fct.loginfailed: FC port 10a, NPIV port 0 failed fabric login with status of 3 and an extended status of x4.
12/16/2024 11:32:29 AM	error	jamaica	scsitar.get.slifct.linkBreak: Link break detected on Fibre Channel target HBA 10a with event status 1, topology type 1, status1 0x0, status2 0x0.
12/16/2024 11:32:22 AM	error	jamaica	scsitar.get.fct.loginfailed: FC port 10a, NPIV port 0 failed fabric login with status of 3 and an extended status of x1a.

Novembro de 2024

Nova API de alertas de segurança de workload

Recupere detalhes de alerta forense com o novo Workload Security "[Cloudsecure_forensics.alerts API](#)".

cloudsecure_forensics.alerts.v1

- GET** `/v1/cloudsecure/alerts` Returns information on alerts generated in the Storage Workload Security environment.
- GET** `/v1/cloudsecure/alerts/{alertId}` Returns details of alerts generated in the Storage Workload Security environment.

Analise as alterações de configuração no seu ambiente

As alterações de configuração são uma das causas mais comuns de problemas na TI moderna. A nova funcionalidade do Data Infrastructure Insights (DII) "[análise de alterações](#)" permite que você entenda claramente as mudanças que causam problemas no seu ambiente. Acelere o tempo de solução de problemas mostrando todas as alterações nos dispositivos e componentes de infraestrutura relacionados que possam ter causado um problema. Além disso, quando você ou sua equipe realizam alterações planejadas, você pode validar essas alterações rapidamente e garantir que não haja efeitos inesperados antes que os níveis de serviço sejam afetados.

The screenshot displays the Data Infrastructure Insights (DII) interface. On the left, there's a sidebar with filters for resources like 'vmwareD5fc1:Tier3_VMwareD501' and 'store-db-backup2'. The main area shows a timeline of events, including a 'Config Change' event at 8:07:54 AM. A table below the timeline lists the changes:

Attribute Name	Previous	New
powerState	poweredOff	poweredOn
guestState	notRunning	running

Below the table, there are two line graphs: 'diskLatency.total (ms)' and 'diskIops.total (IO/s)'. The 'diskIops.total' graph shows a significant increase in activity starting around 8:18 AM, coinciding with the configuration change.

Suporte ao KubeVirt: Monitore workloads de máquina virtual em execução no cluster do Kubernetes

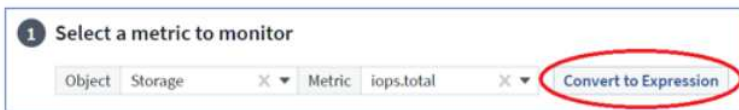
O DII agora oferece suporte total ao KubeVirt, a solução de virtualização nativa do Kubernetes usada por plataformas como o OpenShift Virtualization e o Harvester. Obtenha visibilidade completa das métricas, eventos, alterações de configuração e tráfego de rede das máquinas virtuais e cargas de trabalho de contêiner nos clusters do Kubernetes.

Outubro de 2024

Desbloquear novos Insights com expressões personalizadas em monitores

As expressões permitem que você execute operações aritméticas em monitores de detecção de métrica e anomalias. Aqui estão alguns exemplos:

- Taxa: IOPS/TB para detetar onde os limites de nível de serviço estão sendo alcançados em provedores de storage em nuvem.
- Porcentagem: Usado/disponível para calcular a utilização
- Agregação: Combine vários tipos de erros de porta física em um monitor
- Comparação: Compare a utilização atual do espaço livre de recursos com o ponto ideal do espaço livre para identificar recursos que não estão sendo executados em plena capacidade.



Minimizar interrupções de alerta durante o período de manutenção

O Windows permite suprimir notificações de alerta durante períodos de manutenção programados, ajudando-o a evitar interrupções desnecessárias.

Com o Maintenance Windows, pode programar períodos de manutenção específicos durante os quais as notificações de alerta são suprimidas, para os objetos e métricas que escolher. Por exemplo, você pode suprimir notificações de alerta acionadas por sistemas de armazenamento específicos, quando esses sistemas de armazenamento estão em um período de atualização planejado.

Note que apenas as notificações de alerta são suprimidas (e-mail, webhook); os alertas em si ainda são mostrados na página observabilidade > Alertas > todos os Alertas.

1 Select criteria for alert suppression (a and/or b)

a Storage Device Filter By Storage *grenada*

b Filter By Monitor +

Recent Alerts (108) Last 3 Hours

monitor	currentSeverity	triggeredOn
ONTAP Volume Capacity Time To Full	Warning	Storage: grenada Storage Virtual Machine: svm-sap01 Internal Volume: H13_shared cluster_uuid: a68d2fce-cee8-11e9-909d-00a0989e2cde cluster_vendor: NetApp cluster_model: AFF-A800
ONTAP Volume Capacity Time To Full	Warning	Storage: grenada Storage Virtual Machine: svm-esx Internal Volume: cbc_esxi_prod_win_ds_01 cluster_uuid: a68d2fce-cee8-11e9-909d-00a0989e2cde

2 Select whether to suppress alerts or notifications

Detect alerts but suppress notifications

3 Set up suppression window

Start Date **Start Time** (America/New_York - UTC -04:00)

End Date **End Time** (America/New_York - UTC -04:00) Suppress indefinitely

Simplifique o gerenciamento de alertas com novas regras de notificação de alerta

Simplifique o gerenciamento de notificações entre monitores e equipes.

Controle a entrega de alertas nos canais da sua organização, garantindo que as informações certas cheguem à equipe certa. Não é necessário gerenciar monitores separados para equipes diferentes; rotear alertas com base em atributos de objeto relacionados (nome do armazenamento, data center, nome do aplicativo) ou monitorar atributos (grupo, gravidade).

1 Filter alerts for notifications (a and/or b)

a Object Attributes Filter By relatedObject.dataCenter.name "Boston"

b Filter By Monitor monitor.group ONTAP Infrastructure

Recent Alerts (0) Last 24 Hours

Registrar análises em painéis

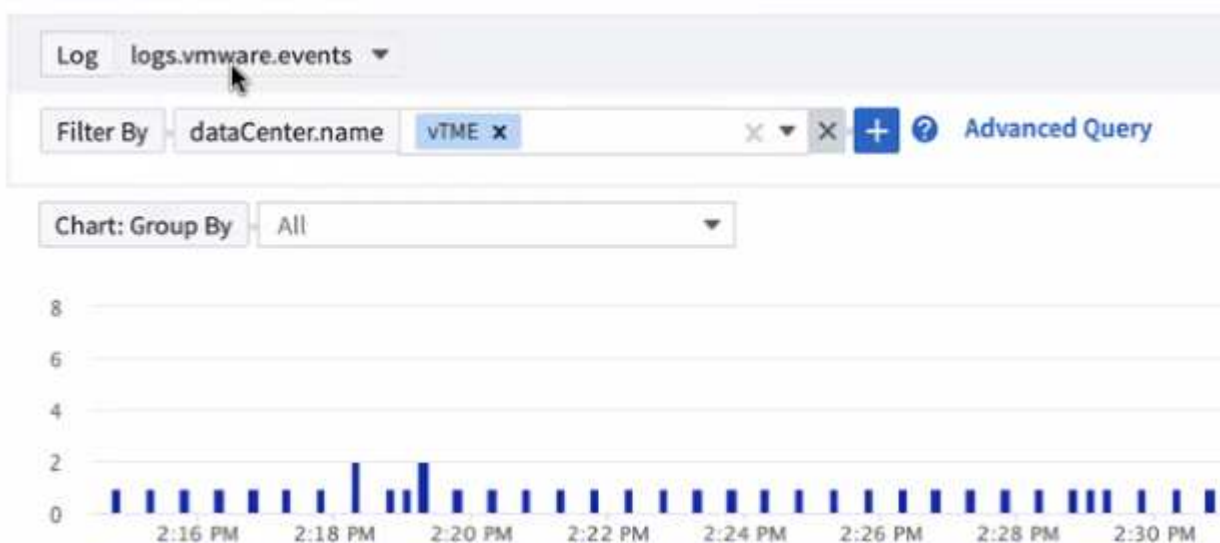
Agora, você pode incluir eventos de log em seus painéis para visualizar dados de eventos e ter uma compreensão mais abrangente e contextual do seu ambiente. Investigue logs e visualize métricas relacionadas sem sair do painel!



Melhor observabilidade do VMware com eventos VMware

Gerencie e solucione problemas proativamente seu ambiente VMware com eventos em tempo real. Os eventos VMware fornecem insights sobre migrações de VM, alocações de recursos e integridade do host. Agora disponível para uso em consultas, painéis e monitores. Requer o VMware versão 8 ou superior. Basta selecionar a fonte `logs.VMware.events`.

Os eventos VMware também são usados para a nova análise de alteração de configuração do DII, mencionada acima.



Atualizações do Data Collector:

- **Pure FlashBlade:** Este coletor reúne dados de inventário e desempenho de clusters FlashBlade que expõem a versão 2 da API REST.

Setembro de 2024

Introdução ao Insights de infraestrutura de dados, anteriormente Cloud Insights

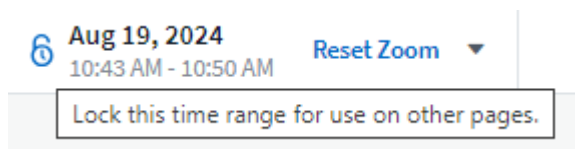
Na terça-feira, 24 de setembro de 2024, a NetApp mudou oficialmente o nome de Cloud Insights para **informações de infraestrutura de dados (DII)**. Isso foi anunciado durante a conferência de usuários do Insight por Haiyan Song em sua apresentação principal do palco e em um comunicado de imprensa sobre o produto da conferência Insight.

O serviço DII permanece o mesmo; não há alterações ou modificações de recursos. Esta é uma alteração de nome para alinhar melhor o nome do serviço com seus recursos para toda a infraestrutura DE TI.

Agosto de 2024

Exibir dados específicos ao seu intervalo de tempo

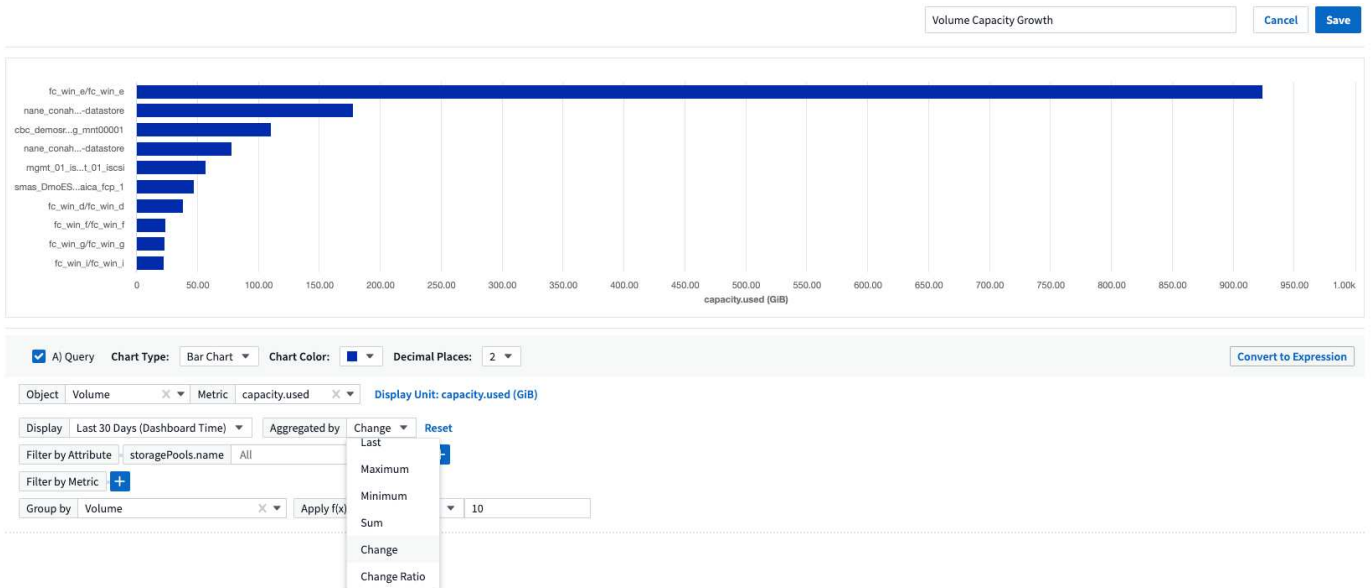
Investigando um alerta? Ampliação em um gráfico? Essas ações alteram o intervalo de tempo para essas páginas. Agora você pode bloquear esse intervalo de tempo, navegar para outras páginas do Cloud Insights e ver dados específicos desse intervalo de tempo bloqueado. Investigar e solucionar problemas ficou muito mais fácil!



Análise de taxa de mudança e mudança (%)

As agregações de tempo de relação de mudança ajudam você a identificar mudanças significativas e tendências em valores métricos ao longo do tempo. Esses insights são essenciais para entender o que mudou, como um aumento considerável da capacidade para um tempo específico ou uma mudança no desempenho de uma única porta.

- **Alterar** - observe a mudança em uma métrica entre dois pontos dentro de um período selecionado.
- **Relação de mudança** - observe a mudança proporcional em uma métrica entre dois pontos, em relação ao ponto inicial, dentro de um período selecionado.




Exportar os resultados da consulta de log para .CSV

Ao visualizar os resultados da consulta de log, exporte facilmente até 10.000 linhas para .CSV clicando no novo botão "Exportar". Isso aprimora a acessibilidade de dados, facilita a análise e a geração de relatórios de dados e facilita a integração perfeita com outras ferramentas do Data Processing.

Log Entries

Last updated 08/15/2024 1:01:49 PM  

timestamp ↓	source	message



Resolver alertas por tempo

O Cloud Insights agora oferece a opção de resolver um alerta quando a métrica monitorada permanece dentro do intervalo aceitável por uma duração especificada. Isso permite que você se concentre em problemas genuínos, reduzindo o ruído associado às métricas repetidamente cruzando limites definidos consolidando vários alertas para um.

3 Define alert resolution

Resolve when the metric returns to the acceptable range

Resolve when the metric is within the acceptable range for

15

Minute(s) ▼

Minute(s)

Hour(s)

Day(s)

Julho de 2024

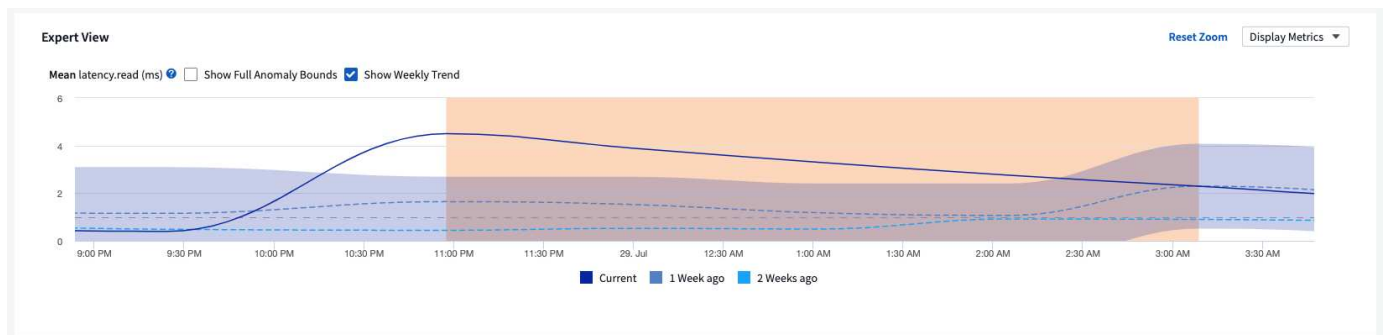
AI Ops: Detecção de anomalias

O Cloud Insights usa o aprendizado de máquina para detectar mudanças inesperadas nos padrões de dados no ambiente e fornecer alertas proativos para ajudar a identificar problemas com antecedência.

Um data center se comporta de maneiras diferentes em diferentes momentos do dia e em diferentes dias da semana. Cloud Insights usa sazonalidade semanal para comparar o comportamento histórico para cada dia e hora.

O Monitoramento de detecção de anomalias pode fornecer alertas para situações como quando a definição de "normal" não é clara, onde o comportamento muda ao longo do tempo, ou quando se trabalha com grandes quantidades de dados onde a definição manual de limiares é impraticável.

"[Monitores de detecção de anomalias](#)" Novo alerta quando anomalias como essa ocorrem em métricas de objeto que você escolher.



Melhorias na segurança da carga de trabalho

Suporte a NFS 4,1

O Coletor de dados SVM agora oferece suporte a versões NFS de até **NFS 4,1** com ONTAP 9.15,1 ou posterior.

Nova API de atividade Forensics

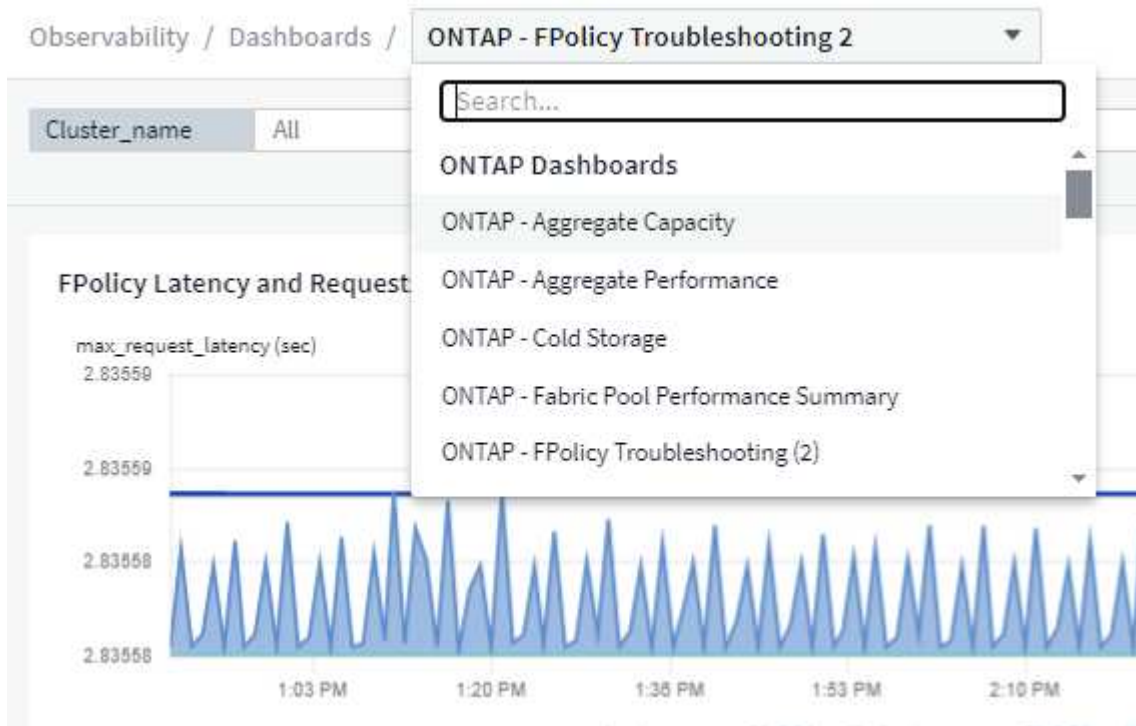
A atividade Forensics "**API**" tem uma nova versão. Ao chamar a API para atividade Forensics, use a API **cloudsecure_forensics.Activities.v2**.

Observe que se você estiver fazendo várias chamadas para essa API, para obter melhores resultados, certifique-se de que as chamadas ocorram sequencialmente, em vez de em paralelo. Várias chamadas paralelas podem fazer com que a API termine o tempo limite.

Navegação mais fácil no painel de instrumentos

Esse recurso é essencial para simplificar seus fluxos de trabalho operacionais e facilitar a colaboração entre as equipes.

Aggrupar seus dashboards facilita a obtenção rápida da visibilidade de que você precisa e, agora, com o novo menu de navegação, você pode alternar entre diferentes dashboards sem perder seu lugar, facilitando a exploração e o gerenciamento de sua infraestrutura. Alinhe os grupos do painel com seus runbooks operacionais para aprimorar ainda mais sua experiência.



Junho de 2024

Suporte ao sistema operacional

Os seguintes sistemas operacionais são suportados com unidades de aquisição Cloud Insights, além dos seguintes "já suportado":

- Red Hat Enterprise Linux 8,9, 8,10, 9,4
- Rocky 9,4
- AlmaLinux 9,3 e 9,4

Mai de 2024

Resolva alertas automaticamente com base no tempo

Os alertas de log agora podem ser resolvidos com base no tempo; se a condição de alerta parar de ocorrer, o Cloud Insights pode resolver o alerta automaticamente após um tempo especificado ter passado. Você pode optar por resolver o alerta em minutos, horas ou dias.

3 Define alert resolution

- Resolve instantly
- Resolve based on criteria

Resolve automatically after

Day(s) ▼

if the condition **above** stops occurring.

Resolve based on log entry

Minute(s)

Hour(s)

Day(s)

Abril de 2024

Suporte iSCSI para Kubernetes

O Cloud Insights agora tem suporte para mapear o storage iSCSI associado ao Kubernetes, permitindo a solução de problemas mais rápida usando o mapa de rede do Kubernetes e a capacidade de fornecer relatórios de chargeback ou showback por meio de relatórios.

The screenshot displays the NetApp Cloud Insights interface. On the left, the 'Workload Map' shows a network diagram with nodes for 'order', 'order-postgres', 'payment', and '172-30-2-59.order.netap... ore-01.svc.cluster.local'. A tooltip for 'order-postgres-pv' shows 'connections_total: 1'. On the right, the 'Persistent Volume' details panel is open, showing 'Persistent Volume Details' for 'ci-demo-01' (Type: iSCSI). It includes a summary tree, labels, and storage metrics. The 'Storage Metrics' section contains four charts: IOPS (35.88 IO/s), Latency (0.54 ms), Throughput (143.78 KB/s), and Used Capacity (60.16%). Below this is a 'Backend Storage Performance' table.

PV Name	Workload	Type	Backend Storage	Used Capacity (%)	Total Cap. (GiB)
order-postgres-pv	order-postgres	NFS	cvoPostgresProd05:dataVolume06	60.16	80.84

Suporte ao sistema operacional

Os seguintes sistemas operacionais são suportados com unidades de aquisição Cloud Insights, além dos seguintes "já suportado":

- Oracle Enterprise Linux 8,8
- Red Hat Enterprise Linux 8,8
- Rocky 9,3
- OpenSUSE Leap 15,1 até 15,5
- SUSE Enterprise Linux Server 15, 15 SP2 a 15 SP5

Março de 2024

Detalhes do agente de segurança da carga de trabalho

Cada um dos seus agentes de segurança de carga de trabalho tem sua própria página de destino, onde você pode ver facilmente informações resumidas sobre o Agente, bem como os coletores de dados e diretório de usuário instalados associados a esse Agente.

Agent Summary

Name agent-1	Connection Status Connected - Need Help?
IP 10.11.12.13	Last Reported a few seconds ago Mar 5, 2024 9:40 AM
Version 1.602.0	

Installed Data Collectors

[+ Data Collector](#)

Name ↑	Status	Type	Cluster/SVM IP	SVM Name	Last Reported	
DSC	Running	ONTAP SVM	10.102.103.104	sgornall_svm	a few seconds ago Mar 5, 2024 9:40 AM	⋮

Installed User Directory Collectors

[+ User Directory Collector](#)



Name ↑	Status	Type	Server	Forest Name/Search Base	Last Reported	
AD_EditRename	Running	Active Directory	10.200.203.204	wslab1.netapp.com	a few seconds ago Mar 5, 2024 9:40 AM	⋮

Trace mais dados mais rapidamente

Ao analisar dados na página inicial de um ativo, adicionar dados adicionais aos gráficos do Expert View é um piscar de olhos. Para cada tabela na página de destino, se um tipo de objeto tiver dados relevantes, passe o Mouse sobre esse objeto para exibir o ícone "Adicionar à Visão Avançada". A seleção deste ícone adiciona esse objeto aos recursos adicionais e o exibe nos gráficos do Expert View.

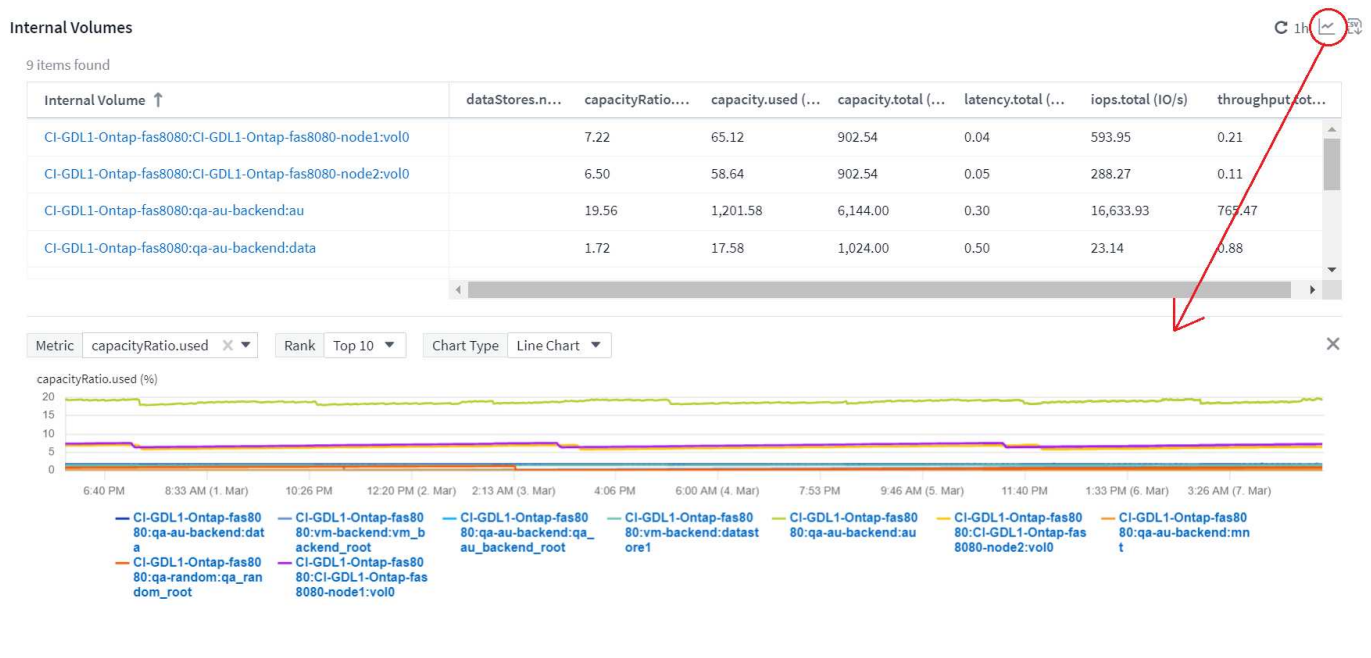
2 items found

Storage Node ↑ **Add to Expert View**

CI-GDL1-Ontap-fas8080-node1  

CI-GDL1-Ontap-fas8080-node2

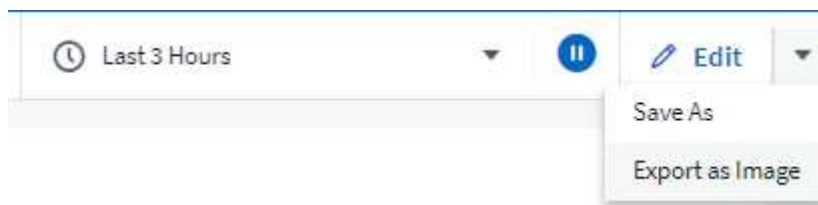
Ou talvez você queira ver os dados de uma tabela de Landing page em seu próprio gráfico. Basta selecionar o ícone *Show Chart* para abrir o gráfico abaixo da tabela:



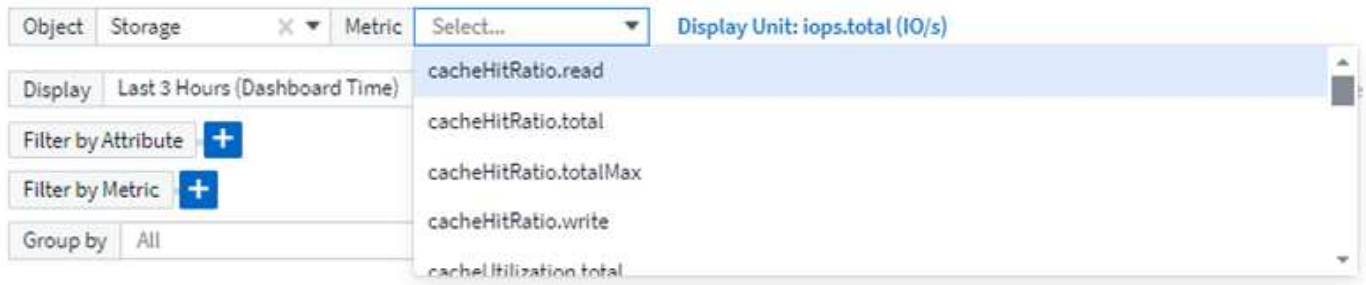
Fevereiro de 2024

Melhorias de usabilidade

Salve um **snapshot** do seu painel atual selecionando *Exportar como imagem* no canto direito suspenso. O Cloud Insights cria um .PNG dos estados atuais do widget.



Seleção de objetos e métricas é mais fácil do que nunca para Widgets, monitores, etc. escolha o tipo de objeto desejado e, em seguida, selecione uma métrica relevante para esse objeto na lista suspenso separada.



Exportar coletor de dados e Unidade de aquisição lista para .CSV selecionando o ícone na parte superior dessas páginas.



Reorganizamos a página Ajuda > suporte para que seja mais fácil encontrar o que você está procurando e, como você pediu, adicionamos links diretos nesta página para **API Swagger** e documentação do usuário.

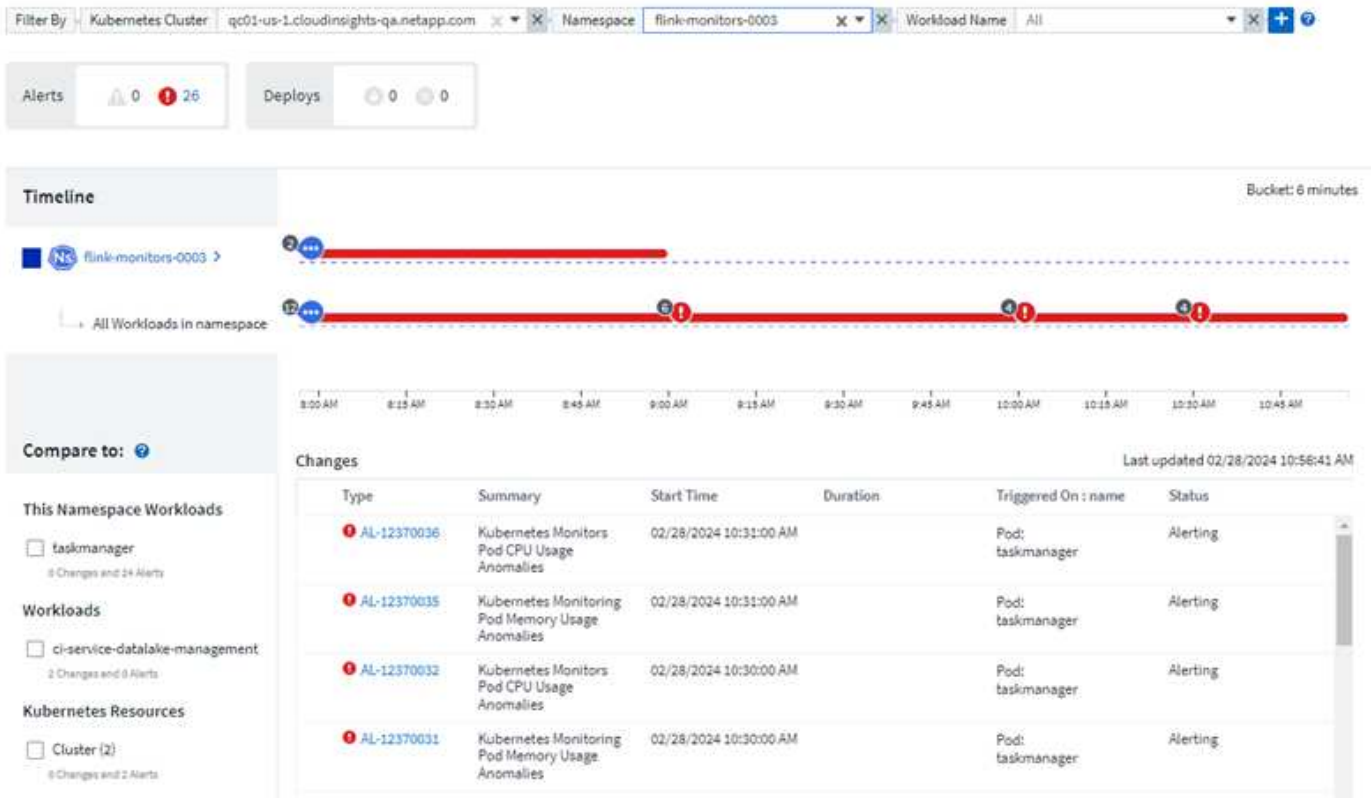
API Access:
To integrate Cloud Insights with other applications see the [Cloud Insights API List and documentation](#).

Links na coluna "triggeredOn" na página da lista Alertas navegarão para a Landing Page apropriada, se uma Landing Page estiver disponível para esse objeto.

alertId	triggeredTime ↓	currentSeverity	monitor	triggeredOn
AL-12371406	4 minutes ago Feb 28, 2024 4:50 PM	Warning	Kubernetes Cluster Saturation	Kubernetes_Cluster: gcs01-us-1.cloudinsights.netapp.com

Veja todas as alterações em seu namespace

A análise de alterações do Kubernetes agora permite que você veja uma linha do tempo de alterações ao selecionar Cluster e namespace. Anteriormente, a carga de trabalho também deve ter sido selecionada. Ao filtrar em cluster e namespace, a linha do tempo de todas as alterações de workload nesse namespace é mostrada em uma linha.



Registros relacionados para alertas

Ao visualizar um alerta de log, as entradas de log relacionadas são mostradas em uma nova tabela. Uma entrada de log é relacionada se ocorrer na mesma fonte e período de tempo que o alerta, e está sujeita às mesmas condições. Selecione "Analyze Logs" (analisar registros) para explorar mais.

Related Logs

[Analyze Logs](#)

timestamp ↓	message
02/28/2024 11:07:21 AM	iscsi.loginFailure: ISCSI: iSCSI login failure, 'Invalid TargetName iqn.1992-08.com.netapp:sn.6ed012db378611ee8f24005056b3dcd8:vs.3 from Initiator iqn.1994-05.com.redhat:dc7292e4b936 at IP address 10.192.38.34'
02/28/2024 11:06:24 AM	iscsi.loginFailure: ISCSI: iSCSI login failure, 'Invalid TargetName iqn.1992-08.com.netapp:sn.091b27ae993c11ee9765005056b3f163:vs.3 from Initiator iqn.1994-05.com.redhat:e861299d2ffc at IP address 10.192.33.88'
02/28/2024 11:06:24 AM	iscsi.loginFailure: ISCSI: iSCSI login failure, 'Invalid TargetName iqn.1992-08.com.netapp:sn.091b27ae993c11ee9765005056b3f163:vs.3 from Initiator iqn.1994-05.com.redhat:e861299d2ffc at IP address 10.192.33.88'

Colete dados do switch ONTAP

O Cloud Insights pode coletar dados dos switches back-end do sistema ONTAP; basta habilitar a coleta na seção *Configuração Avançada* do coletor de dados e garantir que o sistema ONTAP esteja configurado para fornecer "informações do interruptor" e tenha o conjunto apropriado "permissões".

API de coletor de dados de segurança de carga de trabalho

Em ambientes grandes, você pode automatizar a criação do coletor de Workload Security usando a nova API Data Collectors. Navegue até **Admin > API Access > API Documentation** e selecione o tipo de API *Workload Security* para saber mais.

Janeiro de 2024

Experimente os recursos do Cloud Insights que você ainda não usou

Além de sua avaliação inicial do Cloud Insights, você também pode aproveitar "[Avaliações do módulo](#)". Por exemplo, se você se inscreveu no Cloud Insights e monitora máquinas virtuais e storage, ao adicionar o Kubernetes ao seu ambiente, entrará automaticamente em uma avaliação de 30 dias da observabilidade do Kubernetes. O uso de unidade gerenciada de observabilidade do Kubernetes não será considerado em relação aos seus direitos inscritos até que o período de teste termine.

Quão saudáveis são as minhas cargas de trabalho?

A integridade da carga de trabalho está disponível rapidamente na página **Kubernetes > explorar > cargas de trabalho**, para que você possa ver rapidamente quais cargas de trabalho estão com bom desempenho e quais podem precisar de alguma ajuda. Identifique facilmente se o problema de integridade está relacionado a alterações de infraestrutura, rede ou configuração e faça uma análise detalhada da causa raiz.

Workload Name	Health ↓	Running Pods	Desired Pods	Compute & Storage	Network	Changes	Namespace	Kubernetes Cluster
point-of-sale >	Unhealthy	0	1	Critical		0	netapp-fitness-store-01 >	ci-demo-01 >
frontend >	Unhealthy	2	2		Critical	0	netapp-fitness-store-01 >	ci-demo-01 >
catalog >	Healthy	1	1	Critical (Resolved)		2	netapp-fitness-store-01 >	ci-demo-01 >
billing >	Healthy	1	1			13	netapp-fitness-store-01 >	ci-demo-01 >
cart >	Healthy	1	1			0	netapp-fitness-store-01 >	ci-demo-01 >
cart-red >	Healthy	1	1			0	netapp-fitness-store-01 >	ci-demo-01 >
catalog >	Healthy	1	1			0	netapp-fitness-store-01 >	ci-demo-01 >
chaos-c >	Healthy	3	3			0	chaos-mesh >	ci-demo-01 >
chaos-d >	Healthy	6	7			0	chaos-mesh >	ci-demo-01 >
chaos-dashboard >	Healthy	1	1			0	chaos-mesh >	ci-demo-01 >
chaos-dns-server >	Healthy	1	1			0	chaos-mesh >	ci-demo-01 >

Atualizações do Data Collector

Identificação do domínio de dados

O coletor de domínio de dados foi melhorado para identificar melhor os sistemas de HA para durabilidade em eventos de failover esta alteração causará uma identificação **única** dos dispositivos de domínio de dados em sistemas HA, o que fará com que quaisquer anotações nesses ativos sejam removidas (porque esses arrays serão reidentificados). Você precisará reanexar anotações aos objetos do domínio de dados.

Algoritmo ML DE detecção de ransomware aprimorado

O Workload Security inclui um novo algoritmo de ML de detecção de ransomware de 2nda geração para detectar os ataques mais sofisticados com mais rapidez e precisão.

"Sazonalidade" de comportamentos: O comportamento de fim de semana pode seguir padrões diferentes de dia da semana, ou comportamento da manhã a partir da tarde. Os algoritmos de segurança da carga de trabalho levam essa sazonalidade em conta.

Funcionalidade obsoleta

Ocasionalmente, a funcionalidade é obsoleta à medida que os recursos evoluem. Aqui estão alguns dos recursos e funcionalidades que foram depreciados no Cloud Insights:

A API `cloudsecure_forensics.activities.v1` está obsoleta

A API `cloudsecure_forensics.Activities.v1` está obsoleta. Esta API retorna informações sobre atividades associadas a entidades no ambiente Storage Workload Security. Esta API foi substituída por `cloudsecure_forensics.activities.*v2*_`.

GET for this API anteriormente retornou o seguinte:

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

Esta API agora retorna:

```
{
  "limit": 1000,
  "meta": {
    "page": {
      "after": "lv1vk3pp.4cpzcg4kpybl",
      "before": "lv1xy3dz.4cq5ajdn19fk",
      "size": 1000
    }
  },
  "results": [
    {
      "accessLocation": "10.249.6.220",
```

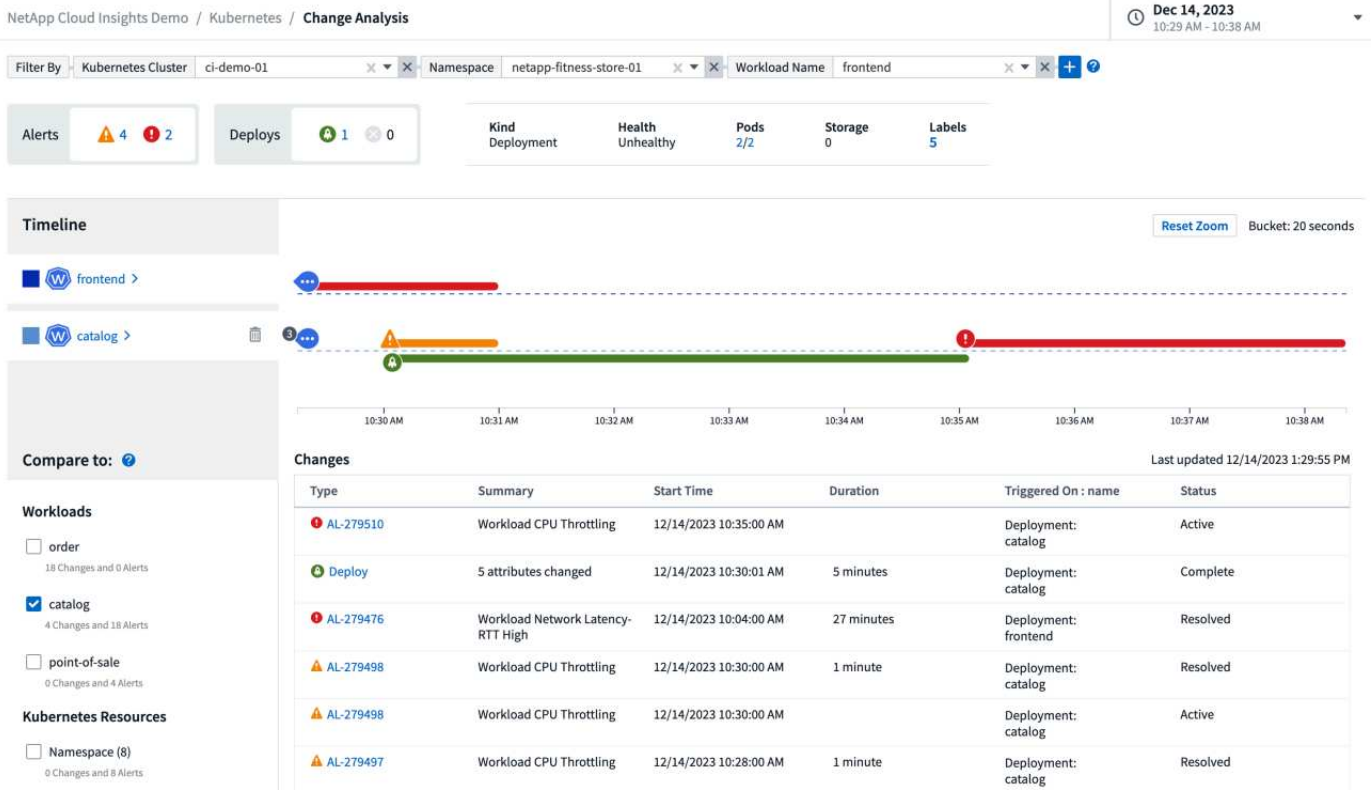
Para obter mais detalhes, consulte a documentação do Swagger em [Admin > API Access > API Documentation > Workload Security](#).

Dezembro de 2023

Mude o Analytics em um relance


O Kubernetes ["Alterar o Analytics"](#) oferece uma visão completa das mudanças recentes no seu ambiente Kubernetes. Alertas e status de implantação estão ao seu alcance. Com o Change Analytics, você pode

controlar todas as alterações de implantação e configuração e correlacioná-las com a integridade e a performance dos serviços, da infraestrutura e dos clusters do K8s.



Dashboard de performance de workload do Kubernetes

A performance do workload está disponível em resumo no abrangente dashboard do Kubernetes Workload Performance. Visualize rapidamente gráficos de tendências de volume, taxa de transferência, latência e retransmissão, bem como uma tabela de tráfego de workload para cada namespace em seu ambiente. Os filtros permitem um foco fácil em áreas de interesse.

 **Kubernetes**

Explore

Change Analysis

Network

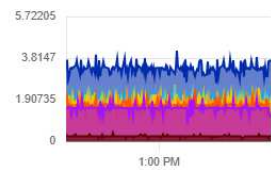
Collectors

Workload Map

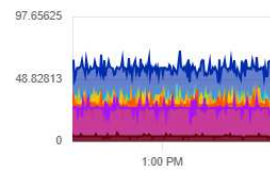
Workload Performance

Cluster: All | src_namespace: All | src_workload_...: All | dst_namespace: All | dst_workload_...: All | scope_cluster: All


Volume



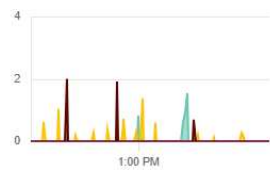
Throughput



Latency-rtt



Retransmission percentage



Workload Traffic Flows

97 items found

src_namespace	src_workload_name	dst_namespace	dst_workload...	tx_bytes_per...	rx_bytes_per...	connections_t...	latency_rtt (ms)	retransr
prod-eu-monitoring	netapp-ci-telegraf-rs	N/A	ec2-52-58-144-...	1.99	0.18	4.32	96.31	0.23
log-alerts-monitoring	netapp-ci-telegraf-rs	N/A	10.192.35.71	18.61	0.32	17.64	0.24	0.13
log-alerts-monitoring	netapp-ci-net-observe...	N/A	10.192.35.71	1.18	0.03	1.00	0.03	0.12

Detalhes da consulta em uma tela

Em uma consulta, selecionar uma linha abre um painel lateral mostrando detalhes de atributos, anotações e métricas para a linha selecionada, fornecendo informações úteis sem a necessidade de perfurar a página inicial do objeto. As ligações na linha ou no painel lateral permitem uma navegação fácil.

The screenshot displays the Cloud Insights interface. On the left, a table shows 29 items found for the 'agent.node_diskio' collector. The table has two columns: 'agent.node_diskio' and 'io_time (ms)'. The data is as follows:

agent.node_diskio	io_time (ms)
dm-0	497.00
dm-1	404.00
sda	104,016.00
sdb	102,913.00
vda	1,973,303,326.00
vda	288,332,246.00
vda	535,153,931.00
vda	5,377,379.00
vda	1,614,535,712.00
vda	70,408,327.00

On the right, the 'agent.node_diskio Details' window is open, showing the following attributes and metrics:

Attributes:

- agent.node_diskio: dm-0
- agent_node_ip: 10.192.149.149
- agent_node_name: ci-qa-vanilla-25
- agent_node_os: CentOS Stream 8
- agent_node_uuid: 0ec824d2-4f50-ea35d513ff9e
- agent_version: Telegraf/1.28.3 Go/1.20.10
- ci_agent_config_version: 1.3
- ci_diskio_config_version: 1.2
- kubernetes_cluster: vanilla25
- name: dm-0

Metrics:

- io_time (ms): 497.00
- iops_in_progress: 0.00
- merged_reads (rds/s): 0.00
- merged_writes (wrs/s): 0.00

Atualizações do Data Collector:

- **Brocade FOS REST:** Este coletor é movido para fora de "Preview" e agora está disponível em geral. Algumas coisas a observar:
 - FOS introduziu sua API REST com FOS 8,2. Mas alguns recursos, como o roteamento, só receberam recursos de API REST com o 9,0.
 - Se você tiver uma malha que consiste em ativos FOS mistos 8,2 vezes mais altos, bem como alguns abaixo de 8,2, o coletor REST do Cloud Insights FOS não descobrirá esses ativos mais antigos. Você pode editar o coletor REST FOS e criar uma lista delimitada por vírgulas do endereço IPv4 desses dispositivos para exclusão desse coletor.
- **SELinux:** O Cloud Insights inclui melhorias na instalação inicial da Unidade de aquisição Linux para garantir robustez da operação em ambientes Linux com a aplicação SELinux ativada. Esses aprimoramentos afetam apenas implantações *new AU*; se você tiver problemas de SELinux relacionados a atualizações de AU, entre em Contato com o suporte da NetApp para corrigir sua configuração de SELinux.

Novembro de 2023

Segurança da carga de trabalho: Pausar/retomar um coletor

Em Workload Security, você pode pausar um coletor de dados se o coletor estiver no estado *Running*. Abra o menu "três pontos" para o coletor e SELECIONE PAUSE. Enquanto o coletor está em pausa, nenhum dado é coletado do ONTAP e nenhum dado é enviado do coletor para o ONTAP. Selecione Resume (Retomar) para começar a recolher novamente.

Informações de suporte do nó de storage

Em uma página inicial do nó de armazenamento, a seção *dados do usuário* fornece informações rápidas sobre sua oferta de suporte, status atual, status do suporte e data de término da garantia. Observe que o Cloud Insights publica atualmente apenas automaticamente essas informações para dispositivos NetApp. Observe também que esses campos de suporte são anotações, para que possam ser usados em consultas e painéis.

User Data

[+ Annotation](#)

Serial Number Active

Yes

Serial Number Support Status

Y

Support Offering

WARRANTY

Warranty End Date

12/31/2023

Mapear tags VMware para anotações do Cloud Insights

O "VMware" coletor de dados permite preencher anotações de texto do Cloud Insights com tags de mesmo nome configuradas no VMware.

Melhorias de confiabilidade do coletor CLI da Brocade para FOS 9,1.1c e firmware superior

Em alguns switches Fibre Channel Brocade com firmware 9,1.1c, a saída de certos comandos CLI pode ser preprended com o texto de banner de login "motd", ou avisos para que os usuários alterem senhas padrão. O coletor Brocade CLI foi aprimorado para ignorar esses dois tipos de texto estranho.

Antes desse aprimoramento, apenas switches FOS 9,1.1c sem Virtual Fabrics presentes provavelmente foram detetáveis com esse tipo de coletor.

Outubro de 2023

Segurança de carga de trabalho aprimorada

A segurança da carga de trabalho foi melhorada com o seguinte:

- **Acesso negado:** A Segurança da carga de trabalho integra-se ao ONTAP para receber "Eventos "Acesso negado"" e fornecer uma camada adicional de análise e respostas automáticas.
- * Tipos de arquivos permitidos*: Se um ataque de ransomware for detetado para uma extensão de arquivo conhecida, essa extensão de arquivo pode ser adicionada a uma "tipos de ficheiro permitidos" lista para

evitar alertas desnecessários.

Ensaio de módulos

Além de sua avaliação inicial do Cloud Insights, você também pode aproveitar "[Avaliações do módulo](#)"o . Por exemplo, se você já se inscreveu no Infrastructure Observability, mas está adicionando o Kubernetes ao seu ambiente, entrará automaticamente em uma avaliação de 30 dias da observabilidade do Kubernetes. Você só será cobrado pelo uso de unidade gerenciada de observabilidade do Kubernetes ao final do período de avaliação.

Restringir o acesso a domínios especificados

Administradores e proprietários de contas agora têm a capacidade de "[Restringir o acesso à Cloud Insights](#)"e-mail domínios que eles especificam. Vá para **Admin > User Management** e selecione o botão *restrict Domains*.

Restrict Domains ✕

Select which domains have access to Cloud Insights:

No restrictions (Cloud Insights available on all domains)

Limit access to default domains (acme.com, gmail.com, netapp.com) ?

Limit access to defaults and following domains

✕ ✕

[Learn more about domain restriction.](#) 🔗

Cancel Save

Atualizações do Data Collector

As seguintes alterações de coletor de dados/Unidade de aquisição estão em vigor:

- **Isilon / PowerScale REST:** Vários novos atributos e métricas foram adicionados aos recursos de análise aprimorados do Cloud Insights sob o nome *emc_isilon.node_pool*.*. Esses contadores e atributos capacitarão os usuários a criar painéis e monitores para o consumo de capacidade *node_pool*; os usuários com clusters Isilon construídos a partir de modelos de nós de hardware diferentes terão vários pools de nós e entender seu consumo de capacidade HDD/SSD/total em um nível de pool de nós é útil para monitoramento e Planejamento.

- **Suporte à autenticação "conta de serviço" da Rubrik:** O coletor da Cloud Insights agora oferece suporte à autenticação básica HTTP tradicional (nome de usuário e senha) e à abordagem da conta de serviço da Rubrik, que requer um nome de usuário e ID da organização.

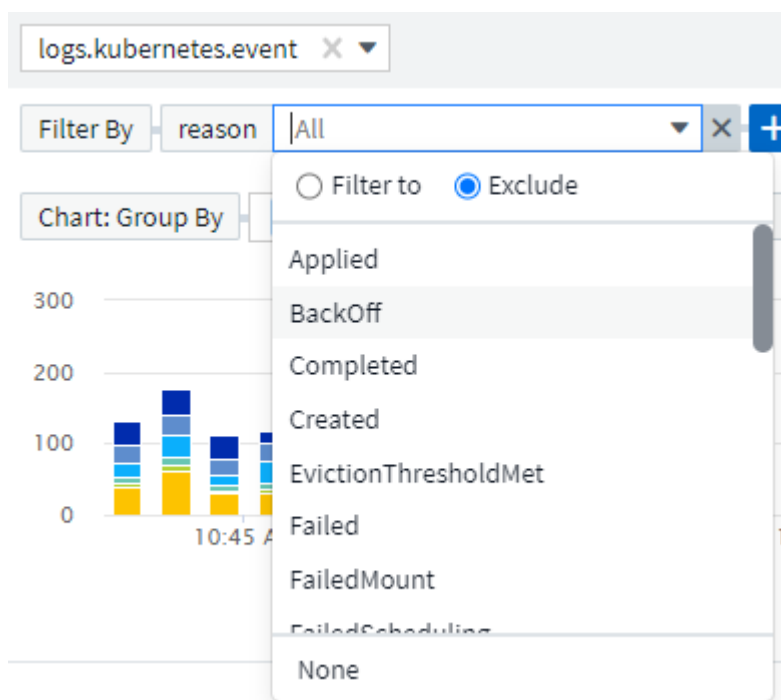
Setembro de 2023

Encontre facilmente o que você quer nos Logs

Consulta de log (**observabilidade > consultas de log > Nova consulta de log**) inclui um número de "melhorias" para tornar a exploração de log mais fácil e mais informativa.

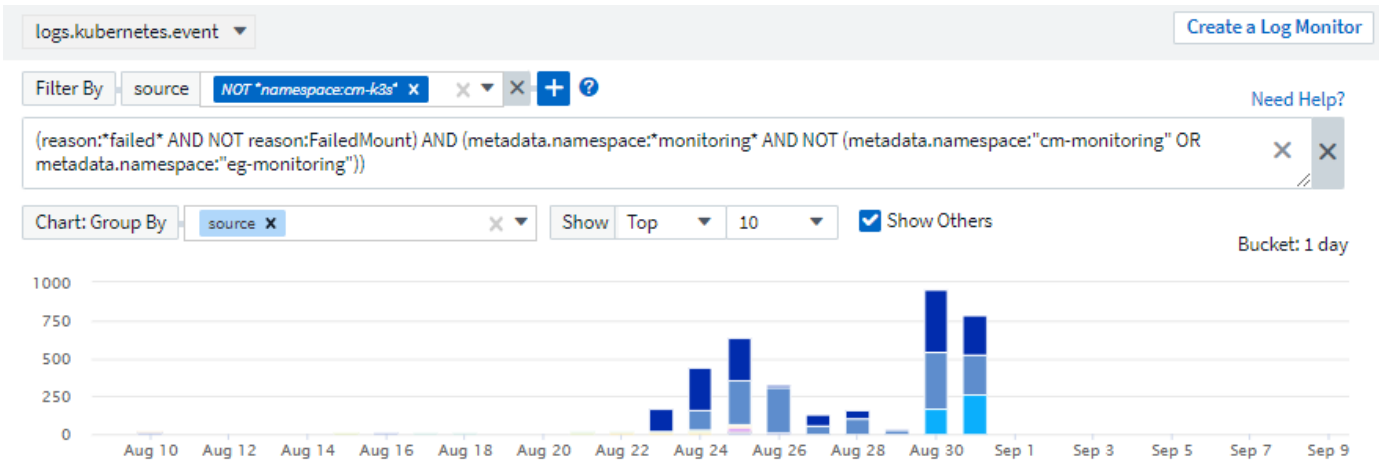
Incluir/excluir

Ao filtrar por um valor, você pode facilmente escolher se deseja **incluir** ou **excluir** resultados que correspondam ao filtro. Selecionar "Excluir" cria um filtro "NÃO <value>". Você pode combinar incluir e excluir valores em um único filtro.



Consulta avançada

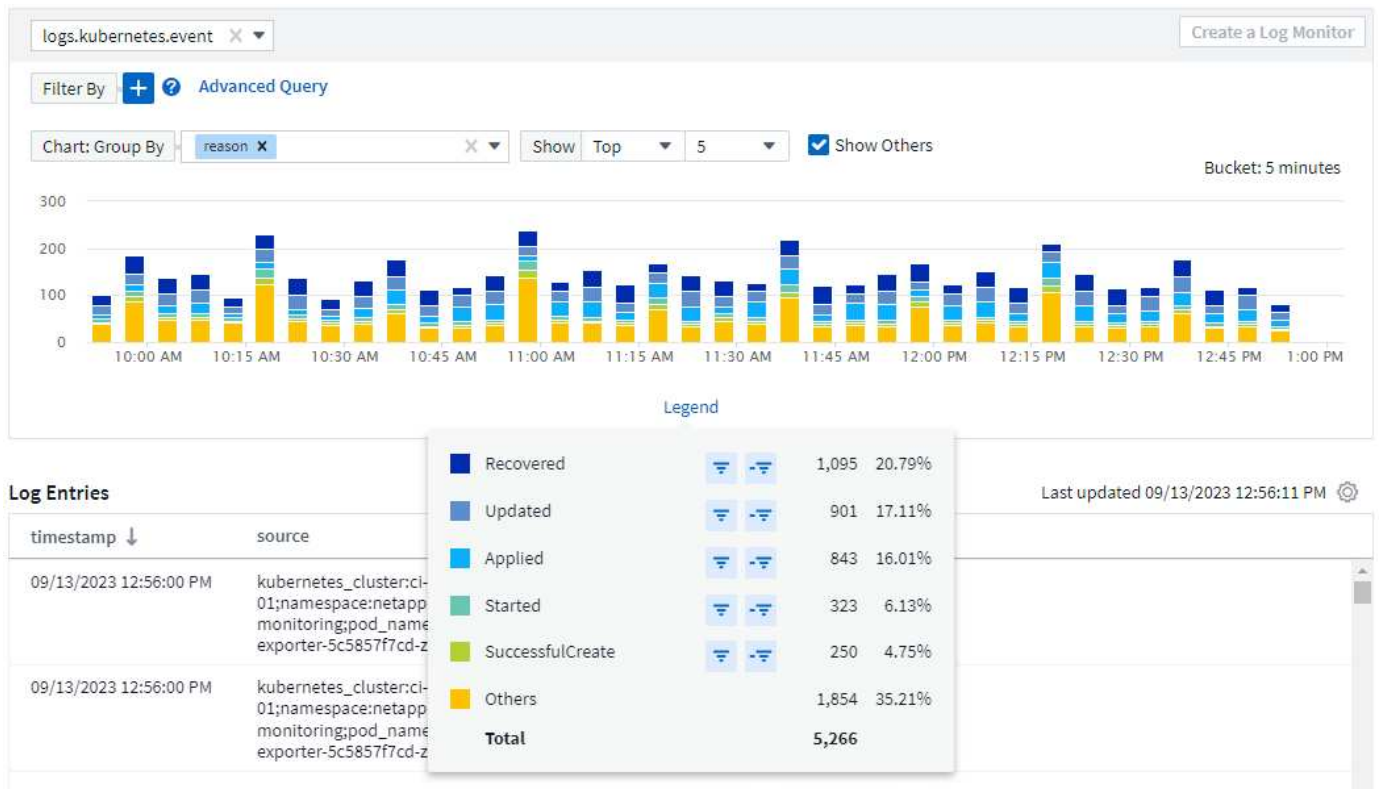
Consulta avançada dá-lhe a oportunidade de criar filtros de "formulário livre", combinando ou excluindo valores usando E, NÃO, OU, curingas, etc.



As consultas "Filtrar por" e Advanced são "E"Unidas para formar uma única consulta. Os resultados são apresentados na lista de resultados e no gráfico.

Agrupando no Gráfico

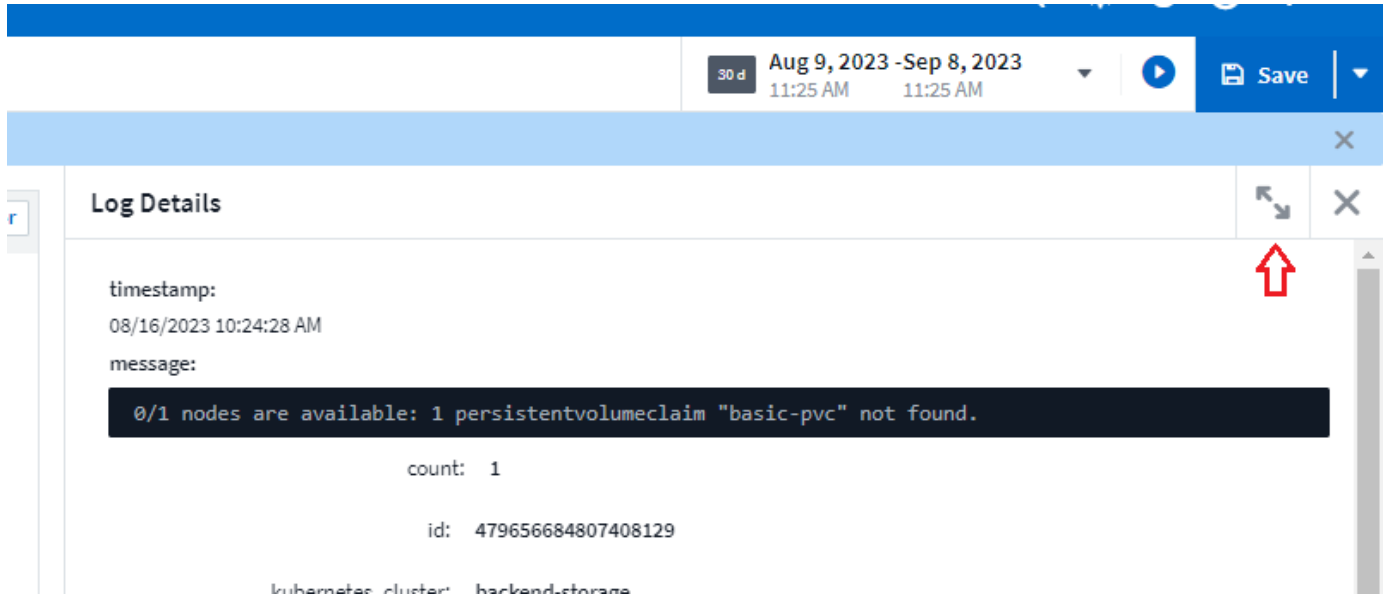
Quando você seleciona um atributo de log para **Agrupar por**, a lista e o gráfico mostram os resultados do filtro atual. No gráfico, colunas agrupadas em cores. Passar o Mouse sobre uma coluna no gráfico exibirá detalhes sobre as entradas específicas, semelhantes às informações gerais mostradas quando você expandir a Legenda do gráfico. Na legenda, você também pode optar por definir um filtro incluir ou excluir para um agrupamento específico.



Painel de detalhes do registro "flutuante"

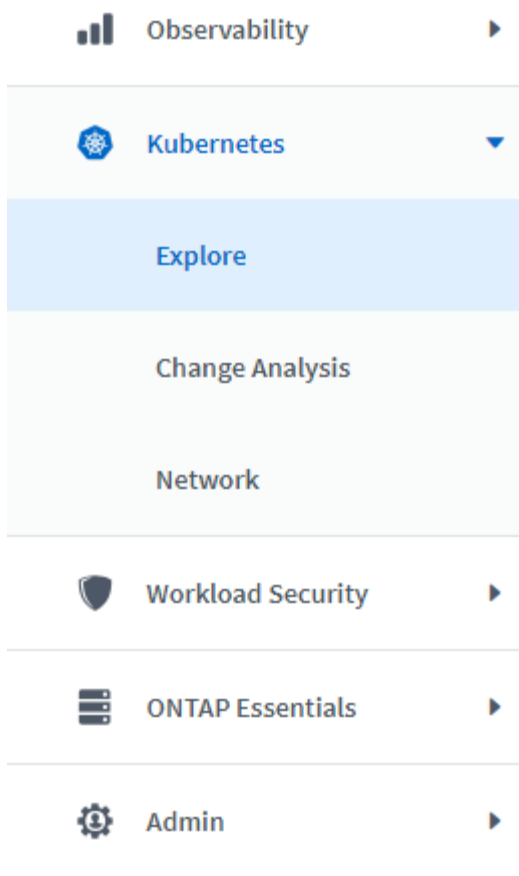
Ao explorar logs usando a consulta de log, selecionar uma entrada na lista abre um painel de detalhes para essa entrada. Agora você pode optar por exibir o painel deslizante "flutuante" (ou seja, exibido sobre o resto

da tela) ou "na página" (ou seja, exibido como seu próprio quadro dentro da página). Para alternar entre estas vistas, selecione o botão "in Page / Floating" (na página / flutuante) no canto superior direito do painel.



Recolher o Menu

Pode recolher o menu de navegação Cloud Insights do lado esquerdo selecionando o botão "minimizar" abaixo do menu. Enquanto o menu é minimizado, passe o Mouse sobre um ícone para ver qual seção ele abre; selecionar o ícone abre o menu e leva você diretamente para essa seção.



◀ Minimize

Melhorias no Data Collector

O Cloud Insights facilitou a exibição e a localização de informações sobre coletores de dados:

- **O processamento de listas de coletores de dados** é mais eficiente, o que significa que o tempo necessário para exibir e navegar nessas listas é muito reduzido. Se você tem um ambiente grande com muitos coletores de dados, você verá uma melhoria significativa ao listar seus coletores de dados.
- A matriz de suporte **Data Collector** passou de um arquivo .PDF para uma página baseada em .html, de forma mais rápida e fácil de manter. Confira a nova Matrix aqui: https://docs.netapp.com/us-en/cloudinsights/reference_data_collector_support_matrix.html

Agosto de 2023

Coleta de dados do Isilon/PowerScale Logs e do Advanced Analytics

Os coletores Isilon Rest e PowerScale Rest contêm as seguintes melhorias:

- Os eventos de log do Isilon estão disponíveis para uso em consultas e alertas
- Os atributos analíticos avançados do Isilon estão disponíveis para uso em consultas, painéis e alertas:
 - emc_isilon.cluster
 - emc_isilon.node
 - emc_isilon.node_disk
 - emc_isilon.net_iface

Estes são ativados por predefinição para utilizadores dos coletores de REPOUSO Isilon e/ou de REPOUSO PowerScale. O NetApp incentiva fortemente os usuários do coletor baseado na CLI do Isilon a migrar para o novo coletor baseado na API REST para receber melhorias como as acima.

Mapa de carga de trabalho aprimorado

O mapa de carga de trabalho é mais utilizável e menos barulhento; ele agrupa todos os serviços externos semelhantes em um nó se eles se comunicam com as mesmas cargas de trabalho, reduzindo a complexidade do gráfico e facilitando a compreensão de como os serviços são interconetados.

Escolher um nó agrupado exibirá uma tabela detalhada com as métricas de tráfego de rede para cada serviço externo relevante para esse nó.

Ajuste de uso da unidade gerenciada do Kubernetes

No caso de um recurso de computação em seu ambiente de cluster do Kubernetes ser contado pelo Operador de Monitoramento do Kubernetes do NetApp e por um coletor de dados de infraestrutura subjacente (por exemplo, VMware), seu uso desses recursos será ajustado para garantir a contagem mais eficiente de unidades gerenciadas. Você pode exibir os ajustes de MU do Kubernetes na página Admin > assinatura, nas guias Sumário e uso.

Separador Summary (Resumo):

Managed Unit (MU) Usage Calculator [Estimate Renewal Cost](#)

<input checked="" type="checkbox"/> Infrastructure Observability ?	82	Hosts	289,47	Raw TiB	55,75	Object TiB	Current Usage	Managed Units = 114.75
<input checked="" type="checkbox"/> Kubernetes Observability ?	64	vCPUs	Current Usage					Managed Units = 16
Adjustments:								
<input checked="" type="checkbox"/> Kubernetes Observability ?	2	Hosts	Adjustment for duplicate Infrastructure Observability Hosts				Managed Units = (1)	

Consumed Managed Units = **130/500**

Separador utilização:

Infrastructure Observability
 Kubernetes Observability

Installed Cluster Agents (3) ? Filter...

Name	vCPUs	Metered Managed Units	Managed Units Adjustment	Consumed Managed Units ↓
oc4-kp	48	12.00	(0.00)	12.00
july-deploy	8	2.00	(0.00)	2.00
twonode	8	2.00	(1.00)	1.00

Alterações do coletor/aquisição:

As seguintes alterações de coletor de dados/Unidade de aquisição estão em vigor:

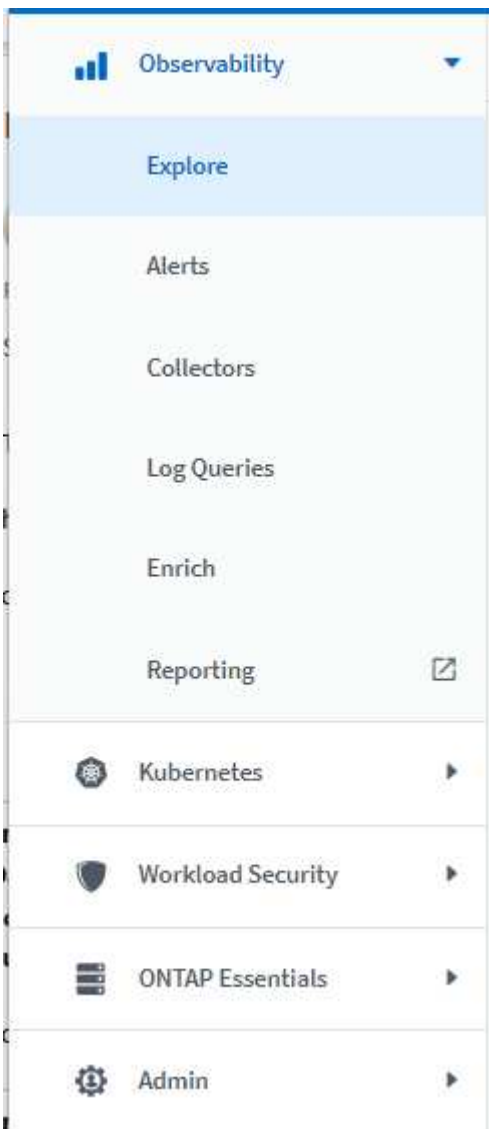
- As unidades de aquisição agora suportam RHEL 8,7.

Menus melhorados

Atualizamos o menu de navegação à esquerda para oferecer melhor suporte aos fluxos de trabalho de nossos clientes. Novos itens de nível superior, como *Kubernetes*, fornecem acesso acelerado ao que o cliente precisa, e um console consolidado de administradores suporta a função de proprietário do locatário.

Aqui estão alguns exemplos adicionais das mudanças:

- O menu *observability* de nível superior exibe consultas de descoberta de dados, alertas e log
- A funcionalidade "Acesso à API" para observabilidade e segurança de workload estão em um menu
- Da mesma forma, para a funcionalidade "notificações" de segurança de observabilidade e carga de trabalho, também agora em um menu



Aqui está uma breve lista dos recursos que você pode encontrar em cada menu:

Observabilidade:

- Explorar (painéis, consultas métricas, Insights de infraestrutura)
- Alertas (monitores e alertas)
- Coletores (coletores de dados e unidades de aquisição)
- Consultas de registo
- Enrich (Anotações e regras de Anotação, aplicativos, Resolução do dispositivo)
- Relatórios

Kubernetes:

- Exploração de cluster e mapa de rede

Segurança da carga de trabalho:

- Alertas
- Forense
- Coletores
- Políticas

Essenciais do ONTAP -

- Proteção de dados
- Segurança
- Alertas
- Infraestrutura
- Rede
- Cargas de trabalho *VMware

Admin:

- Acesso à API
- Auditoria
- Notificações
- Informações de subscrição
- Gerenciamento de usuários

Julho de 2023

Mostrar mudanças recentes

As páginas de destino do Data Collector agora incluem uma lista de mudanças recentes. Basta clicar no botão "mudanças recentes" na parte inferior de qualquer Landing page do coletor de dados para exibir as alterações recentes do coletor de dados.

Changes Reported by This Data Collector (1)

Time ↓	Change
07/06/2023 6:39:12 PM	<input type="checkbox"/> Storage CI-GDL1-Ontap-fas8080 configuration changed Property Display IP is changed from "10.192.122.10" to "10.192.122.12" Property Manage URL is changed from "HTTPS://10.192.122.10:443" to "HTTPS://10.192.122.12:443"

[Hide Recent Changes](#)

Melhorias do operador

As seguintes melhorias foram feitas na "[Operador do Kubernetes](#)" implantação:

- Opção para ignorar a coleção de métricas do docker
- Capacidade de adicionar e personalizar tolerações para telegraf Daemonsets e Replicasets

Insight: Recupere o storage frio

O "[Recupere o Insight do storage frio da ONTAP](#)" agora suporta FlexGroups, e agora está disponível para todos os clientes.

Assinatura da imagem do operador

Para clientes que usam um repositório privado para o Operador de Monitoramento do Kubernetes do NetApp, agora você pode copiar a chave Pública de assinatura de imagem durante a instalação do Operador, permitindo que você confirme a autenticidade do software baixado. Selecione o botão *Copy Image Signature Public Key* durante a etapa opcional para *carregar a imagem do operador para o seu repositório privado*.

[Copy Image Signature Public Key](#)

Reveal Image Signature Public Key

```
-----BEGIN PUBLIC KEY-----  
MIIBOjANBgkqhkiG9w0BAQEFAAOCAQY8AMIIBigKCAYEAoA/Iww7C/1DfDrwYKwPL  
hJzSbT7BnsV/j6Wh/U9Qv4MWhYPCT/uW8ucMPkIHK56bVeiy1di23TL16p+M7y2y  
JjgBSYJdEEOLlopj+X6W/N00B4kHMDLV8VXzJ0lk3zcT2NHiySzB/IYicTfhelpI  
hJzSbT7BnsV/j6Wh/U9Qv4MWhYPCT/uW8ucMPkIHK56bVeiy1di23TL16p+M7y2y  
NiX7KwYpG6K8YSIW89MvTwbgAr7S76liw8Um6VsnsXF655h3dd769UhahiQqv6Z5
```

Agregação, formatação condicional e muito mais para consultas

Agregação, seleção de unidade, formatação condicional e renomeação de coluna estão entre os recursos mais úteis de um widget de tabela de painel e agora esses mesmos recursos estão disponíveis para "[Consultas](#)".

143 items found

Table Row Grouping	Metrics & Attributes
agent.node_diskio ↑	io_time (ms)
nvme0n1	20,604,960.00
nvme0n1	29,184,970.00
nvme0n1	4,642,684.00
nvme0n1	31,918,988.00
nvme0n1	29,258,256.00
nvme0n1	18,022,164.00
nvme0n1	28,483,300.00
nvme0n1	69,835,016.00
nvme0n1	15,952,780.00
nvme0n1	44,169,696.00
nvme0n1	12,138,928.00
nvme0n1	5,234,528.00
nvme0n1	34,260,552.00

▼ Aggregation

Group By: Avg

Time Aggregate By: Last

▼ Unit Display

Base Unit: millisecond (ms)

Displayed In: millisecond (ms)

▼ Conditional Formatting Reset

If value is: > (Greater than)

Warning: Optional ms

Critical: Optional ms

> Rename Column

Esses recursos estão disponíveis agora para dados do tipo integração (Kubernetes, métricas avançadas do ONTAP, etc.) e estarão disponíveis em breve para objetos de infraestrutura (armazenamento, volume, switch, etc.).

API para auditoria

Agora você pode usar uma API para consultar ou exportar eventos auditados. Vá para Admin > API Access e selecione o link *API Documentation* para obter informações.

audit

POST

/audit/export Export audit data

POST

/audit/query Run a query for audit

Coletor de dados: Trident Economy

A Cloud Insights agora oferece suporte ao Trident Economy Driver, realizando estes benefícios:

- Obtenha visibilidade do mapeamento Qtree do pod-to-ONTAP e das métricas de performance.
- Forneça solução de problemas aprimorada e navegação fácil dos pods do Kubernetes ao storage de back-end
- Detectar proativamente problemas de desempenho no back-end com monitores

Junho de 2023

Confira seu uso

A partir de junho de 2023, o Cloud Insights fornece um detalhamento do uso da Unidade gerenciada com base no conjunto de recursos. Agora você pode visualizar e monitorar o uso de unidade gerenciada (MU) para sua infraestrutura, bem como o uso de MU vinculado ao Kubernetes.



O monitoramento e o mapa da rede do Kubernetes estão disponíveis para todos

O "[Desempenho da rede do Kubernetes e mapa](#)" simplifica a solução de problemas mapeando dependências entre workloads Kubernetes, fornecendo visibilidade em tempo real das latências de desempenho da rede Kubernetes e anomalias para identificar problemas de desempenho antes que eles afetem os usuários. Muitos clientes acharam isso útil durante o Preview, e agora está disponível para todos desfrutarem.

Alterações do coletor/aquisição:

As seguintes alterações de coletor de dados/Unidade de aquisição estão em vigor:

- As MUs de domínio de dados e Cohesity são dosadas a 40 TiB : 1 MU.
- As unidades de aquisição agora suportam RHEL e Rocky 9,0 e 9,1.

Novos painéis do ONTAP Essentials

Os seguintes painéis do ONTAP Essentials estão disponíveis em ambientes de visualização e agora estão disponíveis para todos:

- Painel de segurança
- Painel de proteção de dados (inclui visões gerais de proteção local e remota)

Monitores adicionais do sistema

Os seguintes monitores do sistema estão incluídos no Cloud Insights:

- Storage VM FCP Service indisponível
- Storage VM iSCSI Service indisponível

Maio de 2023

Instalação aprimorada do operador de monitoramento do Kubernetes

A instalação e configuração do ["Operador de monitoramento do Kubernetes do NetApp"](#) é mais fácil do que nunca com as seguintes melhorias:

- O ambiente ["definições de configuração"](#) é mantido em um único arquivo de configuração auto-documentado.
- Instruções passo a passo para fazer o upload de imagens do operador de monitoramento do Kubernetes para o seu repositório privado.
- Simples de atualizar com um único comando para atualizar seu monitoramento Kubernetes e manter configurações personalizadas.
- Mais seguro: As chaves de API estão gerenciando segredos com segurança.
- Fácil de integrar e implantar com suas ferramentas de automação de CI/CD.

Virtualização de storage

O Cloud Insights pode diferenciar entre um storage array com armazenamento local ou virtualização de outros storage arrays. Isso possibilita relacionar os custos e diferenciar a performance do front-end todo o caminho até o back-end da sua infraestrutura.

Storage Summary

Model:
V-Series

Vendor:
NetApp

Family:
V-Series

Serial Number:
1306894

IP:
192.168.7.41

Virtualized Type:
Virtual

Backend Storage:
Sym-000050074300343

Microcode Version:
8.0.2 7-Mode

Raw Capacity:
0.0 GiB

Latency - Total:
N/A

IOPS - Total:
N/A

Throughput - Total:
N/A

Management:

FC Fabrics Connected:
7

Alert Monitors:

Novos parâmetros do Webhook

Ao criar uma "Webhook" notificação, agora você pode incluir esses parâmetros na definição do webhook:

- %%TriggereOnKeys%%
- %%TriggeredOnValues%%

Geração de relatórios sobre dados do Kubernetes

Os dados do Kubernetes coletados pelo Cloud Insights, incluindo volumes persistentes (PV), PVC, workloads, clusters e namespaces, agora estão disponíveis para uso em relatórios. Isso permite chargeback, tendências, previsões, cálculos TTF e outros relatórios de negócios sobre métricas do Kubernetes.

Monitores de sistema ONTAP padrão ativados para novos clientes

Muitos monitores do sistema ONTAP estão ativados (ou seja, *retomado*) por padrão em novos ambientes Cloud Insights. Anteriormente, a maioria dos monitores tinha padrão para o estado *Pausado*. Como as necessidades de negócios variam de empresa para empresa, recomendamos sempre dar uma olhada no "monitores do sistema" seu ambiente e pausar ou retomar cada uma com base em suas necessidades de alerta.

Abril de 2023

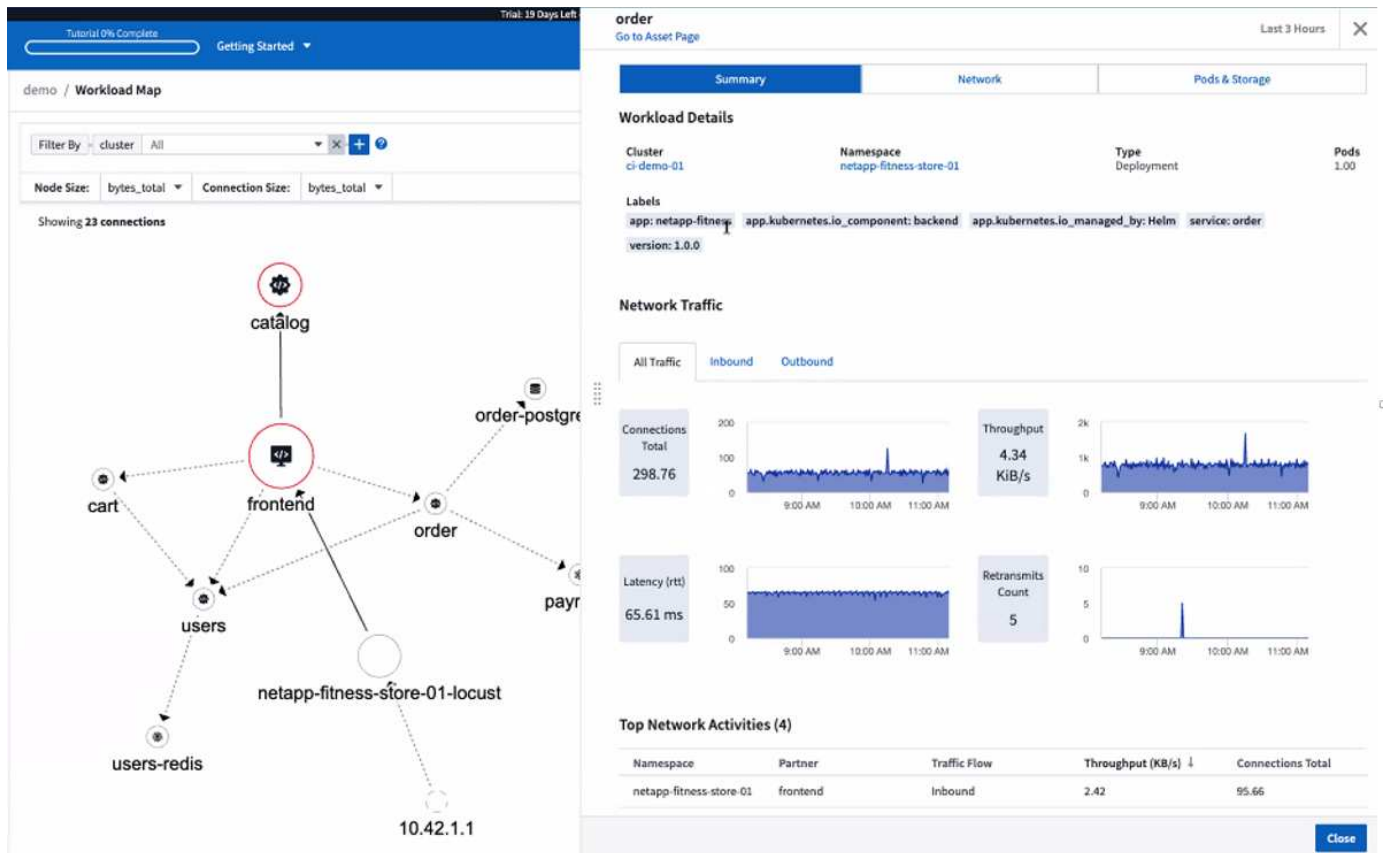
Monitoramento e mapa de performance do Kubernetes

O "[Desempenho da rede do Kubernetes e mapa](#)" recurso simplifica a solução de problemas mapeando dependências entre workloads do Kubernetes. Ele oferece visibilidade em tempo real das latências de performance e anomalias da rede Kubernetes para identificar problemas de performance antes que eles afetem os usuários. Essa funcionalidade ajuda as organizações a reduzir os custos gerais analisando e auditando os fluxos de tráfego do Kubernetes.

Principais recursos:

- O mapa de carga de trabalho apresenta dependências e fluxos de carga de trabalho do Kubernetes e destaca problemas de rede e desempenho.
- Monitore o tráfego de rede entre pods, cargas de trabalho e nós do Kubernetes; identifique a origem dos problemas de latência e tráfego.
- Reduzir os custos gerais analisando o tráfego de rede de entrada, saída, cross-region e cross-zone.

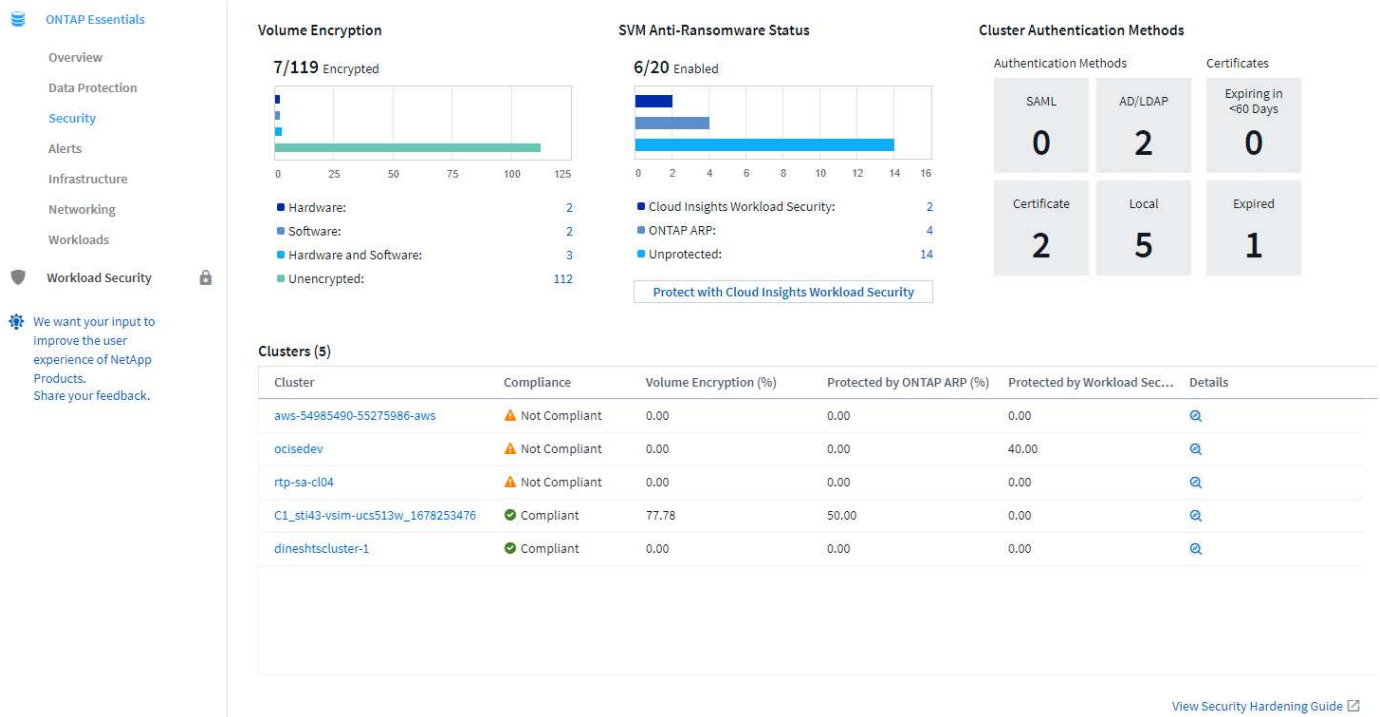
Mapa de workload mostrando detalhes de "Slideout":



O monitoramento e o mapa de performance do Kubernetes estão disponíveis como "Pré-visualização" recurso.

Painel de segurança do ONTAP Essentials

O "Painel de segurança" oferece uma visão instantânea da situação de segurança atual, mostrando gráficos para criptografia de volume de hardware e software, status anti-ransomware e métodos de autenticação de cluster. O Painel de Segurança está disponível como um "Pré-visualização" recurso.



Recupere o storage frio da ONTAP

O Insight *Reclaim ONTAP Cold Storage* fornece dados sobre capacidade inativa, potencial economia de custo/energia e itens de ação recomendados para volumes em sistemas ONTAP.



84 Workloads on storage **umeng-aff300-01-02** contains a total of 1.2 TiB of cold data.

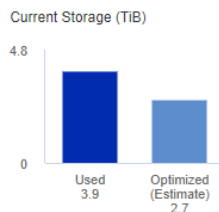
You could lower costs 5.6% a year and reduce your carbon footprint by moving cold storage to the cloud.

Detected: 16 days ago, 9:21 AM
(ACTIVE)
Apr 14, 2023 12:06PM

Estimated Yearly Cost Savings*

\$1,228.80

Move 1.2 TiB of data to the cloud



kWh Reduction Yearly Savings**

76.75 kWh

Hold or cycle down available storage

2 x 1 TiB SSDs = 76.75 kWh per year **

*Visit the [NetApp TCO Calculator](#) for your actual cost savings.
Go to [Annotation Page](#) to edit the cloud tier cost in the tier annotation.

** Based on average disk power consumption


Com este Insight, você pode responder a perguntas como:

- Que quantidade de dados inativos em um cluster de storage estão armazenados em (a) discos SSD de alto custo, (b) discos HDD e (c) discos virtuais?
- Quais workloads são os maiores contribuintes em relação ao storage não otimizado?
- Qual é a duração (em dias) que os dados ficaram inativos em uma determinada carga de trabalho?

Recuperar o storage frio do ONTAP é considerado um "Preview" recurso e, portanto, está sujeito a alterações.

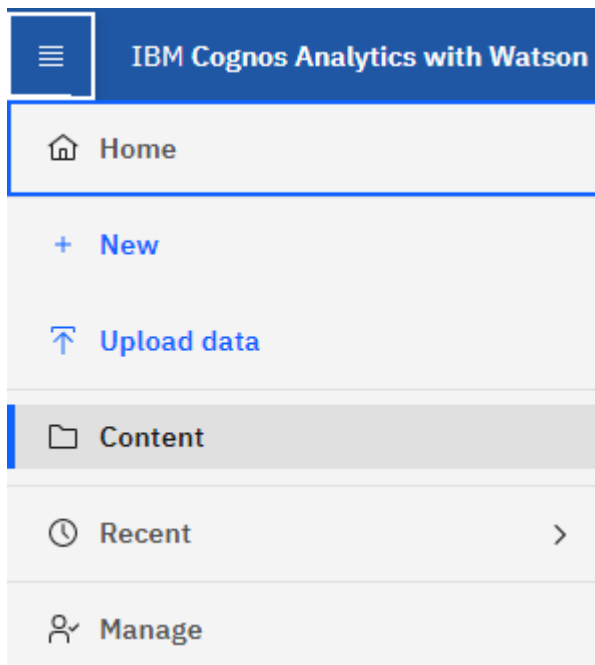
A notificação de assinatura também controla as mensagens de banner

Definir destinatários para notificações de assinatura (Admin > notificações) agora também controla quem verá notificações de banner no produto relacionadas à assinatura.

 Your subscription is expiring in 2 days. [View Subscription](#)

A reportagem tem um novo visual

Você notará que as telas de relatórios do Cloud Insights têm uma nova aparência e que algumas das opções de navegação do menu foram alteradas. Estes ecrãs e alterações de navegação foram atualizados no atual "Documentação de relatórios".



Monitores em pausa por predefinição

Para novos ambientes Cloud Insights, esteja ciente de que "monitores definidos pelo sistema" não envie notificações de alerta por padrão. Você precisará ativar notificações para qualquer monitor que você deseja alertá-lo, adicionando um ou mais métodos de entrega para o monitor. Para ambientes Cloud Insights existentes, a lista de destinatários de notificação *global* padrão foi removida para todos os monitores definidos pelo sistema atualmente no estado *pausado*. As notificações definidas pelo usuário permanecem inalteradas, assim como as configurações de notificação para monitores definidos pelo sistema atualmente ativos.

Procurando a guia API Metering?

A Monitoração de API foi movida da página de assinatura para a página **Admin > API Access**.

Março de 2023

Conexão com a nuvem para ONTAP 9.9 ou superior obsoleta

O coletor de dados Cloud Connection for ONTAP 9.9 está sendo obsoleto. A partir de 4 de abril de 2023, os coletores de dados do Cloud Connection em seu ambiente não coletarão mais dados e, em vez disso, apresentarão um erro ao polling. O coletor de dados do Cloud Connection será removido completamente do Cloud Insights em uma atualização subsequente.

Antes de 4 de abril de 2023, é obrigatório configurar um novo coletor de dados do software de gerenciamento de dados NetApp ONTAP para qualquer sistema ONTAP coletado atualmente pelo Cloud Connection. "[Saiba mais](#)".

Janeiro de 2023

Novos monitores de registro

Adicionamos quase duas dúzias "[monitores adicionais do sistema](#)" para alertar para links de interconexão quebrados, problemas de heartbeat e muito mais. Além disso, três novos monitores de log de proteção de dados foram adicionados para alertar sobre alterações de resincronização automática do SnapMirror, Espelhamento do MetroCluster e resincronização do FabricPool.

Note que alguns desses monitores serão *enabled* por padrão; você deve *pause* eles se você não quiser alertá-los. Observe também que esses monitores não estão configurados para entregar notificações; você deve configurar destinatários de notificação nesses monitores se quiser enviar alertas por e-mail ou webhook.

Exportação .CSV para todos os Widgets de Tabela do Painel

Garantir a acessibilidade aos seus dados é essencial, por isso disponibilizamos a exportação .CSV para todas as consultas de métricas, widgets de tabela de dashboard e páginas de destino de objetos, independentemente do tipo de dados (ativo ou integração) que está a consultar.

Personalizações de dados como seleção de colunas, renomeação de colunas e conversões de unidades também estão incluídas na nova funcionalidade de exportação.

Dezembro de 2022

Explore a proteção contra ransomware e outros recursos de segurança durante a avaliação do Cloud Insights

A partir de hoje, a inscrição em uma nova avaliação do Cloud Insights permite que você explore recursos de segurança, como detecção de ransomware e política de resposta automatizada de bloqueio de usuário. Se você não se inscreveu para o seu Teste, faça-o hoje!

Os workloads do Kubernetes têm sua própria página inicial

Os workloads são uma parte essencial do seu ambiente Kubernetes. Portanto, o Cloud Insights agora fornece páginas iniciais para esses workloads. Aqui, você pode visualizar, explorar e solucionar problemas que afetam seus workloads do Kubernetes.

Filter By + ⓘ

1/1

Pods: Current / Desired

-

Up-to-date

-

Unavailable

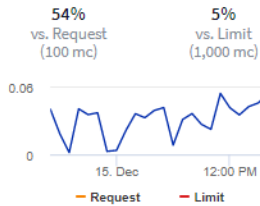
Namespace **dockerimage-monitoring** Type **ReplicaSet** Date Created **Dec 9, 2022 4:37 PM**

Labels

-

54mc

CPU

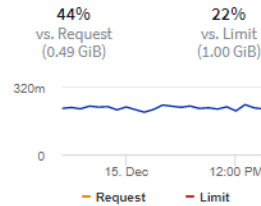


Highest CPU Demand by Pod

2.8m [telegraf-rs-2xsj2](#)

0.22GiB

Memory



Highest Memory Demand by Pod

0.21 GiB [telegraf-rs-2xsj2](#)

0.00GiB

Total PVC Capacity claimed

Pods (1)

Pod Name ↑	Status	Healthy Containers	cpu_usage_nanocores (mc)	memory_rss_bytes (GiB)
telegraf-rs-2xsj2	● Healthy Running	1 of 1	3	0.21

Verifique suas somas de verificação

Você nos pediu para fornecer valores de checksum durante a instalação do agente para Windows e Linux e achamos que é uma ótima ideia. Então aqui estão eles:

☑ Manually Verifying Telegraf Checksums

The Cloud Insights agent installer performs integrity checks, but some users may want to perform their own verifications before installing or applying downloaded artifacts.

For more information, read about [verifying checksums](#) before proceeding to the next step.

The SHA256 checksum for this telegraf.pkg is:

```
cbd0d8d0512b65fbcd0c786d8d0512b651de0e1cf003e0a0d9df01d8d0512b65
```

Melhorias de alertas de log

Agrupar por

Ao criar ou editar um Monitor de Registros, agora você pode definir atributos "Agrupar por" para permitir alertas mais focados. Procure os atributos "Agrupar por" abaixo das configurações de "filtro" na definição do monitor.

1 Select the log to monitor

The screenshot shows a configuration interface for selecting logs to monitor. It includes a 'Log Source' dropdown set to 'logs.netapp.ems'. Below it, a 'Filter By' section contains several filters: 'ems.ems_message_type' with a dropdown set to 'Nblade.vscanConnBackPressure', 'ems.cluster_vendor' set to 'NetApp', and 'ems.cluster_model' with a list of models: 'FAS*', 'AFF*', 'ASA*', and 'FDvM*'. A 'Group By' section is also present, listing 'ems.cluster_uuid', 'ems.cluster_vendor', 'ems.cluster_model', 'ems.cluster_name', 'ems.svm_uuid', and 'ems.svm_name'.

Essa alteração traz monitores métricos e monitores de log para a paridade de recursos normalizando o aspecto "Agrupar por" das Definições do Monitor. Essa paridade permitirá que os clientes clonem/dupliquem monitores padrão definidos pelo sistema **All** para maior personalização.

Duplicação

Agora você pode clonar (duplicar) os monitores Log de alterações, Log do Kubernetes e Log de coletores de dados. Isso cria um novo monitor de log personalizado que você pode modificar para suas definições específicas.

The screenshot shows a table titled 'Data Collection (4)'. The table has columns for Name, Metric / Parameters, Severity, Time Frame, and Status. There are two rows of data. The first row is 'Acquisition Unit Heartbeat-Critical' with a severity of 'Critical' and status 'Active'. The second row is 'Acquisition Unit Heartbeat-Warning' with a severity of 'Warning' and status 'Active'. A red arrow points to a 'Duplicate' button in the actions column of the second row.

Name	Metric / Parameters	Severity	Time Frame	Status
Acquisition Unit Heartbeat-Critical	logs.cloud_insights.acquisition (source = acquisition_unit:*, acquisition_unit.status = "Heartbeat Overdue", acquisition_unit.overdue_time >= 600 sec)	Critical	Once	Active
Acquisition Unit Heartbeat-Warning	logs.cloud_insights.acquisition (source = acquisition_unit:*, acquisition_unit.status = "Heartbeat Overdue", acquisition_unit.overdue_time >= 300 sec)	Warning	Once	Active

11 novos monitores ONTAP padrão cobrindo SnapMirror para continuidade de negócios

Adicionamos quase uma dúzia de novos "monitores do sistema" para o SnapMirror for Business Continuity (SMBC), que alertam sobre mudanças nos certificados SMBC e mediadores ONTAP.

Novembro de 2022

Mais de 40 novos monitores de segurança, coleta de dados e CVO!

Adicionamos dezenas de novos monitores definidos pelo sistema para alertá-lo para possíveis problemas com o Cloud volumes, segurança e proteção de dados. Leia mais sobre esses monitores "aqui".

Outubro de 2022

Detecção de ransomware melhor e mais precisa com a integração do ONTAP Autonomous ransomware Protection

O Cloud Secure melhora a detecção de ransomware pela integração com o ONTAP "Proteção autônoma contra ransomware"(ARP).

O Cloud Secure recebe eventos ARP do ONTAP em potencial atividade de criptografia de arquivos de volume e.

- Correlaciona os eventos de criptografia de volume com a atividade do usuário para identificar quem está causando o dano,
- Implementa políticas de resposta automática para bloquear o ataque,
- Identifica quais arquivos foram afetados, ajudando a recuperar mais rapidamente e a conduzir investigações de violação de dados.

Setembro de 2022

Monitores disponíveis na Edição básica

ONTAP "Monitores predefinidos" agora disponível para uso na Edição básica do Cloud Insights. Isso inclui mais de 70 monitores de infraestrutura e 30 exemplos de carga de trabalho.

Painéis de energia e StorageGRID da ONTAP

A galeria do dashboard inclui um novo painel para potência e temperatura ONTAP, bem como quatro painéis para StorageGRID. Se o seu ambiente estiver coletando métricas de energia e/ou dados StorageGRID do ONTAP, importe esses painéis selecionando * na Galeria*.

Visibilidade de limite imediata nas tabelas

A formatação condicional permite que você defina e realce limiares de nível de aviso e nível crítico em widgets de tabela, trazendo visibilidade instantânea para outliers e pontos de dados excepcionais.

14 items found in 1 group

Table Row Grouping	Expanded Detail	Metrics & Attributes	
All	Storage Pool	capacityRatio.used (%)	capacity.provisioned (GiB)
All (14)	--	95.15	
--	rtp-sa-cl06-02:aggr_data1_rtp_sa_cl06_02	0.79	
--	rtp-sa-cl06-01:aggr_data1_rtp_sa_cl06_01	2.45	
--	rtp-sa-cl06-02:aggr0_rtp_sa_cl06_02_root	95.15	
--	rtp-sa-cl06-01:aggr0_rtp_sa_cl06_01_root	95.15	

Formatting: Show Expanded Details Conditional Formatting: Background Color + Icon Show In Range as green

> Aggregation

> Unit Display

Conditional Formatting Reset

If value is

Warning %

Critical %

> Rename Column

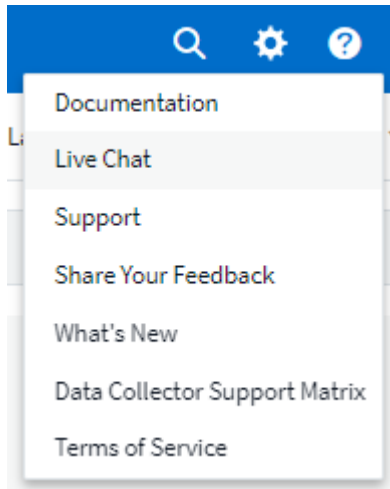
Monitor de segurança

O Cloud Insights pode alertá-lo quando deteta que o modo FIPS está desativado no sistema ONTAP. Leia

mais sobre "[Monitores do sistema](#)", e assista a este espaço para mais monitores de segurança, em breve!

Converse de qualquer lugar

Converse com um especialista de suporte da NetApp em qualquer tela do Cloud Insights selecionando o novo link **Ajuda > Chat ao vivo**. A ajuda está disponível no ícone "?" no canto superior direito do ecrã.



Insights mais visíveis

Se o seu ambiente estiver passando "[Insight](#)" por *recursos compartilhados sob estresse* ou *namespaces Kubernetes funcionando fora do espaço*, as páginas de destino de ativos para recursos afetados agora incluem links para o próprio Insight, fornecendo exploração e solução de problemas mais rápidos.

Novos coletores de dados

- Amazon S3 (disponível em prévia)
- Brocade FOS 9,0.x
- Dell/EMC PowerStore 3.0.0.0

Outras atualizações do Data Collector

Todas as fontes de dados agora são otimizadas para retomar a pesquisa de desempenho após atualizações e/ou patches da Unidade de aquisição.

Suporte ao sistema operacional

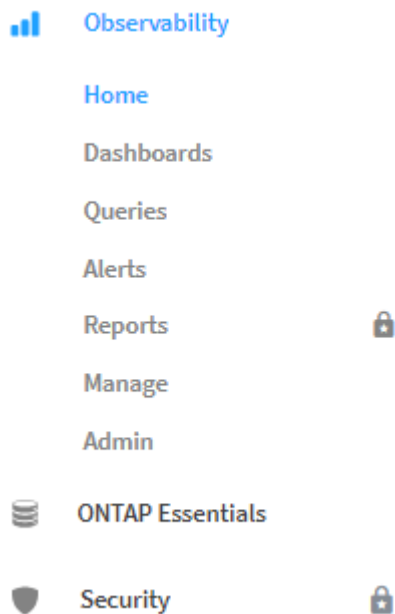
Os seguintes sistemas operacionais são suportados com unidades de aquisição Cloud Insights, além dos seguintes "[já suportado](#)":

- Red Hat Enterprise Linux 8,5, 8,6

Agosto de 2022

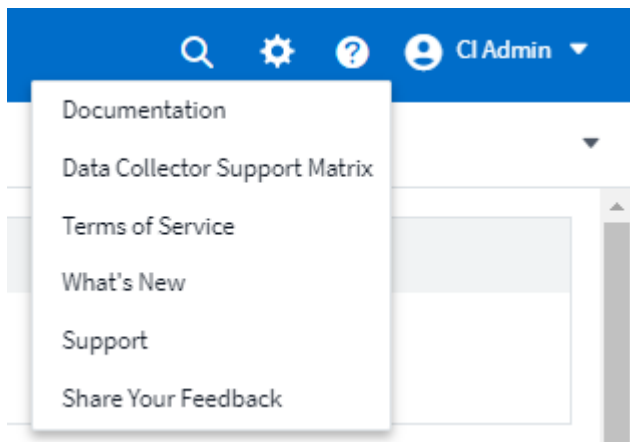
Cloud Insights tem um novo visual!

A partir deste mês, "Monitor and Optimize" foi renomeado como **observabilidade**. Você encontrará todos os seus recursos favoritos, como painéis, consultas, alertas e relatórios aqui. Além disso, procure por Cloud Secure no novo menu **Segurança**. Note que apenas os menus foram alterados; a funcionalidade da funcionalidade permanece a mesma.



Procurando o menu **Ajuda**?

Ajuda agora vive no canto superior direito da tela.

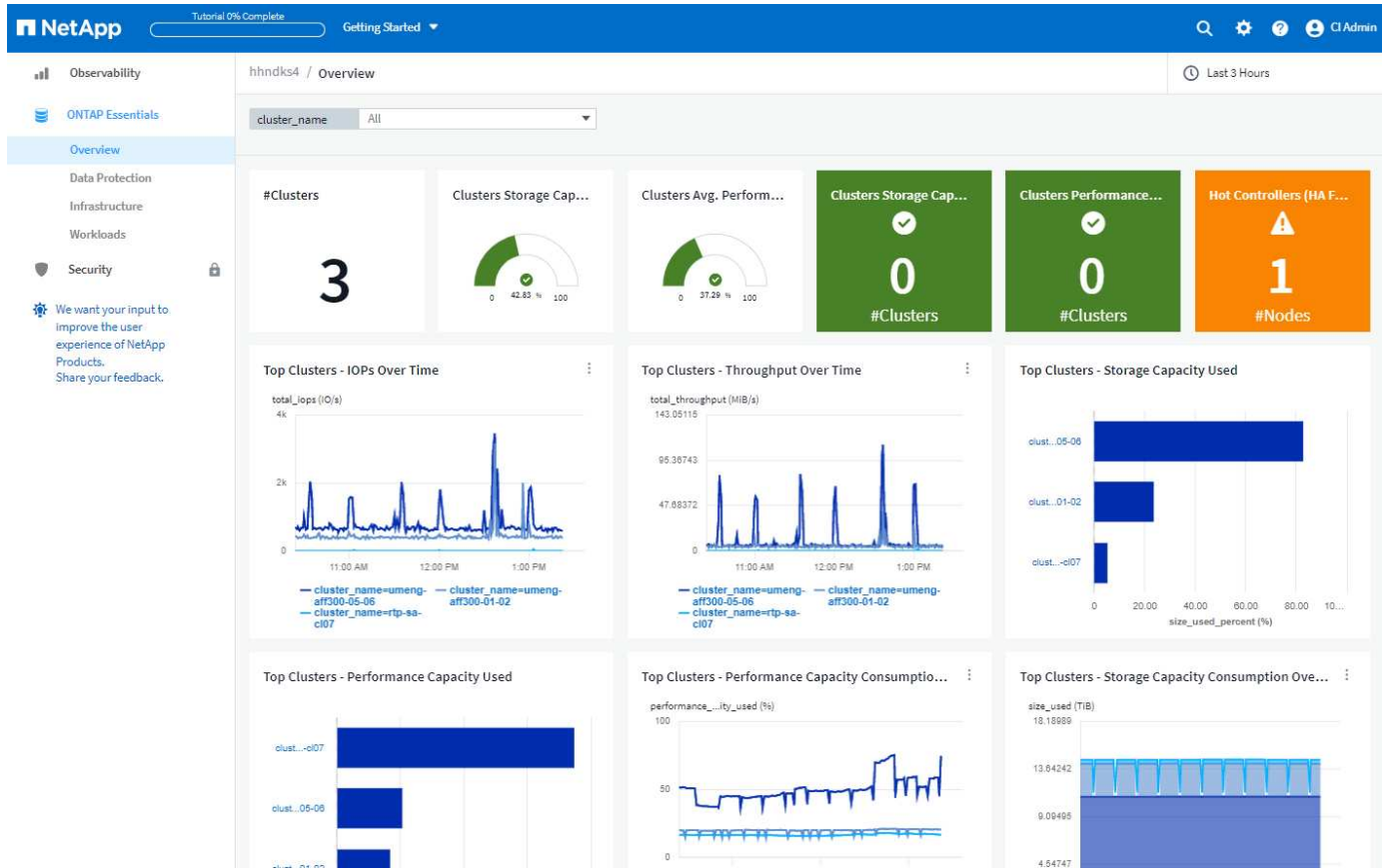


Não sabe por onde começar? Confira o ONTAP Essentials!

"Princípios Básicos da ONTAP" É um conjunto de painéis e workflows que fornece visualizações detalhadas sobre seus inventários, workloads e proteção de dados da NetApp ONTAP, incluindo previsões diárias completas de capacidade de storage e performance. Você pode ver até mesmo se quaisquer controladores estão sendo executados com alta utilização. O ONTAP Essentials é o local ideal para todas as suas necessidades de monitorização NetApp ONTAP!

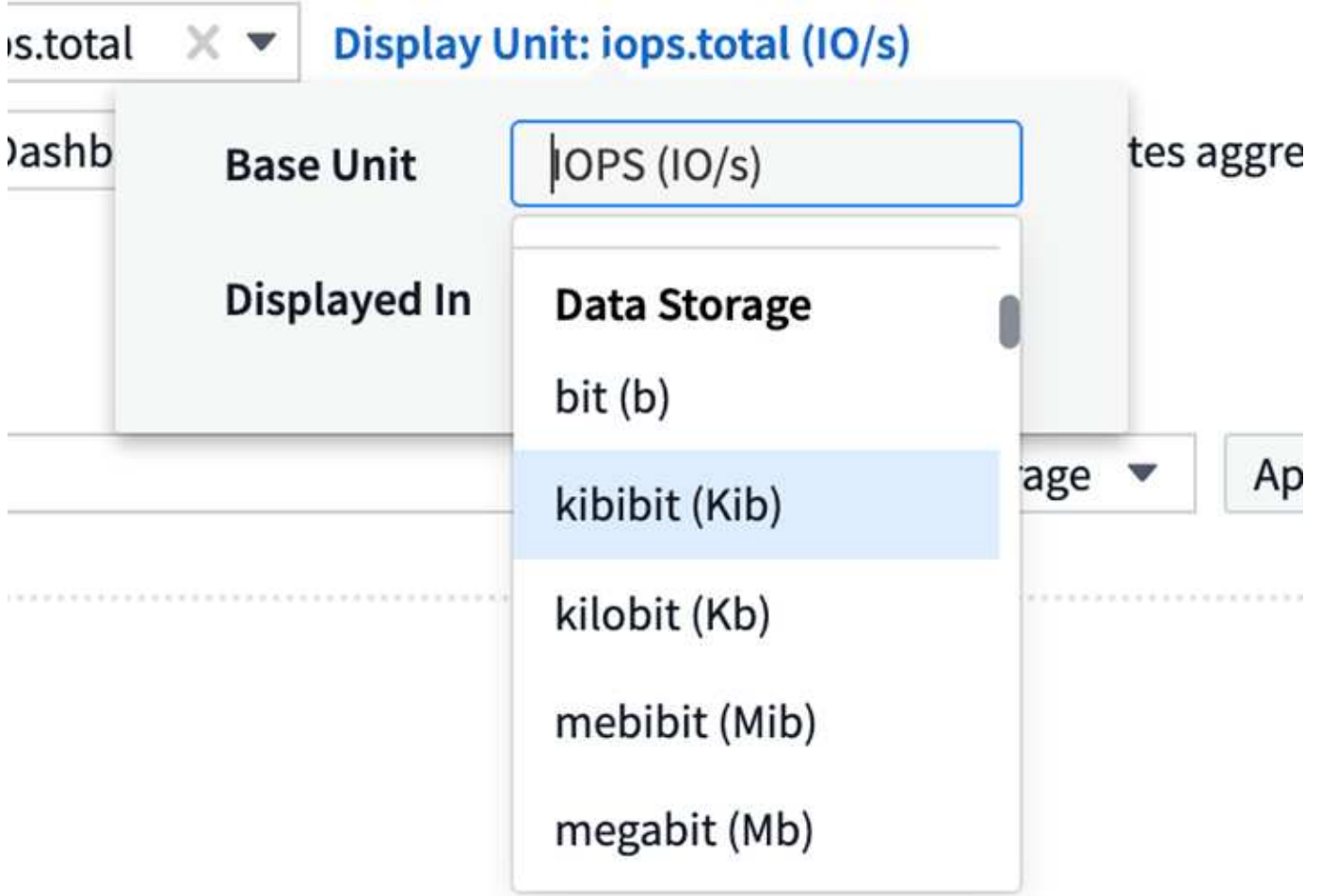
O ONTAP Essentials - disponível em todas as edições - foi projetado para ser intuitivo para os operadores e

administradores de ONTAP existentes, facilitando a transição do Gerenciador Unificado ActiveIQ para as ferramentas de gerenciamento baseadas em serviços.



As famílias de dados de armazenamento são mescladas

Você pediu, e agora você tem. As unidades de dados base-2 e base-10 de armazenamento agora são combinadas em uma família, de bits e bytes a tebibits e terabytes, facilitando a exibição de dados em seus painéis. As taxas de dados também são uma grande família própria.



Quanta energia o meu armazenamento está usando?

Exiba e monitore o consumo de energia, a temperatura e a velocidade do ventilador do seu compartimento de armazenamento ONTAP usando as métricas NetApp_ONTAP.storage_shelf, NetApp_ONTAP.System_node e NetApp_ONTAP.cluster (somente consumo de energia).

Cloud Insights (Trial) Tutorial 0% Complete Getting Started ▾ CI Admin ▾

MONITOR & OPTIMIZE ▾ diwlwtk / All Metric Queries / Storage Shelf Last 3 Hours Save ▾

netapp_ontap.storage_shelf

Filter By + ⓘ

Group cluster_name X

2 items found in 2 groups

Table Row Grouping	Expanded Detail	Metrics & Attributes							
cluster_name	netapp_ontap.storage_s...	average_...	power	min_ambient_...	min_temperat...	max_temperat...	average_temp...	average_fan_s...	min_fan_spe
rtp-sa-cl06 (1)	1.0	23.00	0.26	23.00	25.00	38.00	30.86	2,997.50	2,970.00
umeng-aff300-01-02 (1)	1.1	27.00	0.15	27.00	30.00	41.00	32.40	2,970.00	2,940.00

30.00

Share your feedback! We want your input to help

Recursos graduados em Preview

Os seguintes recursos foram removidos do Preview e agora estão disponíveis para todos os clientes:

Recurso	Descrição
Namespaces do Kubernetes estão ficando sem espaço	Os namespaces <i>Kubernetes em execução fora do espaço</i> Insight oferecem uma visão das cargas de trabalho nos namespaces do Kubernetes que correm o risco de ficar sem espaço, com uma estimativa do número de dias restantes antes que cada espaço fique cheio. "Leia mais"
Recurso compartilhado sob estresse	O insight <i>Shared Resource sob estresse</i> usa IA/ML para identificar automaticamente onde a contenção de recursos está causando degradação do desempenho no seu ambiente, destaca quaisquer cargas de trabalho afetadas por ele e fornece ações recomendadas para correção, permitindo que você resolva problemas de desempenho com mais rapidez. "Leia mais"
Cloud Secure – Bloquear o acesso do usuário ao ataque	Maior proteção para dados essenciais aos negócios, com a capacidade de bloquear o acesso do usuário quando um ataque é detectado. O acesso pode ser bloqueado automaticamente, usando políticas de resposta automatizadas ou manualmente a partir das páginas de alerta ou detalhes do usuário. "Leia mais"

Como é a saúde da minha coleta de dados?

O Cloud Insights fornece dois novos monitores de batimentos cardíacos para suas unidades de aquisição, bem como dois monitores para alertá-lo sobre falhas no coletor de dados. Eles podem ser usados para alertá-lo rapidamente sobre problemas de coleta de dados.

Os seguintes monitores estão agora disponíveis no grupo de monitores *coleta de dados*:

- Unidade de aquisição Heartbeat-Critical
- Aviso de batimento cardíaco da unidade de aquisição
- O coletor falhou
- Aviso do coletor

Observe que esses monitores estão no estado *Pausado* por padrão. Ative-os para serem alertados sobre problemas de coleta de dados.

Tokens de API de renovação automática

Os tokens de acesso à API agora podem ser definidos para renovação automática. Ao ativar esse recurso, tokens de acesso à API novos/atualizados serão gerados automaticamente para tokens expirados. Os agentes do Cloud Insights que usam um token expirando serão atualizados automaticamente para usar o token de acesso à API novo/atualizado correspondente, permitindo que eles continuem operando sem interrupções. Basta marcar a caixa "renovar token automaticamente" ao criar seu token. Esse recurso é atualmente suportado em agentes do Cloud Insights executados na plataforma Kubernetes com o mais recente Operador de Monitoramento do Kubernetes do NetApp.

Basic Edition dá-lhe mais do que antes

A sua avaliação está a terminar, mas ainda não tem a certeza se uma subscrição é adequada para si? O Basic Edition sempre deu a você a chance de continuar usando o Cloud Insights com seu coletor de dados ONTAP atual, mas agora você pode continuar capturando dados de versão, topologia e IOPS/taxa de transferência/latência da VMware. Os clientes da NetApp com suporte premium em seus sistemas de storage também terão direito a suporte para Cloud Insights.

Quer saber mais?

Consulte a seção **Centro de Aprendizagem** da página Ajuda > suporte para obter links para as ofertas de cursos da Universidade NetApp Cloud Insights!

Suporte ao sistema operacional

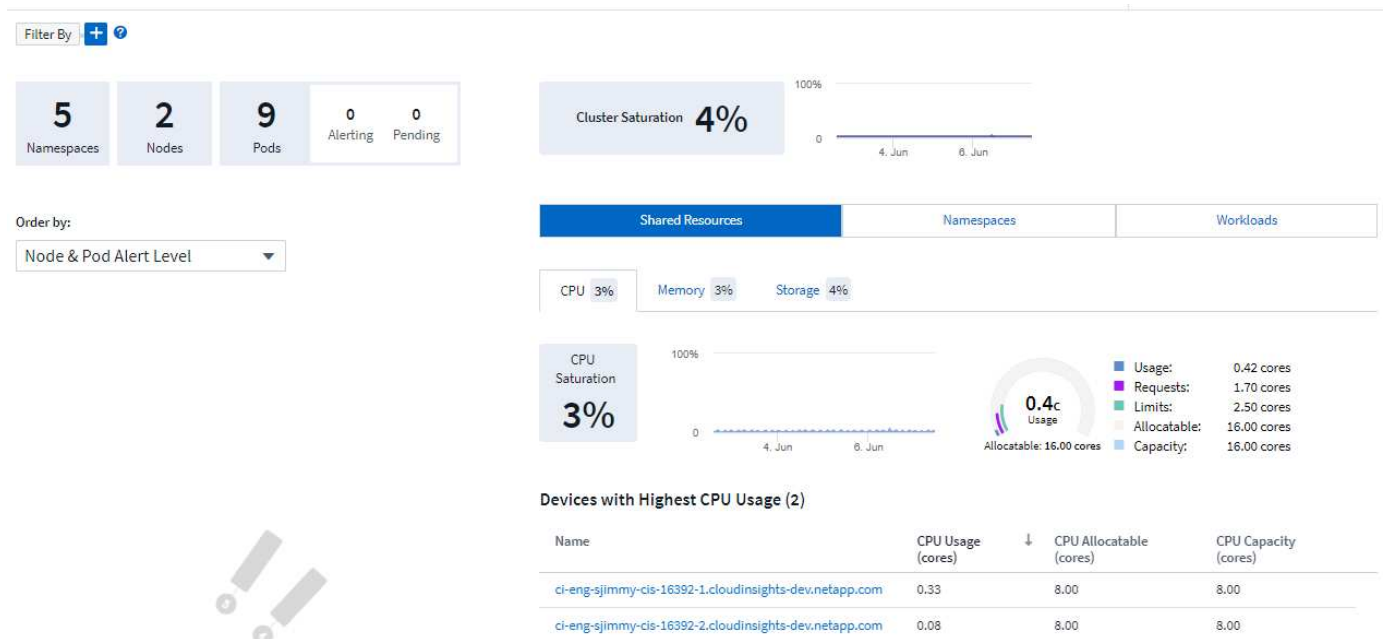
O seguinte sistema operacional é suportado com unidades de aquisição Cloud Insights, além das seguintes "já suportado":

- Windows 11

Junho de 2022

Saturação do cluster do Kubernetes e outros detalhes

O Cloud Insights facilita mais do que nunca explorar seu ambiente Kubernetes com uma página de detalhes do cluster aprimorada que fornece detalhes de saturação, bem como uma visão mais limpa de namespaces e workloads.



A página de lista de clusters também oferece uma visualização rápida da saturação, além das contagens de nó, pod, namespace e workload:

Filter By + ?

Clusters (2)

Name ↑	Overall Saturation (%)	CPU Saturation (%)	Memory Saturation (%)	Storage Saturation (%)	Nodes	Pods	Namespaces	Workloads
self	56	25	56	31	2	63	18	68
setoK3s	4	2	3	4	2	9	5	7

Quantos anos tem o seu cluster Kubernetes?

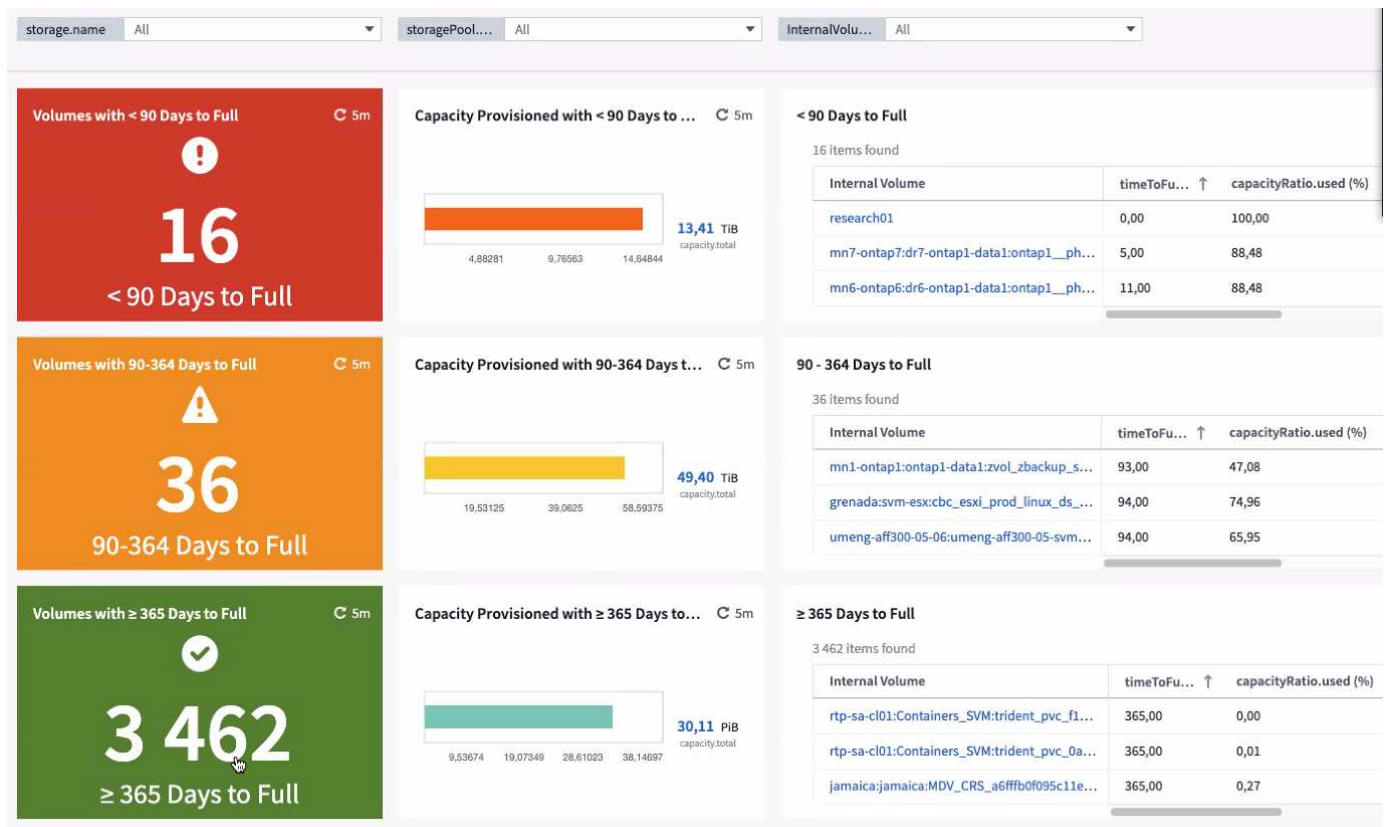
O seu cluster está apenas começando no mundo, ou já experimentou uma longa vida digital? *Age* foi adicionado como uma métrica de tempo coletada para nós do Kubernetes.

2 items found in 2 groups

Table Row Grouping		Expanded Detail	Metrics & Attributes
<input type="checkbox"/> node_name ↑	kubernetes_cluster	kubernetes.node	age (day)
<input type="checkbox"/> ci-aumonitor-1 (1)	aumonitor	ci-aumonitor-1	10.82
<input type="checkbox"/> ci-aumonitor-2 (1)	aumonitor	ci-aumonitor-2	10.82

Previsão do tempo para o máximo de capacidade

O Cloud Insights fornece um painel para prever o número de dias até a capacidade acabar para cada volume interno monitorado. Esses valores podem ajudar a reduzir significativamente o risco de uma interrupção.

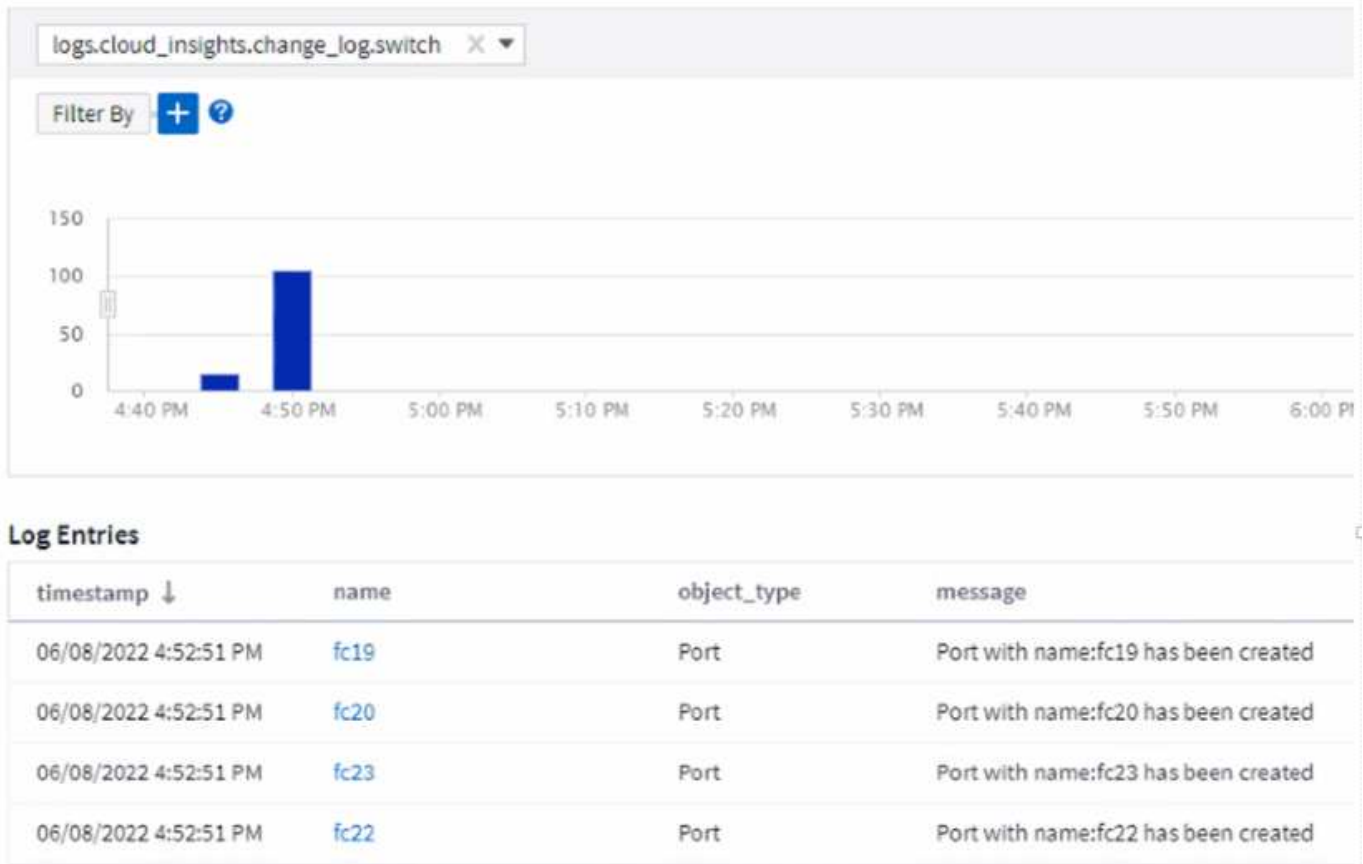


Os contadores TTF também estão disponíveis para armazenamento, pool de armazenamento e volume. Continue assistindo a esse espaço para painéis adicionais para esses objetos.

Observe que a previsão de tempo para tempo integral está saindo do *Preview* e será implementada para todos os clientes.

O que mudou no meu ambiente?

As entradas de registro de alterações do ONTAP podem ser visualizadas no explorador de registros.



Suporte ao sistema operacional

Os seguintes sistemas operacionais são suportados com unidades de aquisição Cloud Insights, além dos seguintes "já suportado":

- Fluxo CentOS 9
- Windows 2022

Agente Telegraf atualizado

O agente para ingestão de dados de integração telegraf foi atualizado para a versão **1.22.3**, com melhorias de desempenho e segurança. Os usuários que desejam atualizar podem consultar a seção de atualização apropriada da "[Instalação do agente](#)" documentação. As versões anteriores do agente continuarão a funcionar sem a necessidade de ação do usuário.

Recursos de visualização

O Cloud Insights destaca regularmente uma série de novas funcionalidades de pré-visualização interessantes. Se você estiver interessado em visualizar um ou mais desses recursos, entre em Contato com o "[Equipe de](#)

[vendas da NetApp](#)" para obter mais informações.

Recurso	Descrição
Namespaces do Kubernetes estão ficando sem espaço	Os namespaces <i>Kubernetes em execução fora do espaço</i> Insight oferecem uma visão das cargas de trabalho nos namespaces do Kubernetes que correm o risco de ficar sem espaço, com uma estimativa do número de dias restantes antes que cada espaço fique cheio. " Leia mais "
Cloud Secure – bloqueie o acesso do usuário em caso de ataque	Maior proteção para dados essenciais aos negócios, com a capacidade de bloquear o acesso do usuário quando um ataque é detetado. O acesso pode ser bloqueado automaticamente, usando políticas de resposta automatizadas ou manualmente a partir das páginas de alerta ou detalhes do usuário. " Leia mais "
Recurso compartilhado sob estresse	O insight <i>Shared Resource sob estresse</i> usa IA/ML para identificar automaticamente onde a contenção de recursos está causando degradação do desempenho no seu ambiente, destaca quaisquer cargas de trabalho afetadas por ele e fornece ações recomendadas para correção, permitindo que você resolva problemas de desempenho com mais rapidez. " Leia mais "

Maio de 2022

Bate-papo ao vivo com o suporte da NetApp

Agora você pode conversar ao vivo com a equipe de suporte da NetApp! Na página Ajuda > suporte, basta clicar no ícone Chat ou clicar em *Chat* na seção "Fale Conosco" para iniciar uma sessão de chat. O suporte por bate-papo está disponível nos EUA durante a semana para usuários do Standard e Premium Edition.



Operador do Kubernetes

Facilitamos a colocação em funcionamento com o monitoramento avançado do Kubernetes e o explorador de clusters do Cloud Insights.

O "[Operador de monitoramento do Kubernetes](#)" (NKMO) é o método preferido para a instalação do Kubernetes para o Cloud Insights Insights, para uma configuração mais flexível de monitoramento em menos etapas, bem como oportunidades aprimoradas de monitoramento de outros softwares executados no cluster do K8s.

Clique no link acima para obter mais informações e pré-requisitos

Gerencie usuários e convites com API

Agora você pode gerenciar usuários e convites usando a poderosa API do Cloud Insights. Leia mais no ["API Swagger Documentação"](#).

Alertas de coleta de dados

Não perca as métricas críticas devido a um coletor falhado!

É mais fácil do que nunca acompanhar seus coletores de dados com novidades **"alertas"** para falhas de coletor de dados e unidade de aquisição. Observe que esses monitores são *Pausado* por padrão. Para ativar, navegue até a página monitores e localize e retome "Acquisition Unit Shutdown" (Desligamento da unidade de aquisição) e "Collector Failed" (Falha no coletor).

Alerta sobre alterações de armazenamento do ONTAP

Não deixe que mudanças inesperadas de armazenamento levem a interrupções!

Agora você pode configurar o Cloud Insights para alertar quando a modificação ou remoção de FlexVols, nós e SVMs forem detetadas em sistemas ONTAP.

Recursos de visualização

O Cloud Insights destaca regularmente uma série de novas funcionalidades de pré-visualização interessantes. Se você estiver interessado em visualizar um ou mais desses recursos, entre em Contato com o ["Equipe de vendas da NetApp"](#) para obter mais informações.

Recurso	Descrição
Namespaces do Kubernetes estão ficando sem espaço	Os namespaces <i>Kubernetes em execução fora do espaço</i> Insight oferecem uma visão das cargas de trabalho nos namespaces do Kubernetes que correm o risco de ficar sem espaço, com uma estimativa do número de dias restantes antes que cada espaço fique cheio. "Leia mais"
Previsão de tempo para o volume interno e a capacidade de volume para o total	O Cloud Insights é capaz de prever o número de dias até que a capacidade se esgote para cada volume interno e volume monitorado. Esse valor pode ajudar a reduzir significativamente o risco de uma interrupção.
Cloud Secure – bloqueie o acesso do usuário em caso de ataque	Maior proteção para dados essenciais aos negócios, com a capacidade de bloquear o acesso do usuário quando um ataque é detetado. O acesso pode ser bloqueado automaticamente, usando políticas de resposta automatizadas ou manualmente a partir das páginas de alerta ou detalhes do usuário. "Leia mais"

Recurso compartilhado sob estresse

O insight *Shared Resource sob estresse* usa IA/ML para identificar automaticamente onde a contenção de recursos está causando degradação do desempenho no seu ambiente, destaca quaisquer cargas de trabalho afetadas por ele e fornece ações recomendadas para correção, permitindo que você resolva problemas de desempenho com mais rapidez. ["Leia mais"](#)

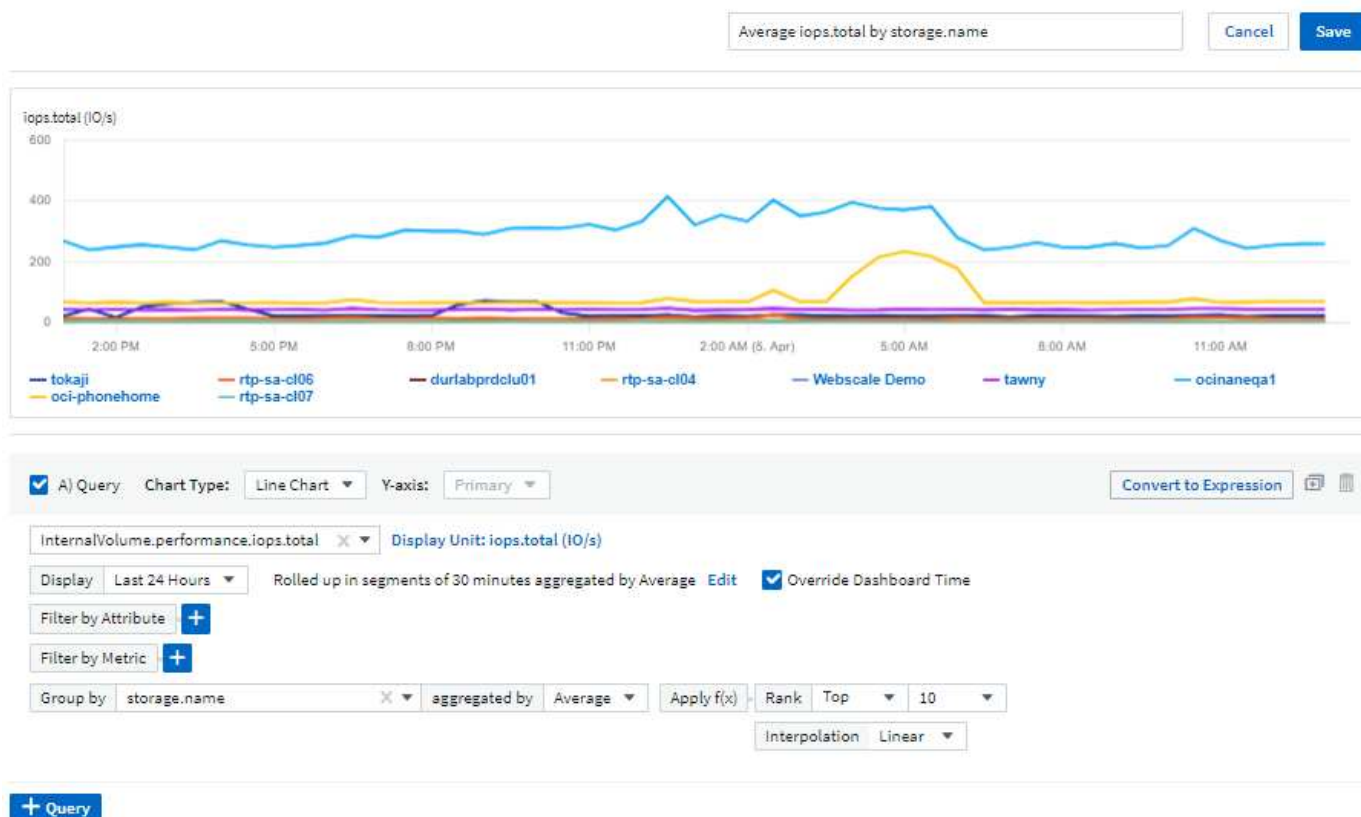
Abril de 2022

Compartilhe seu feedback!

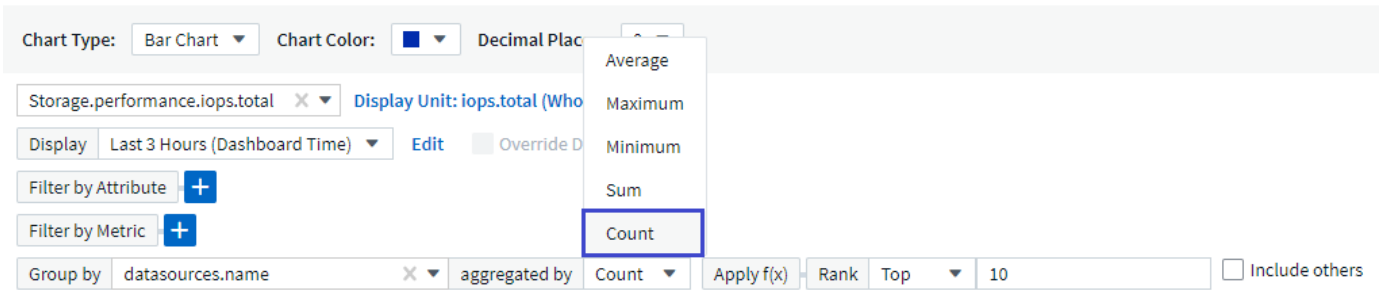
Queremos que a sua opinião ajude a moldar o Cloud Insights. Ganhe pontos e prêmios participando do programa **Insights to Action** da NetApp. ["Inscreva-se agora!"](#)

Editor de Dashboard atualizado

Revisamos nossas ferramentas de criação de dashboard para facilitar a visualização de seus dados ainda mais rapidamente. Navegue até a página "painéis" do Cloud Insights para editar um painel existente, adicionar um de nossa galeria de painel ou criar um novo painel para conferir.



Um novo método de agregação de contagem também foi introduzido. Ao agrupar dados em widgets de gráfico de barras, gráfico de colunas e gráfico de pizza, você pode exibir de forma rápida e fácil o número de objetos relevantes para a métrica selecionada.



Além disso, os gráficos de linha agora permitem que você selecione um dos três "interpolação" métodos:

- Nenhum - Nenhuma interpolação é feita
- Linear - interpola um ponto de dados entre os pontos existentes
- Stair - usa o ponto de dados anterior como o ponto de dados interpolado

Monitoramento aprimorado para sua infraestrutura Kubernetes

O Cloud Insights mantém você atualizado sobre as alterações no seu ambiente Kubernetes alertando-o quando pods, daemonsets e replicaset são criados ou removidos, bem como quando novas implantações são criadas. O Kubernetes monitora o padrão para o estado *pausado*, então você deve habilitar apenas os específicos de que precisa.

Recursos de visualização

O Cloud Insights destaca regularmente uma série de novas funcionalidades de pré-visualização interessantes. Se você estiver interessado em visualizar um ou mais desses recursos, entre em Contato com o ["Equipe de vendas da NetApp"](#) para obter mais informações.

Recurso	Descrição
Previsão de tempo para o volume interno e a capacidade de volume para o total	O Cloud Insights é capaz de prever o número de dias até que a capacidade se esgote para cada volume interno e volume monitorado. Esse valor pode ajudar a reduzir significativamente o risco de uma interrupção.
Cloud Secure – bloqueie o acesso do usuário em caso de ataque	Maior proteção para dados essenciais aos negócios, com a capacidade de bloquear o acesso do usuário quando um ataque é detectado. O acesso pode ser bloqueado automaticamente, usando políticas de resposta automatizadas ou manualmente a partir das páginas de alerta ou detalhes do usuário. "Leia mais"
Recurso compartilhado sob estresse	O recurso compartilhado sob insight sobre estresse usa IA/ML para identificar automaticamente onde a contenção de recursos está causando degradação do desempenho no seu ambiente, destaca quaisquer workloads afetados pela TI e fornece ações recomendadas para correção, permitindo que você resolva problemas de desempenho com mais rapidez. "Leia mais"

Novo coletor de dados

- **Cohesity SmartFiles** - este coletor baseado em API REST adquirirá um cluster Cohesity, descobrindo as "visualizações" (como volumes internos de IC), os vários nós, bem como coletando métricas de desempenho.

Outras atualizações do Data Collector

A coleta e a exibição de dados de desempenho foram melhoradas nos seguintes coletores de dados:

- CLI do Brocade
- Dell/EMC VPLEX, PowerStore, Isilon/PowerScale, VNX Block/CLARiiON CLI, XtremIO, Unity/VNXe
- Pure FlashArray

Esses aprimoramentos de desempenho já estão disponíveis em todos os coletores de dados do NetApp, bem como no VMware e no Cisco, e serão implementados para todos os outros coletores de dados nos próximos meses.




Março de 2022

Conexão com a nuvem para ONTAP 9.9 ou superior

O "[Conexão de nuvem NetApp para ONTAP 9.9 ou superior](#)" coletor de dados elimina a necessidade de instalar uma unidade de aquisição externa, simplificando assim a solução de problemas, manutenção e implantação inicial.

Novo FSX para monitores NetApp ONTAP

Monitorar seu ambiente do FSX for NetApp ONTAP é fácil, com novidades "[monitores definidos pelo sistema](#)" para infraestrutura (métricas) e cargas de trabalho (logs).

FSX Infrastructure (1)		+ Monitor	Bulk Actions ▾	Filter...	
<input type="checkbox"/>	Name	Metric / Parameters	Severity	Time Frame	Status
<input type="checkbox"/>	FSx Volume Cache Miss Ratio	netapp_ontap.workload_v olume.cache_miss_ratio	 Warning @ > 95 %  Critical @ > 100 %	For 30 minutes	 Paused

FSX Workload Examples (5)

[+ Monitor](#)

Bulk Actions ▾

Filter...

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

Novos recursos do Cloud Secure disponíveis para todos

Seu ambiente está mais seguro do que nunca com os seguintes recursos do Cloud Secure agora geralmente disponíveis:

Recurso	Descrição
Destruição de dados – detecção de ataque de exclusão de arquivos	Detecte atividades anormais de exclusão de arquivos em grande escala, bloqueie o acesso a arquivos maliciosos por usuários mal-intencionados e tire snapshots automáticos com políticas de resposta automáticas.
Notificações separadas para avisos e alertas	Notificações de aviso e alerta podem ser enviadas para destinatários separados, garantindo que a equipe certa possa se manter informada

Agente Telegraf atualizado

O agente para ingestão de dados de integração telegraf foi atualizado para a versão **1.21.2**, com melhorias de desempenho e segurança. Os usuários que desejam atualizar podem consultar a seção de atualização apropriada da "[Instalação do agente](#)" documentação. As versões anteriores do agente continuarão a funcionar sem a necessidade de ação do usuário.

Atualizações do Data Collector

- O coletor de dados dos switches Fibre Channel Broadcom foi otimizado para reduzir o número de comandos CLI emitidos com cada sondagem de inventário.

Fevereiro de 2022

O Cloud Insights resolve vulnerabilidades do Apache Log4j

A segurança do cliente é uma prioridade máxima na NetApp. O Cloud Insights inclui atualizações para suas bibliotecas de software para resolver as vulnerabilidades recentes do Apache Log4j.

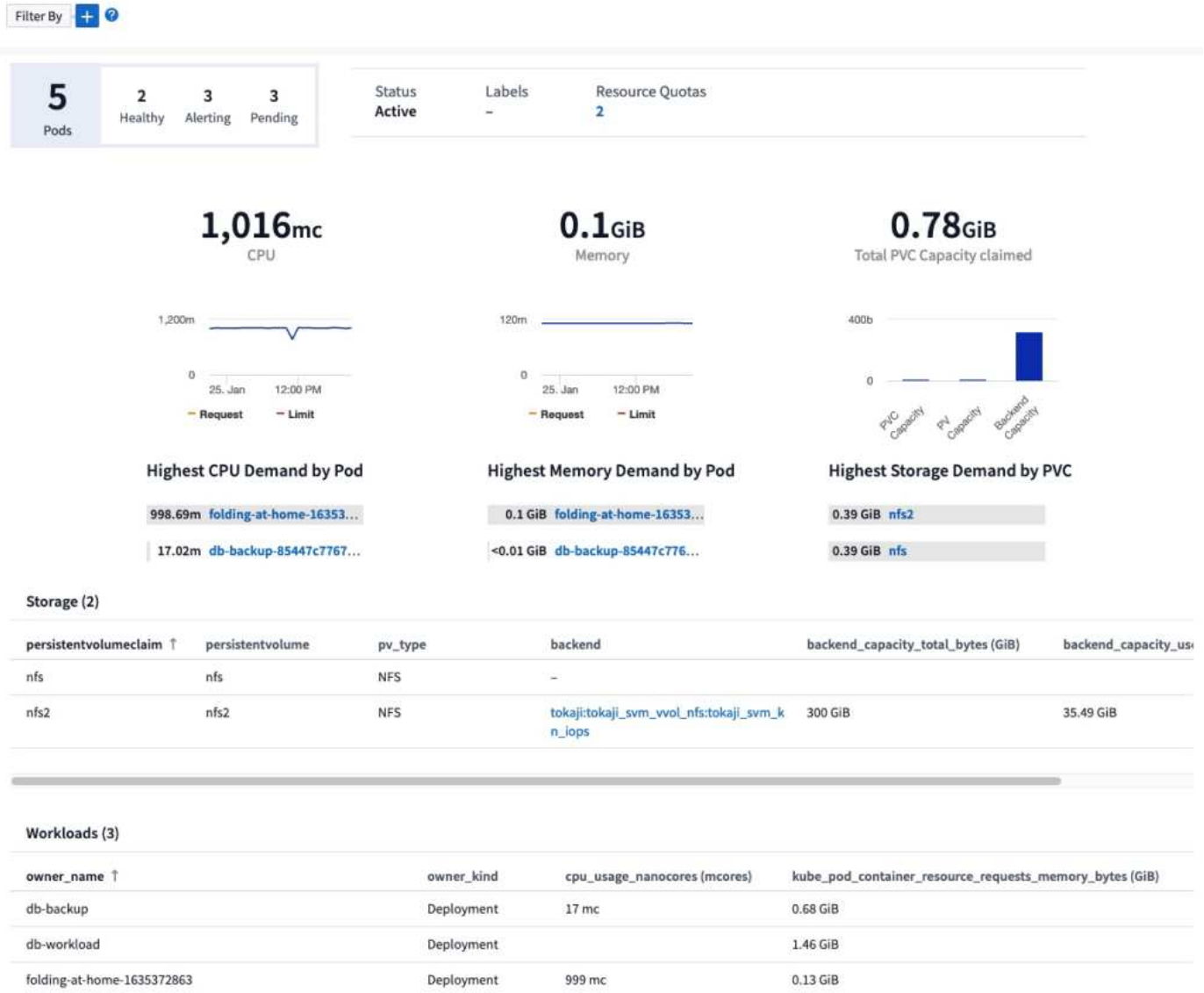
Consulte o seguinte no site do Aviso de Segurança de Produtos da NetApp:

["CVE-2021-44228"](#) ["CVE-2021-45046"](#) ["CVE-2021-45105"](#)

Você pode ler mais sobre essas vulnerabilidades e a resposta do NetApp no ["Sala de imprensa da NetApp"](#).

Página de detalhes do namespace do Kubernetes

Explorar seu ambiente Kubernetes agora está melhor do que nunca, com páginas de detalhes informativos para os namespaces do seu cluster. A página de detalhes do namespace fornece um resumo de todos os ativos usados por um namespace, incluindo todos os recursos de storage no back-end e suas utilizações de capacidade.



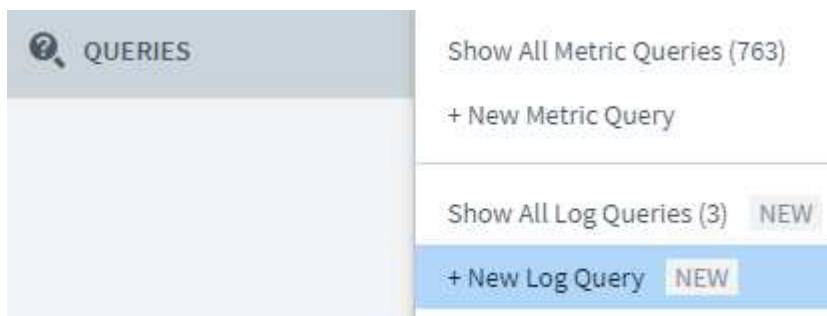
Dezembro de 2021

Integração mais profunda para sistemas ONTAP

Simplifique os alertas para falhas de hardware da ONTAP e muito mais com a nova integração com o sistema de gerenciamento de eventos (EMS) da NetApp. ["Explorar e alertar"](#) Em mensagens ONTAP de baixo nível no Cloud Insights para informar e melhorar fluxos de trabalho de solução de problemas e reduzir ainda mais a dependência das ferramentas de gerenciamento do ONTAP Element.

A consultar registros

Para sistemas ONTAP, as consultas do Cloud Insights incluem um poderoso ["Explorador de registros"](#), permitindo que você investigue e solucione facilmente as entradas de log do EMS.



Notificações de nível de coletor de dados.

Além de monitores criados por sistema e personalizados para alertas, você também pode definir notificações de alerta para coletores de dados do ONTAP, permitindo especificar destinatários para alertas em nível de coletor, independentemente de outros alertas de monitor.

Maior flexibilidade das funções do Cloud Secure

Os usuários podem ter acesso a recursos do Cloud Secure com base em ["funções"](#) definido por um administrador:

Função	Acesso à Cloud Secure
Administrador	Pode executar todas as funções do Cloud Secure, incluindo as de Alertas, forenses, coletores de dados, políticas de resposta automatizadas e APIs para Cloud Secure. Um administrador também pode convidar outros usuários, mas só pode atribuir funções do Cloud Secure.
Utilizador	Pode visualizar e gerir Alertas e visualizar Forensics. A função de usuário pode alterar o status de alerta, adicionar uma nota, tirar snapshots manualmente e bloquear o acesso do usuário.
Convidado	Pode visualizar Alertas e Forensics. A função convidado não pode alterar o status de alerta, adicionar uma nota, tirar snapshots manualmente ou bloquear o acesso do usuário.

Suporte ao sistema operacional

O suporte ao CentOS 8.x está sendo substituído pelo suporte ao **CentOS 8 Stream**. O CentOS 8.x chegará ao fim da vida útil em 31 de dezembro de 2021.

Atualizações do Data Collector

Foram adicionados vários nomes de coletores de dados do Cloud Insights para refletir as alterações de fornecedor:

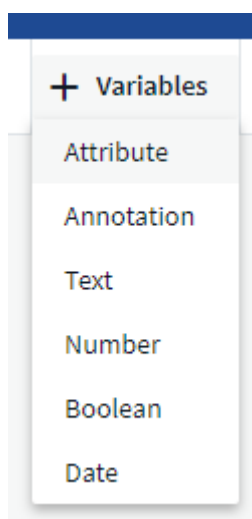
Fornecedor/modelo	Nome anterior
Dell EMC PowerScale	Isilon
HPE Alletra 9000 / Primera	3PAR
HPE Alletra 6000	Ágil

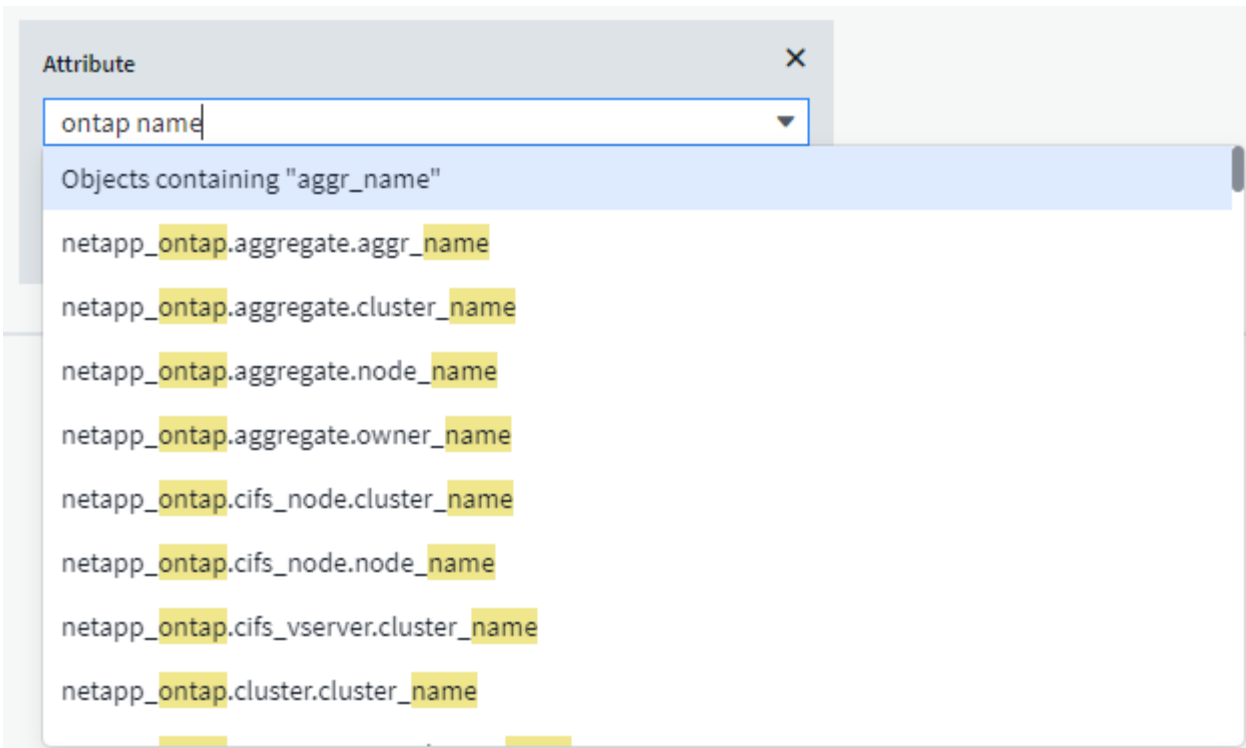
Novembro de 2021

Painéis adaptativos

Novas variáveis para atributos e a capacidade de usar variáveis em widgets.

Os dashboards agora são mais poderosos e flexíveis do que nunca. Crie painéis adaptativos com variáveis de atributo para filtrar rapidamente painéis. Usando esses e outros pré-existentes "variáveis", você agora pode criar um painel de alto nível para ver as métricas de todo o seu ambiente e filtrar facilmente pelo nome do recurso, tipo, localização e muito mais. Use variáveis de número em widgets para associar métricas brutas a custos, por exemplo, custo por GB para armazenamento como serviço.





Acesse o banco de dados de relatórios via API

Recursos aprimorados para integração com ferramentas de relatórios, ITSM e automação de terceiros: O poderoso do Cloud Insights "API" permite que os usuários consultem o banco de dados de relatórios Cloud Insights diretamente, sem passar pelo ambiente de relatórios Cognos.

Tabelas POD na página de destino da VM

Navegação otimizada entre as VMs e os pods do Kubernetes usando-os: Para melhorar a solução de problemas e o gerenciamento do espaço livre de performance, uma tabela de pods do Kubernetes associados agora aparecerá nas páginas iniciais da VM.

Kubernetes Pods 5m

15 items found

pod_name ↑	kubernetes_cluster	namespace	owner_kind	owner_name
calico-kube-controllers-649b7b795b-ktp2n	ci-rancher	kube-system	ReplicaSet	calico-kube-controllers-649b7b795b
canal-mpvhx	ci-rancher	kube-system	DaemonSet	canal
cattle-cluster-agent-74c7797cc5-b9jhz	ci-rancher	cattle-system	ReplicaSet	cattle-cluster-agent-74c7797cc5
cattle-node-agent-bn225	ci-rancher	cattle-system	DaemonSet	cattle-node-agent
coredns-autoscaler-79599b9dc6-dtwpj	ci-rancher	kube-system	ReplicaSet	coredns-autoscaler-79599b9dc6

Atualizações do Data Collector

- O ECS agora relata firmware para armazenamento e nó
- Isilon melhorou a detecção de prompt
- O Azure NetApp Files coleta dados de performance mais rapidamente
- O StorageGRID agora oferece suporte ao logon único (SSO)
- A CLI do Brocade relata adequadamente o modelo para X&-4

Sistemas operacionais adicionais suportados

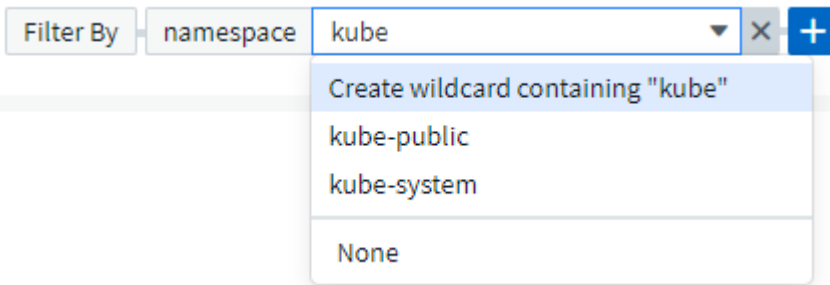
A Unidade de aquisição Cloud Insights suporta os seguintes sistemas operativos, além dos já suportados:

- CentOS (64 bits) 8,4
- Oracle Enterprise Linux (64 bits) 8,4
- Red Hat Enterprise Linux (64 bits) 8,4

Outubro de 2021

Filtros em K8S páginas Explorer

"Explorador do Kubernetes" Os filtros de página oferecem controle focado dos dados exibidos para a exploração do cluster, nó e pod do Kubernetes.



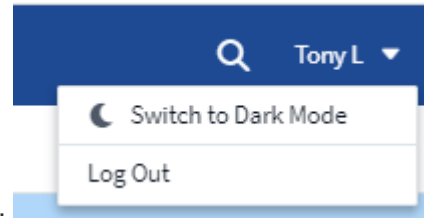
K8s dados para relatórios

Os dados do Kubernetes agora estão disponíveis para uso nos relatórios, permitindo que você crie chargeback ou outros relatórios. Para que os dados de chargeback do Kubernetes sejam passados para relatórios, você precisa ter uma conexão ativa com o Cloud Insights e o cluster de back-end. Se não houver dados recebidos do storage de back-end, o Cloud Insights não poderá enviar dados de objeto do Kubernetes para o relatório.

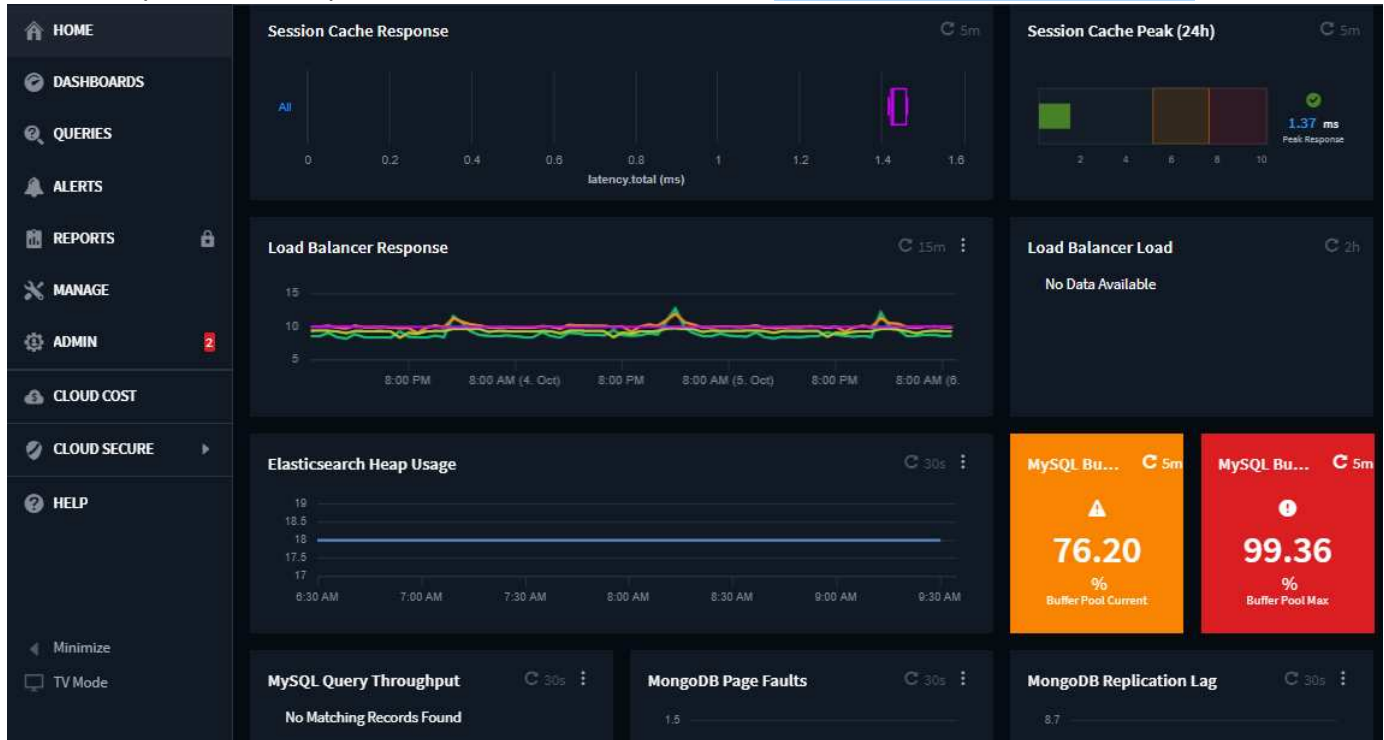


Dark Theme chegou

Muitos de vocês pediram um tema escuro, e Cloud Insights respondeu. Para alternar entre tema claro e



escuro, clique na lista suspensa ao lado do nome de usuário.



Suporte ao Data Collector

Fizemos algumas melhorias nos coletores de dados do Cloud Insights. Aqui estão alguns destaques:

- Novo coletor para o Amazon FSX for ONTAP

Setembro de 2021

As políticas de desempenho agora são monitores

Monitores e Alertas suplantaram políticas de desempenho e violações em todo o Cloud Insights. ["Alertas com monitores"](#) fornece maior flexibilidade e insights sobre possíveis problemas ou tendências em seu ambiente.

AutoComplete sugestões, curingas e expressões em monitores

Ao criar um monitor para alertas, digitar um filtro agora é preditivo, permitindo que você pesquise e encontre facilmente as métricas ou atributos do seu monitor. Além disso, você tem a opção de criar um filtro curinga com base no texto digitado.

1 Select a metric to monitor

StoragePool.performance.utilization.read

Filter By name sas1

Group Avg

Unit Displayed In

Create wildcard containing "sas1"

tawny03:tawny03sas1

tawny04:tawny04sas1

None

Agente Telegraf atualizado

O agente para ingestão de dados de integração telegraf foi atualizado para a versão **1.19.3**, com melhorias de desempenho e segurança. Os usuários que desejam atualizar podem consultar a seção de atualização apropriada da "[Instalação do agente](#)" documentação. As versões anteriores do agente continuarão a funcionar sem a necessidade de ação do usuário.

Suporte ao Data Collector

Fizemos algumas melhorias nos coletores de dados do Cloud Insights. Aqui estão alguns destaques:

- O coletor do Microsoft Hyper-V agora usa o PowerShell em vez do WMI
- As VMs do Azure e o coletor VHD agora são até 10 vezes mais rápidos devido a chamadas paralelas
- O HPE Nimble agora oferece suporte a configurações federadas e iSCSI

E como estamos sempre melhorando a coleta de dados, aqui estão algumas outras mudanças recentes de nota:

- Novo coletor para EMC Powerstore
- Novo coletor para Hitachi Ops Center
- Novo coletor para a plataforma de conteúdo Hitachi
- Coletor ONTAP aprimorado para relatar pools de malha
- ANF aprimorado com pool de storage e performance de volume
- EMC ECS aprimorado com nós de armazenamento e desempenho de armazenamento, bem como a contagem de objetos em buckets
- EMC Isilon aprimorado com métricas de nó de storage e Qtree
- EMC Symetrix aprimorado com métricas de limite de QOS de VOLUME
- IBM SVC e EMC PowerStore aprimorados com o número de série pai dos nós de storage

Agosto de 2021

Nova Interface de Usuário da Página de Auditoria

O "[Página de auditoria](#)" fornece uma interface mais limpa e agora permite a exportação de eventos de auditoria para arquivo .CSV.

Gerenciamento aprimorado de funções do usuário

O Cloud Insights agora permite ainda maior liberdade para atribuir funções de usuário e controles de acesso. Agora, os usuários podem receber permissões granulares para monitoramento, geração de relatórios e Cloud Secure separadamente.

Isso significa que você pode permitir que mais usuários tenham acesso administrativo a funções de monitoramento, otimização e relatórios, ao mesmo tempo em que restringe o acesso a seus dados confidenciais de auditoria e atividade do Cloud Secure apenas àqueles que precisam dele.

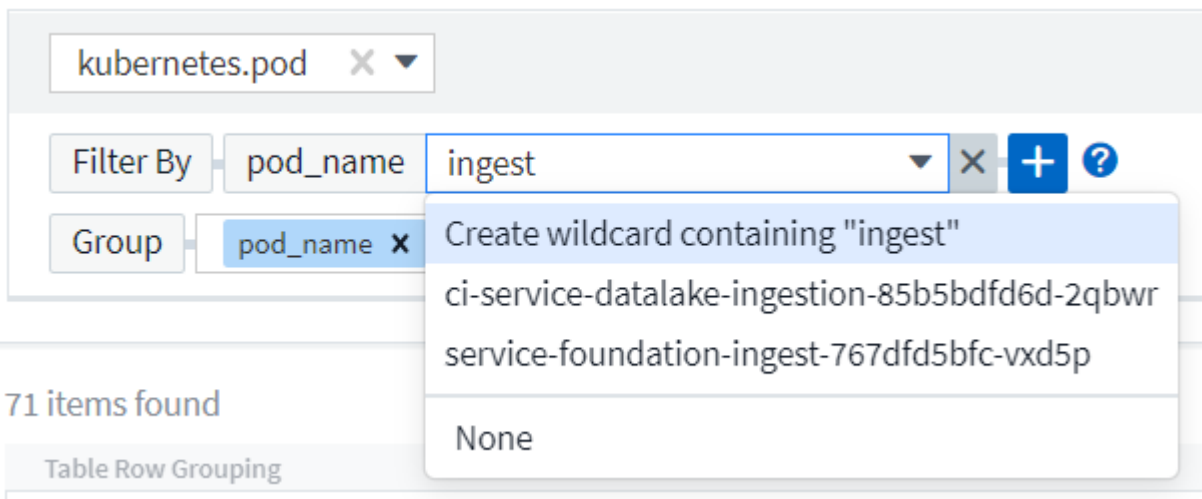
["Saiba mais"](#) Sobre os diferentes níveis de acesso na documentação do Cloud Insights.

Junho de 2021

Complete sugestões, curingas e expressões automaticamente em filtros

Com esta versão do Cloud Insights, você não precisa mais saber todos os nomes e valores possíveis nos quais filtrar em uma consulta ou widget. Ao filtrar, você pode simplesmente começar a digitar e o Cloud Insights irá sugerir valores com base no seu texto. Não é mais procurar nomes de aplicativos ou atributos do Kubernetes antes do tempo apenas para encontrar os que você deseja mostrar no seu widget.

À medida que você digita um filtro, o filtro exibe uma lista inteligente de resultados dos quais você pode escolher, bem como a opção de criar um filtro * curinga* com base no texto atual. Selecionar esta opção irá retornar todos os resultados que correspondem à expressão curinga. É claro que você também pode selecionar vários valores individuais que você deseja adicionar ao filtro.



Além disso, você pode criar **expressões** em um filtro usando NOT OU OU, ou você pode selecionar a opção "nenhum" para filtrar valores nulos no campo.

Leia mais sobre ["opções de filtragem"](#) em consultas e widgets.

APIs disponíveis por Edição

As poderosas APIs da Cloud Insights estão mais acessíveis do que nunca, com as APIs de alertas agora disponíveis nas edições Standard e Premium. As seguintes APIs estão disponíveis para cada edição:

Categoria da API	Básico	Padrão	Premium
Unidade de aquisição	✓	✓	✓
Coleta de dados	✓	✓	✓
Alertas		✓	✓
Ativos		✓	✓
Ingestão de dados		✓	✓

Visibilidade do fotovoltaico e do Pod do Kubernetes

O Cloud Insights oferece visibilidade do storage de back-end para seus ambientes Kubernetes com insights sobre pods do Kubernetes e volumes persistentes (PVS). Agora você pode rastrear contadores PV, como IOPS, latência e taxa de transferência, desde o uso de um único Pod por meio de um contador PV até um PV e até o dispositivo de armazenamento back-end.

Em uma página inicial volume ou volume interno, duas novas tabelas são exibidas:

Kubernetes PVs

2 items found

PV ↑	Cluster	PV Capacity (GiB)	Phase	StorageClass
cvo-shared-storage-pv	QA_K8S_CLUSTER	0.73	Bound	
test-mysql-shared-storage-pv	QA_K8S_CLUSTER	7.32	Bound	

Kubernetes Pods

2 items found

Pod ↑	Cluster	Namespace	PV	Workload Type	Workload	Latency - Total ...	IOPS - T
cvo-mypod-pvc	QA_K8S_CLUSTER	k8testns	cvo-shared-storage				0.00
test-mysql-0	QA_K8S_CLUSTER	k8testns	test-mysql-shared-	StatefulSet	test-mysql	0.19	2.72

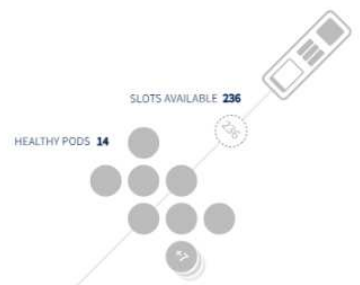
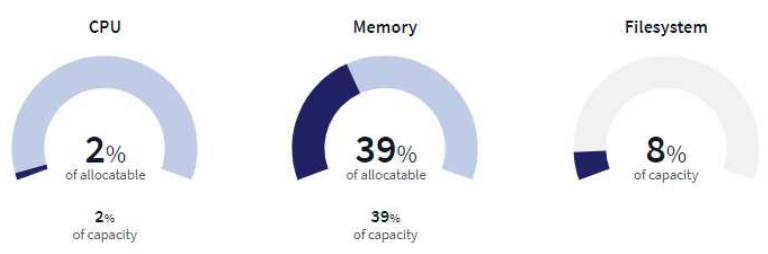
Observe que para aproveitar essas novas tabelas, é recomendável desinstalar o agente do Kubernetes atual e instalá-lo novamente. Você também deve instalar o Kube-State-Metrics versão 2.1.0 ou posterior.

Nó do Kubernetes para links da VM

Em uma página do nó Kubernetes, agora você pode clicar para abrir a página da VM do nó. A página da VM também inclui um link de volta para o próprio nó.

14 Pods
 14 Healthy 0 Alerting

Labels - Node IP 10.30.27.178 Virtual Machine **main-ci-node-general-1b-05** ←



Status ↑	Name	Healthy Containers	Namespace
Healthy	Running ci-service-assets-bcb7447c-lsk29	1 of 1	oci
Healthy	Running ci-service-webui-rest-74b89f5d8-nvlog	1 of 1	oci
Healthy	Running filebeat-gg7r7	1 of 1	kube-system
Healthy	Running ovs-vbjzd	1 of 1	openshift-sdn

NetApp / main-ci-node-general-1b-05

Virtual Machine Summary 5m

<p>Power State: On</p> <p>Guest State: Running</p> <p>Datastore: i-01b052b8d843994e7</p> <p>CPU Utilization - Total: 3.89 %</p> <p>Memory Utilization - Total: N/A</p> <p>Memory: 32.0 GB</p> <p>Capacity - Total: 200.0 GB</p> <p>Capacity - Used: N/A</p>	<p>Latency - Total: 1.21 ms</p> <p>IOPS - Total: 11.06 IO/s</p> <p>Throughput - Total: 0.06 MB/s</p> <p>DNS Name: ip-10-178.ec2.internal</p> <p>IP:</p> <p>OS: CentOS Linux 7 x86_64 HVM EBS ENA 1901_01-</p> <p>Processors: 8</p> <p>Hypervisor Name: us-east-1b</p>	<p>Hypervisor IP: US-EAST-1B</p> <p>Hypervisor OS: Amazon AWS EC2</p> <p>Hypervisor FC Fabrics: 0</p> <p>Hypervisor CPU Utilization: N/A</p> <p>Hypervisor Memory Utilization: N/A</p> <p>Kubernetes Node: ip-10-30-27-178.ec2.internal ←</p> <p>Alert Monitors: VM Capacity VM IOPS</p> <p>View Topology</p>
---	---	--

Os monitores de alerta que substituem as políticas de desempenho

Para habilitar os benefícios adicionais de vários limiares, webhook e entrega de alertas por e-mail, alertando sobre todas as métricas usando uma única interface e muito mais, a Cloud Insights converterá clientes da Edição Standard e Premium de **políticas de desempenho** para **monitores** durante os meses de julho e agosto de 2021. Saiba mais sobre "[Alertas e monitores](#)" e fique atento a essa mudança emocionante.

Cloud Secure é compatível com NFS

O Cloud Secure agora oferece suporte à coleta de dados NFS para ONTAP. Monitore o acesso de usuários SMB e NFS para proteger seus dados contra ataques de ransomware. Além disso, o Cloud Secure oferece suporte a diretórios de usuários do Active Directory e LDAP para coleta de atributos de usuário NFS.

Purga de snapshot do Cloud Secure

O Cloud Secure exclui automaticamente instantâneos com base nas Configurações de exclusão de instantâneos, para economizar espaço de armazenamento e reduzir a necessidade de exclusão manual de instantâneos.

Snapshot Purge Settings

Define purge periods to automatically delete snapshots taken by Cloud Secure.

Attack Automated Response

Delete Snapshot after

Warning Automated Response

Delete Snapshot after

User Created

Delete Snapshot after

Velocidade de coleta de dados Cloud Secure

Um único sistema de agente coletor de dados agora pode postar até 20.000 eventos por segundo no Cloud Secure.

Maio de 2021

Aqui estão algumas das mudanças que fizemos em abril:

Agente Telegraf atualizado

O agente para ingestão de dados de integração telegraf foi atualizado para a versão 1.17.3, com melhorias de desempenho e segurança. Os usuários que desejam atualizar podem consultar a seção de atualização

apropriada da "[Instalação do agente](#)" documentação. As versões anteriores do agente continuarão a funcionar sem a necessidade de ação do usuário.

Adicione ações corretivas a um alerta

Agora você pode adicionar uma descrição opcional, bem como informações adicionais e/ou ações corretivas ao criar ou modificar um Monitor preenchendo a seção **Adicionar uma Descrição de alerta**. A descrição será enviada com o alerta. O campo *insights e ações corretivas* pode fornecer etapas detalhadas e orientações para lidar com alertas e será exibido na seção de resumo da página de destino do alerta.

4 Add an alert description (optional)

Add a description

Add insights and corrective actions

APIs do Cloud Insights para todas as edições

O acesso à API está agora disponível em todas as edições do Cloud Insights. Os usuários da edição básica agora podem automatizar ações para unidades de aquisição e coletores de dados, e os usuários do Standard Edition podem consultar métricas e ingerir métricas personalizadas. A edição Premium continua a permitir o uso total de todas as categorias de API.

Categoria da API	Básico	Padrão	Premium
Unidade de aquisição	✓	✓	✓
Coleta de dados	✓	✓	✓
Ativos		✓	✓
Ingestão de dados		✓	✓
Armazém de dados			✓

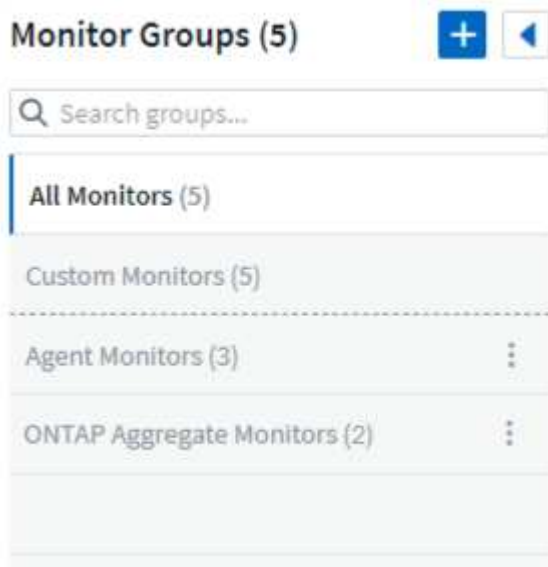
Para obter detalhes sobre o uso da API, consulte o "[Documentação do API](#)".

Abril de 2021

Gerenciamento mais fácil de monitores

"Agrupamento de monitores" simplifica o gerenciamento de monitores em seu ambiente. Vários monitores podem agora ser agrupados e pausados como um. Por exemplo, se você tiver uma atualização ocorrendo em uma pilha de infraestrutura, poderá pausar alertas de todos esses dispositivos com um clique.

Os grupos de monitores são a primeira parte de um novo recurso emocionante que traz o gerenciamento aprimorado de dispositivos ONTAP para o Cloud Insights.



Opções de alertas aprimoradas usando webhooks

Muitos aplicativos comerciais suportam "Webhooks" como uma interface de entrada padrão. O Cloud Insights agora suporta muitos desses canais de entrega, fornecendo modelos padrão para Slack, PagerDuty, Teams e discord, além de fornecer webhooks genéricos personalizáveis para suportar muitos outros aplicativos.

3 Set up team notification(s) (alert your team via email, or Webhook)

By Webhook	Notify team on Critical, Warning	Use Webhook(s) PagerDuty Trigger
	Notify team on Resolved	Use Webhook(s) PagerDuty Resolve

Identificação melhorada do dispositivo

Para melhorar o monitoramento e a solução de problemas, bem como fornecer relatórios precisos, é útil entender os nomes dos dispositivos em vez de seus endereços IP ou outros identificadores. O Cloud Insights agora incorpora uma maneira automática de identificar os nomes dos dispositivos de armazenamento e host físicos no ambiente, usando uma abordagem baseada em regras chamada "Resolução do dispositivo", disponível no menu **Gerenciar**.

Você pediu mais!

Um pedido popular dos clientes tem sido por mais opções padrão para visualizar o intervalo de dados, então adicionamos as cinco novas opções a seguir que estão agora disponíveis em todo o serviço através do seletor de intervalo de tempo:

- Durar 30 minutos
- Últimas 2 horas
- Últimas 6 horas
- Últimas 12 horas
- Últimos 2 dias

Várias assinaturas em um ambiente da Cloud Insights

A partir de abril de 2, o Cloud Insights oferece suporte a várias assinaturas do mesmo tipo de edição para um cliente em uma única instância do Cloud Insights. Isso permite que os clientes alterem partes da subscrição do Cloud Insights com compras de infraestrutura. Contacte as vendas da NetApp para obter assistência com várias subscrições.

Escolha o seu caminho

Ao configurar o Cloud Insights, agora você pode escolher se deseja começar com o Monitoramento e Alerta ou ransomware e detecção de ameaças internas. O Cloud Insights configurará seu ambiente inicial com base no caminho que você escolher. Você pode configurar o outro caminho a qualquer momento depois.

Integração Cloud Secure mais fácil

E é mais fácil do que nunca começar a usar o Cloud Secure, com uma nova lista de verificação de configuração passo a passo.



Secure Your Data from Ransomware & Insider Threat

- Ransomware & insider threat detection
- User data access auditing

Setting up Cloud Secure

- ✓ Add an [Agent](#) on server or VM to collect data ([system requirements](#) [↗](#)).
- ✓ Configure a [User Directory Collector](#) to collect user attributes from active directories (optional step).
- ✓ Configure a [Data Collector](#) to collect file access activity on your storage devices.
- ✓ Define [Automated Response Policies](#) to take automatic action in the event of an attack.

User activity data will appear in the [Forensics](#) section

Como sempre, adoramos ouvir suas sugestões! Envie-os para [ng-cloudinsights-customerfeedback](mailto:ng-cloudinsights-customerfeedback@netapp.com) em [NetApp.com](mailto:ng-cloudinsights-customerfeedback@netapp.com).

Fevereiro de 2021

Agente Telegraf atualizado

O agente para ingestão de dados de integração do telegraf foi atualizado para a versão 1.17.0, que inclui correções de vulnerabilidades e bugs.

Cloud Cost Analyzer

Aproveite o poder do Spot da NetApp com o Cloud Cost, que fornece uma análise de custos detalhada dos gastos passados, presentes e estimados, proporcionando visibilidade sobre a utilização da nuvem em seu ambiente. O dashboard do Cloud Cost oferece uma visão clara das despesas de nuvem e uma análise detalhada de workloads, contas e serviços individuais.

Os custos da nuvem podem ajudar a superar esses grandes desafios:

- Acompanhamento e monitoramento de suas despesas de nuvem
- Identificação de resíduos e potenciais áreas de otimização
- Entrega de itens de ação executáveis

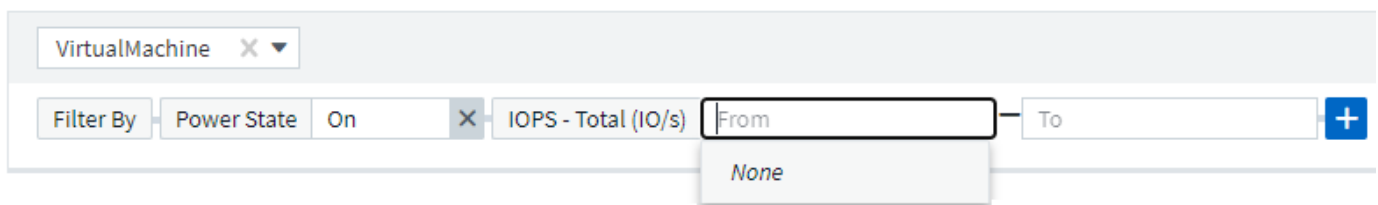
O foco dos custos da nuvem é o monitoramento. Atualize para a conta completa do Spot by NetApp para habilitar a economia automática de custos e a otimização do ambiente.

Consulta de objetos com valores nulos usando filtros

O Cloud Insights agora permite pesquisar atributos e métricas com valores nulos/nulos por meio do uso de filtros. Você pode executar essa filtragem em quaisquer atributos/métricas nos seguintes locais:

- Na página consulta
- Em widgets do Dashboard e variáveis de página
- Na página da lista Alertas
- Ao criar monitores

Para filtrar os valores null/none, basta selecionar a opção *None* quando aparecer no menu suspenso apropriado do filtro.



Suporte a várias regiões

A partir de hoje, oferecemos o serviço Cloud Insights em diferentes regiões do mundo, o que facilita o desempenho e aumenta a segurança para clientes de fora dos Estados Unidos. O Cloud Insights/Cloud Secure armazena informações de acordo com a região em que seu ambiente é criado.

Clique "[aqui](#)" para obter mais informações.

Janeiro de 2021

Métricas ONTAP adicionais renomeadas

Como parte de nosso esforço contínuo para melhorar a eficiência da coleta de dados de sistemas ONTAP, as seguintes métricas do ONTAP foram renomeadas.

Se você tiver widgets de painel ou consultas existentes usando qualquer uma dessas métricas, precisará editá-las ou recriá-las para usar os novos nomes de métricas.

Nome da métrica anterior	Novo Nome métrico
NetApp_ONTAP.disk_constituinte.total_transfers	NetApp_ONTAP.disk_constituinte.total_iops
NetApp_ONTAP.disk.total_transfers	NetApp_ONTAP.disk.total_iops
NetApp_ONTAP.fcp_lif.read_data	NetApp_ONTAP.fcp_lif.read_throughput
NetApp_ONTAP.fcp_lif.write_data	NetApp_ONTAP.fcp_lif.write_throughput

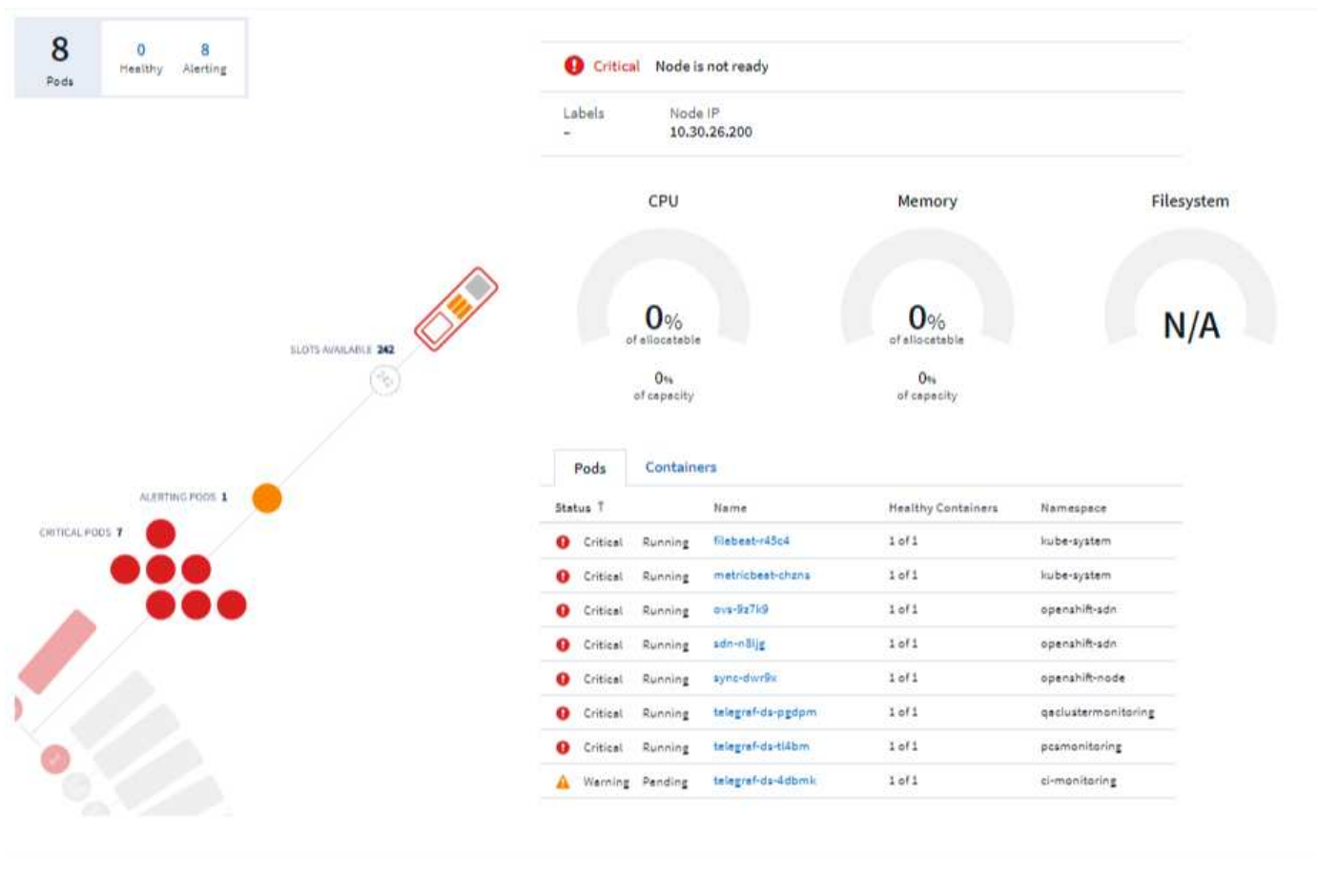
Nome da métrica anterior	Novo Nome métrico
NetApp_ONTAP.iscsi_lif.read_data	NetApp_ONTAP.iscsi_lif.read_throughput
NetApp_ONTAP.iscsi_lif.write_data	NetApp_ONTAP.iscsi_lif.write_throughput
NetApp_ONTAP.lif.recv_data	NetApp_ONTAP.lif.recv_throughput
NetApp_ONTAP.lif.sent_data	NetApp_ONTAP.lif.sent_throughput
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_writ e
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_writ e
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_writ e
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

Nome da métrica anterior	Novo Nome métrico
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

Novo Kubernetes Explorer

O "Explorador do Kubernetes" oferece uma visualização simples da topologia dos clusters do Kubernetes, permitindo que até mesmo não especialistas identifiquem problemas e dependências rapidamente, do nível do cluster até o contêiner e o storage.

Uma ampla variedade de informações pode ser explorada usando os detalhes de pesquisa detalhada do Kubernetes Explorer para status, uso e integridade dos clusters, nós, pods, contêineres e storage em seu ambiente Kubernetes.



Dezembro de 2020

Instalação mais simples do Kubernetes

A instalação do Kubernetes Agent foi simplificada para exigir menos interações com o usuário. "[Instalando o Kubernetes Agent](#)" Agora inclui a coleta de dados do Kubernetes.

Novembro de 2020

Painéis adicionais

Os seguintes novos painéis focados no ONTAP foram adicionados à galeria e estão disponíveis para importação:

- ONTAP: Desempenho e capacidade agregados
- ONTAP FAS/AFF - utilização da capacidade
- ONTAP FAS/AFF - capacidade do cluster
- ONTAP FAS/AFF - eficiência
- ONTAP FAS/AFF - desempenho do FlexVol
- ONTAP FAS/AFF - pontos operacionais/ideais do nó
- ONTAP FAS/AFF: Eficiência de capacidade pré-posta
- ONTAP: Atividade de porta de rede
- ONTAP: Performance de protocolos de nó
- ONTAP: Performance de workload de nós (front-end)
- ONTAP: Processador
- ONTAP: Performance de workload com SVM (front-end)
- ONTAP: Desempenho de workloads de volume (front-end)

Renomear coluna em Widgets de Tabela

Você pode renomear colunas na seção *métricas e atributos* de um widget de tabela abrindo o widget no modo Editar e clicando no menu na parte superior da coluna. Digite o novo nome e clique em *Save* ou clique em *Reset* para definir a coluna de volta para o nome original.

Observe que isso afeta apenas o nome de exibição da coluna no widget de tabela; o nome de métrica/atributo não muda nos próprios dados subjacentes.

Metrics & Attributes	
Metric Name	
qa-ots-cl01	<input type="checkbox"/> Rename Column Reset <input type="text" value="Metric Name"/>
ngslabc90	
kuat	
hkdemo-cluster	

Outubro de 2020

Expansão padrão dos dados de integração

O agrupamento de widgets de tabela agora permite expansões padrão das métricas Kubernetes, dados avançados do ONTAP e nó de agente. Por exemplo, se você agrupar *nodes* do Kubernetes por *Cluster*, verá uma linha na tabela para cada cluster. Em seguida, você pode expandir cada linha de cluster para ver uma lista dos objetos nó.

Suporte Técnico Basic Edition

O suporte técnico está agora disponível para assinantes do Cloud Insights Basic Edition, além das edições Standard e Premium. Além disso, o Cloud Insights simplificou o fluxo de trabalho para criar um ticket de suporte do NetApp.

API pública do Cloud Secure

O Cloud Secure oferece suporte "[APIS REST](#)" para acessar informações de atividade e alerta. Isso é feito por meio do uso de tokens de acesso à API, criados por meio da IU do administrador do Cloud Secure, que são usados para acessar as APIs REST. A documentação do Swagger para essas APIs REST é integrada ao Cloud Secure.

Setembro de 2020

Página de consulta com dados de integração

A página de consulta do Cloud Insights é compatível com dados de integração (ou seja, do Kubernetes, métricas avançadas do ONTAP, etc.). Ao trabalhar com dados de integração, a tabela de resultados da consulta exibe uma exibição "tela dividida", com objeto/agrupamento no lado esquerdo e dados de objeto (atributos/métricas) à direita. Você também pode escolher vários atributos para agrupar dados de integração.

agent.node_fs X

Filter By +

Group agent_node_name X agent_node_os X

3 Items found

Table Row Grouping		Metrics & Attributes	
agent_node_name	agent_node_os	free	inodes_used
WIN2K12R2IMAGE	Microsoft Windows	70,594,338,816.00	0.00
WIN2K19IMAGE	Microsoft Windows	72,546,041,856.00	0.00
ci-qa-chunge-qaau	Red Hat Enterprise Linux Server	169,010,801,322.67	21,844.00

Formatação de exibição de unidade no widget de tabela

A formatação de exibição de unidade agora está disponível em widgets de tabela para colunas que exibem dados de métrica/contador (por exemplo, gigabytes, MB/segundo, etc.). Para alterar a unidade de visualização de uma métrica, clique no menu "três pontos" no cabeçalho da coluna e selecione "Exibição da unidade". Você pode escolher entre qualquer uma das unidades disponíveis. As unidades disponíveis variam de acordo com o tipo de dados métricos na coluna de visualização.

Table Widget

Override Dashboard Time Last 3 Hours X

agent.node X

Filter By + Group agent_node_name X

8 items found

Table Row Grouping		Metrics & Attributes	
agent_node_name ↑		mem.used (GiB)	
ci-qa-avinashp-k8-bakra-1		12.41	
ci-qa-avinashp-k8-bakra-2		9.31	
ci-qa-avinashp-k8-bakra-3		4.46	
ci-qa-avinashp-k8-bakra-4		1.15	
ci-qa-avinashp-k8swheel-1		15.23	

> Aggregation

▼ Unit Display

Base Unit

Displayed In

Cancel Save

Página Detalhe Unidade aquisição

As unidades de aquisição agora têm sua própria página de destino, fornecendo detalhes úteis para cada AU, bem como informações para ajudar na solução de problemas. O "[Página de detalhes AU](#)" fornece ligações aos coletores de dados da UA, bem como informações úteis sobre o estado.

Dependência do Docker do Cloud Secure removida

A dependência do Cloud Secure no Docker foi removida. O Docker não é mais necessário para a instalação do agente do Cloud Secure.

Funções de utilizador de relatórios

Se você tiver o Cloud Insights Premium Edition com relatórios, todos os usuários do Cloud Insights em seu ambiente também terão um login único (SSO) no aplicativo de relatórios (ou seja, Cognos); clicando no link **relatórios** no menu, eles serão automaticamente conectados ao Relatório.

Sua função de usuário no Cloud Insights determina "Função de usuário de relatório" seu :

Função Cloud Insights	Função de relatório	Permissões de relatórios
Convidado	Consumidor	Pode visualizar, programar e executar relatórios e definir preferências pessoais, como as de idiomas e fusos horários. Os consumidores não podem criar relatórios ou executar tarefas administrativas.
Utilizador	Autor	Pode executar todas as funções de consumidor, bem como criar e gerenciar relatórios e painéis.
Administrador	Administrador	Pode executar todas as funções do autor, bem como todas as tarefas administrativas, tais como a configuração de relatórios e o encerramento e reinício de tarefas de relatório.



O relatório Cloud Insights está disponível para ambientes de 500 MUs ou mais.



Se você é um cliente atual do Premium Edition e deseja manter seus relatórios, leia "[nota importante para os clientes existentes](#)"este .

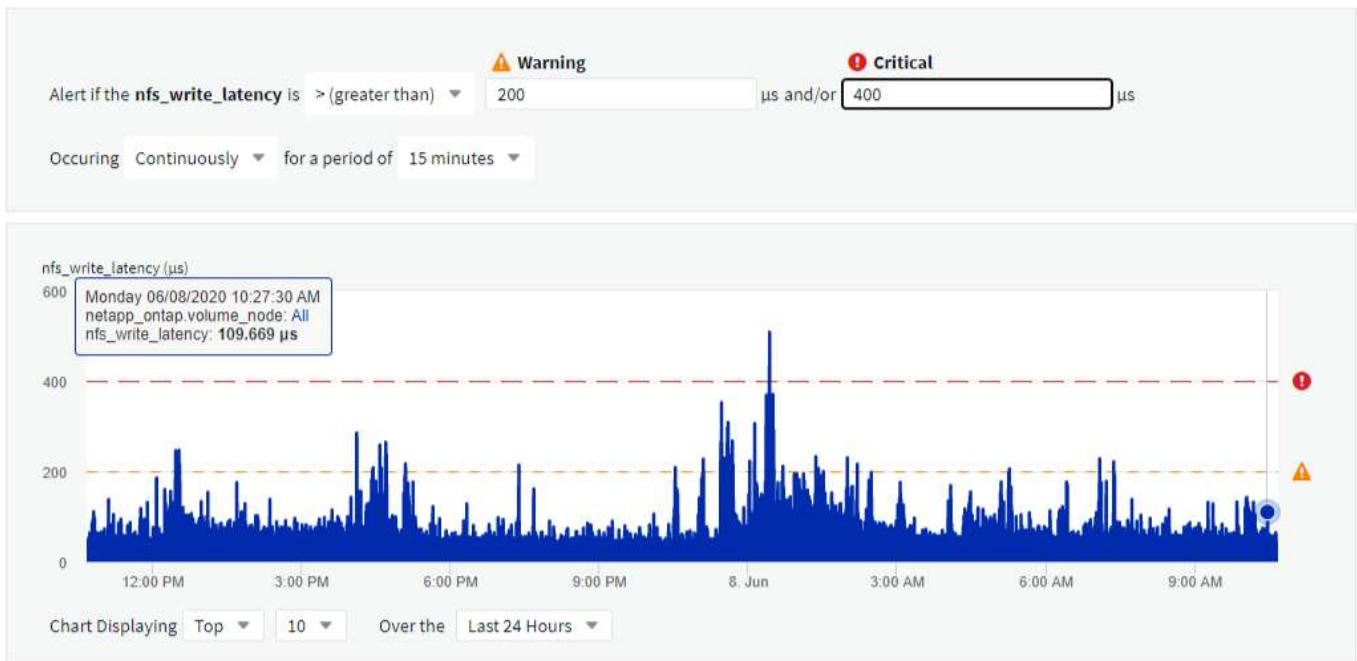
Nova categoria de API para ingestão de dados

O Cloud Insights adicionou uma categoria de API **ingestão de dados**, proporcionando maior controle sobre os dados e agentes personalizados. A documentação detalhada para esta e outras categorias de API pode ser encontrada no Cloud Insights navegando para **Admin > API Access** e clicando no link *Documentação da API*. Também pode anexar um comentário à AU no campo Nota, que é apresentado na página de detalhes da AU, bem como na página da lista da AU.

Agosto de 2020

Monitoramento e alertas

Além da capacidade atual de definir políticas de performance para objetos de storage, VMs, EC2 e portas, a Edição padrão do Cloud Insights agora inclui a capacidade de "[configurar monitores](#)" limites para dados de integração para Kubernetes, métricas avançadas do ONTAP e plugins do Telegraf. Basta criar um monitor para cada métrica de objeto que deseja acionar alertas, definir as condições para os limites de nível de aviso ou nível crítico e especificar o(s) destinatário(s) de e-mail desejado(s) para cada nível. Em seguida, você pode "[ver e gerir alertas](#)" rastrear tendências ou solucionar problemas.



Julho de 2020

Cloud Secure *Faça um Instantâneo Ação*

O Cloud Secure protege seus dados tirando automaticamente um snapshot quando uma atividade maliciosa é detetada, garantindo que seus dados sejam copiados com segurança.

É possível definir políticas de resposta automatizadas que removem um snapshot quando um ataque de ransomware ou outra atividade anormal do usuário é detetada. Também pode tirar um instantâneo manualmente a partir da página de alerta.

Instantâneo automático captado:



POTENTIAL ATTACK: AL_307
Ransomware Attack

Detected
4 days ago
Jul 26, 2020 3:38 AM

Action Taken
Snapshots Taken

Status
In Progress

Last snapshots taken by
Amit Schwartz
Jul 30, 2020 2:54 PM

How To:
Restore Entities

Re-Take Snapshots

Total Attack Results

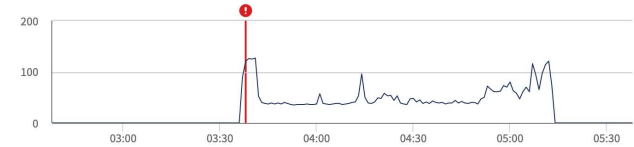
1 Affected Volumes | **0** Deleted Files | **5148** Encrypted Files

5148 Files have been copied, deleted, and potentially encrypted by 1 user account.

This is potentially a sign of ransomware attack. The extension "crypt" was added to each file.

Encrypted Files

Activity per minute



Related Users



Ewen Hall
Developer
Engineering

5148
Encrypted Files

Detected
4 days ago
Jul 26, 2020 3:38 AM

Action Taken
Snapshots Taken

Instantâneo manual:

☰ **Cloud Insights** Abhi Basu Thakur

MONITOR & OPTIMIZE Alerts / **Nabilah Howell had an abnormal change in activity rate** Jul 23, 2020 - Jul 26, 2020
1:44 AM 1:44 AM

Alert Detail

WARNING: AL_306
Nabilah Howell had an abnormal change in activity rate.

Detected
5 days ago
Jul 25, 2020 1:44 PM

Action Taken
None

Status
New

Recommendation: Setup an Automated Response Policy
An Automated Response Policy will trigger measures to contain the damage automatically when a future attack is detected. Try it now.

Take Snapshots

How To:
Restore Entities

Nabilah Howell's Activity Rate Change

Typical	Alert	
122.8 Activities Per Minute	210 Activities Per Minute	↑ 71%

Nabilah Howell's activity rate grew 71% over their typical average.

Activity Rate
Activity per 5 minutes

Atualizações de métrica/contador

Os seguintes contadores de capacidade estão disponíveis para uso na IU do Cloud Insights e na API REST. Anteriormente, esses contadores estavam disponíveis apenas para o Data Warehouse / Reporting.

Tipo Objeto	Contador
Armazenamento	Capacidade - capacidade bruta sobresselente - Falha em bruto

Tipo Objeto	Contador
Pool de storage	Capacidade de dados - capacidade de dados utilizada - total outra capacidade - outra capacidade utilizada - capacidade total - capacidade bruta - limite mole
Volume interno	Capacidade de dados - capacidade de dados utilizada - Total outra capacidade - outra capacidade utilizada - Total Clone Saved Capacity - Total

Detecção de ataque potencial Cloud Secure

O Cloud Secure agora deteta possíveis ataques, como ransomware. Clique em um alerta na página da lista Alertas para abrir uma página de detalhes que mostre o seguinte:

- Tempo de ataque
- Atividade associada do usuário e do arquivo
- Ação tomada
- Informações adicionais para ajudar a rastrear possíveis violações de segurança

Página de alertas mostrando potencial ataque de ransomware:



Página detalhada para um possível ataque de ransomware:



POTENTIAL ATTACK: AL_305
Ransomware Attack

Detected
5 days ago
Jul 11, 2020 4:02 AM

Action Taken
None

Status
New

Total Attack Results

1 Affected Volumes | 0 Deleted Files | 4173 Encrypted Files

4173 Files have been copied, deleted, and potentially encrypted by 1 user account.

This is potentially a sign of ransomware attack.
The extension "crypt" was added to each file.

Encrypted Files

Activity per minute



Related Users



Kristjan Egilsson
Accountant
Finance

4173
Encrypted Files

Detected
5 days ago
Jul 11, 2020 4:02 AM

Action Taken
None



Username
us035
Email
Egilsson@netapp.com
Phone
387224312607

Department
Finance
Manager
Lyndsey Maddox

Top Activity Types

Activity per minute
Last access location: 10.197.144.115

[View Activity Detail](#)



Inscreva-se no Premium Edition pela AWS

Durante a avaliação do Cloud Insights, você pode "auto-subscrição" usar o AWS Marketplace para o Cloud Insights Standard Edition ou Premium Edition. Anteriormente, você só podia se inscrever automaticamente no AWS Marketplace apenas para o Standard Edition.

Widget de tabela melhorado

O widget Tabela de página de dashboard/ativos inclui os seguintes aprimoramentos:

- Visualização "tela dividida": Os widgets da tabela exibem o objeto/agrupamento no lado esquerdo e os dados do objeto (atributos/métricas) à direita.

GroupBy All Override Dashboard Time 🕒 ✕

index_0.index_0 ✕

Filter By + Group agent_version ✕ !

1 Item found ⚙️

Table Row Grouping	Metrics & Attributes				
agent_version	value	consumer	protocol_name	level0	level1
Java/1.8.0_242	1,649.80	CloudInsights	GENERATED	simulated	N/A

- Agrupamento de atributos múltiplos: Para dados de integração (Kubernetes, métricas avançadas do ONTAP, Docker, etc.), você pode escolher vários atributos para agrupamento. Os dados são exibidos de acordo com os atributos de agrupamento/que você escolher.

Agrupamento com dados de integração (mostrado no modo Editar):

Table Widget - Integration Data Example Override Dashboard Time 🕒 Last 7 Days ✕

index_0.index_0 ✕

Filter By + Group agent_version ✕ name ✕ protocol_name ✕ !

500 Items found ⚙️

Table Row Grouping			Metrics & Attributes				
agent_version	name	protocol_name	value	consumer	protocol_name	level0	level1
Java/1.8.0_242	simulated.shinchaku-client-1010.counter.2...	GENERATED	1,597.16	CloudInsights	GENERATED	simulated	shinchaku-
Java/1.8.0_242	simulated.shinchaku-client-1008.counter.1...	GENERATED	1,604.92	CloudInsights	GENERATED	simulated	shinchaku-
Java/1.8.0_242	simulated.shinchaku-client-1015.counter.1...	GENERATED	1,684.82	CloudInsights	GENERATED	simulated	shinchaku-
Java/1.8.0_242	simulated.shinchaku-client-1008.counter.0...	GENERATED	1,677.15	CloudInsights	GENERATED	simulated	shinchaku-

Cancel Save

- O agrupamento de dados de infraestrutura (armazenamento, EC2, VM, portas, etc.) é feito por um único atributo como antes. Ao agrupar por um atributo que não é o objeto, a tabela permitirá que você expanda a linha do grupo para ver todos os objetos dentro do grupo.

Agrupamento com dados de infra-estrutura (apresentados no modo de visualização):

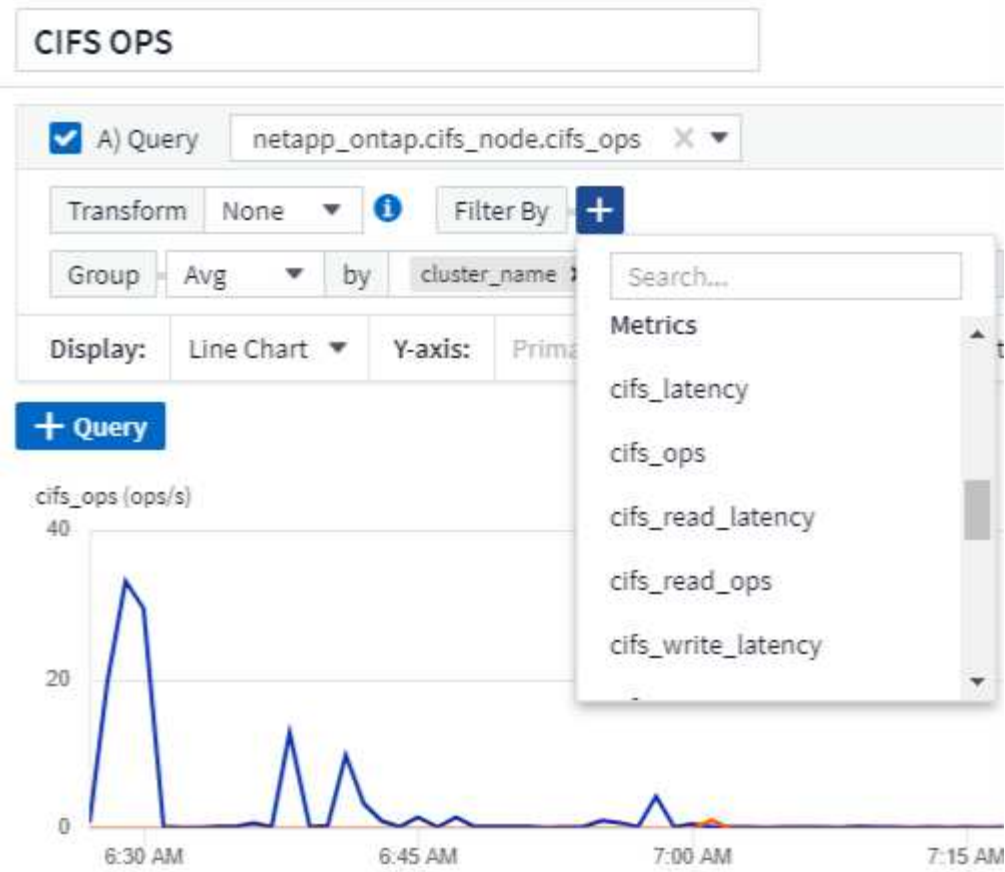
GroupBy Date 🔄 1h

4 items found in 2 groups

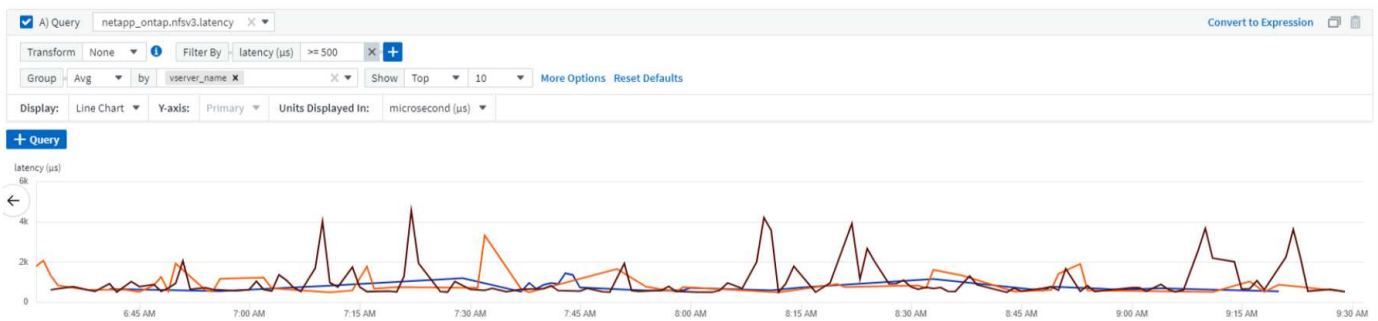
Active Date	Storage Node	Cache Hit Ratio - Total (%)	IOPS - Total (IO...	IOPS - Write (I...	Latency
06/01/2020 (1)	ocinaneqa1-01	N/A	N/A	N/A	N/A
06/01/2020	ocinaneqa1-01	N/A	N/A	N/A	N/A
N/A (3)	--	N/A	N/A	N/A	N/A

Filtragem de métricas

Além de filtrar os atributos de um objeto em um widget, agora você também pode filtrar as métricas.



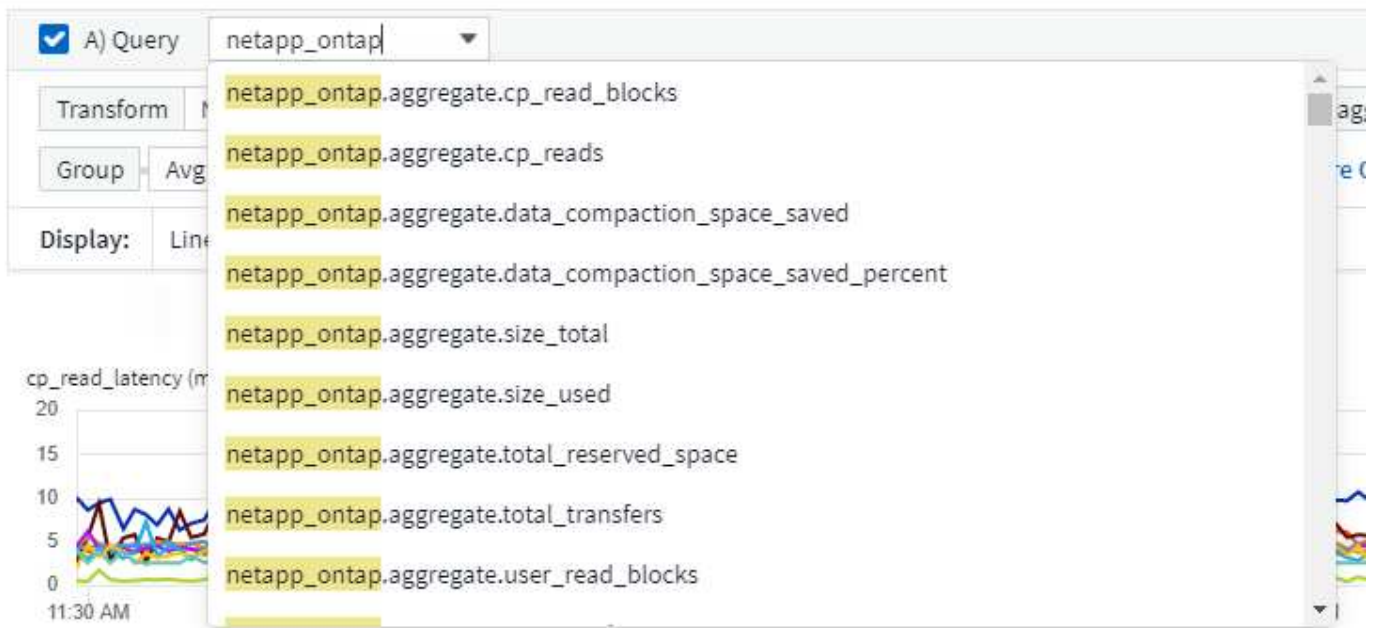
Ao trabalhar com dados de integração (Kubernetes, dados avançados do ONTAP, etc.), a filtragem de métricas remove os pontos de dados individuais/não correspondidos da série de dados plotados, ao contrário dos dados de infraestrutura (armazenamento, VM, portas, etc.), onde os filtros funcionam no valor agregado da série de dados e potencialmente removem todo o objeto do gráfico.



Dados de contador avançados do ONTAP

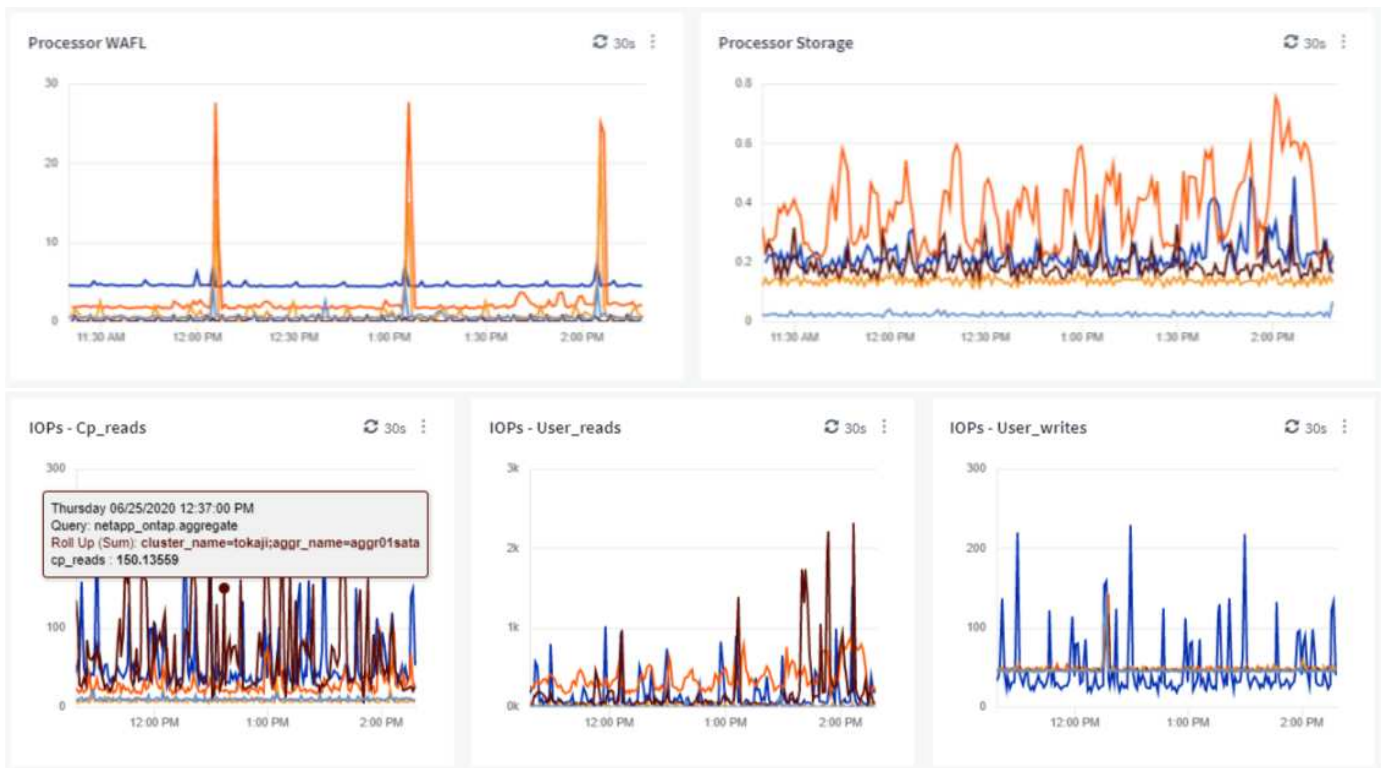
O Cloud Insights aproveita os **dados avançados de contador** específicos do ONTAP da NetApp, que fornecem uma série de contadores e métricas coletados de dispositivos ONTAP. Os dados de contador avançados do ONTAP estão disponíveis para todos os clientes do NetApp ONTAP. Essas métricas permitem uma visualização personalizada e abrangente em widgets e painéis do Cloud Insights.

Os contadores avançados do ONTAP podem ser encontrados pesquisando por "NetApp_ONTAP" na consulta do widget e selecionando entre os contadores.



Você pode refinar sua pesquisa digitando partes adicionais do nome do contador. Por exemplo:

- *lif*
- *agregado*
- *offbox_vscan_server*
- e muito mais



Tenha em atenção o seguinte:

- A coleta avançada de dados será ativada por padrão para novos coletores de dados do ONTAP. Para habilitar a coleta avançada de dados para seus coletores de dados ONTAP existentes, edite o coletor de dados e expanda a seção *Configuração avançada*.
- A recolha avançada de dados não está disponível para ONTAP de 7 modos.

Painéis de contador avançados

O Cloud Insights vem com uma variedade de painéis pré-projetados para ajudá-lo a visualizar os contadores avançados do ONTAP para tópicos como *desempenho agregado*, *carga de trabalho de volume*, *atividade do processador* e muito mais. Se você tiver pelo menos um coletor de dados do ONTAP configurado, eles podem ser importados da Galeria do Painel em qualquer página da lista de painéis.

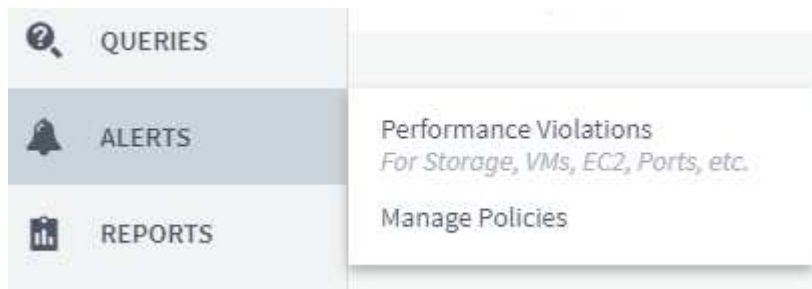
Saiba mais

Mais informações sobre dados avançados do ONTAP podem ser encontradas nos seguintes links:

- <https://mysupport.netapp.com/site/tools/tool-eula/netapp-harvest> (Observação: Você precisará fazer login no suporte da NetApp)
- <https://nabox.org/faq/>

Menu políticas e violações

Políticas de desempenho e violações agora são encontradas no menu **Alertas**. A funcionalidade de política e violação não é alterada.



Agente Telegraf atualizado

O agente para ingestão de dados de integração do telegraf foi atualizado para "versão 1,14"o , que inclui correções de bugs, correções de segurança e novos plugins.

Observação: Ao configurar um coletor de dados do Kubernetes na plataforma Kubernetes, você pode ver um erro "HTTP status 403 Forbidden" no log, devido a permissões insuficientes no atributo "clusterrole".

Para contornar esse problema, adicione as seguintes linhas destacadas à seção *rules*: da função de inclusão de endpoint-access e reinicie os pods de Telegraf.


```

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

```

Junho de 2020

Relatório de erros do coletor de dados simplificado

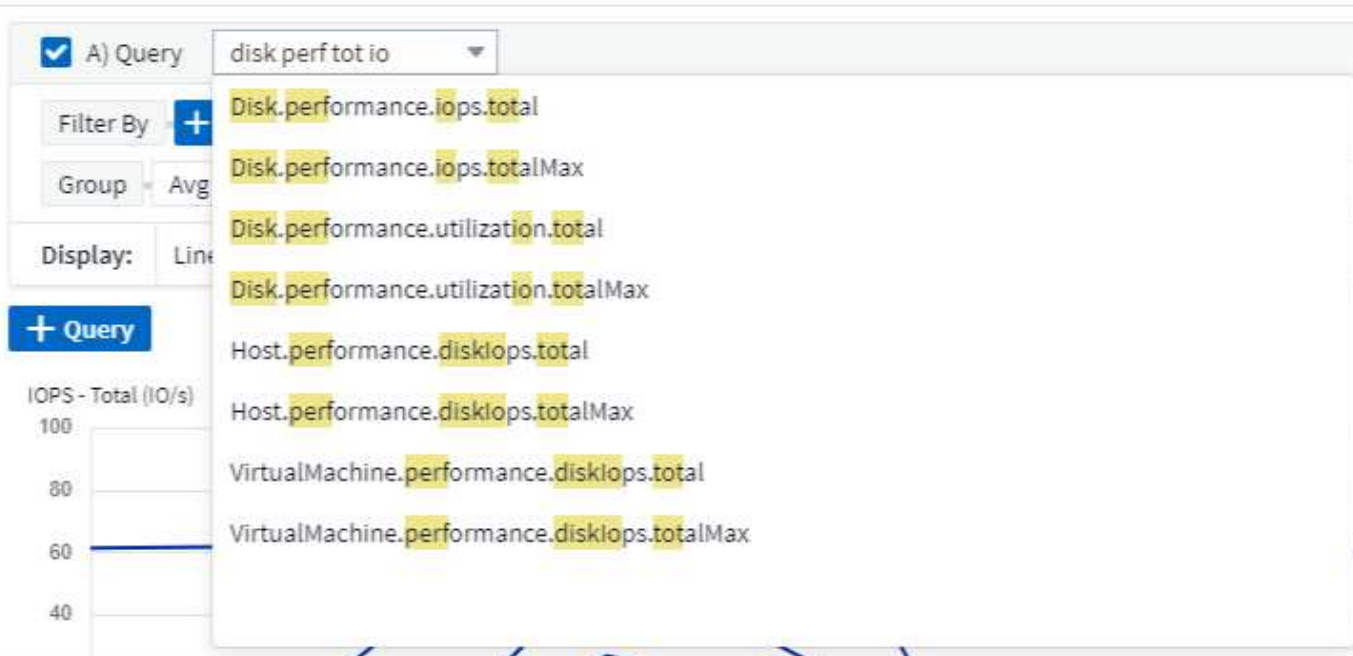
Relatar um erro de coletor de dados é mais fácil com o botão *Send Error Report* na página do coletor de dados. Clicar no botão envia informações básicas sobre o erro para o NetApp e solicita a investigação sobre o problema. Uma vez pressionado, o Cloud Insights reconhece que o NetApp foi notificado e o botão Relatório de erros está desativado para indicar que um relatório de erro para esse coletor de dados foi enviado. O botão permanece desativado até que a página do navegador seja atualizada.



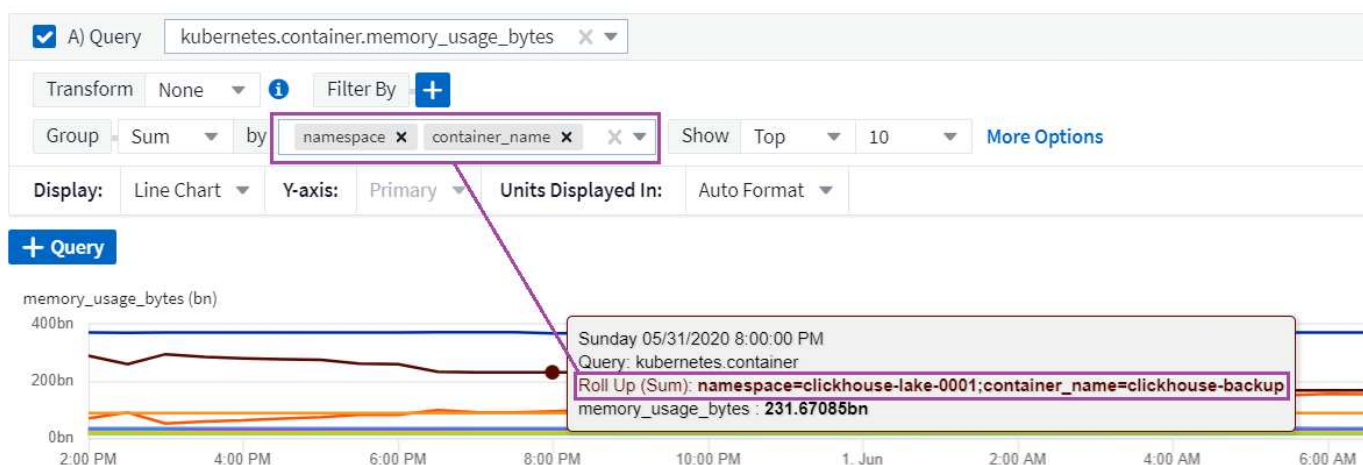
Melhorias no widget

As seguintes melhorias foram feitas nos widgets do painel. Essas melhorias são consideradas funcionalidades de visualização e podem não estar disponíveis para todos os ambientes Cloud Insights.

- Novo seletor de objetos/métricas: Objetos (armazenamento, disco, portas, nós, etc.) e suas métricas associadas (IOPS, latência, contagem de CPU, etc.) estão agora disponíveis em widgets em um único drop-down inclusivo com poderoso recurso de pesquisa. Você pode inserir vários termos parciais na lista suspensa, e o Cloud Insights listará todas as métricas de objetos que atendem a esses termos.



- Agrupamento de várias tags: Ao trabalhar com dados de integração (Kubernetes, etc.), você pode agrupar os dados por várias tags/atributos. Por exemplo, soma o uso da memória pelo namespace do Kubernetes e pelo nome do contêiner.



Maio de 2020

Funções de utilizador de relatórios

As seguintes funções foram adicionadas para relatórios:

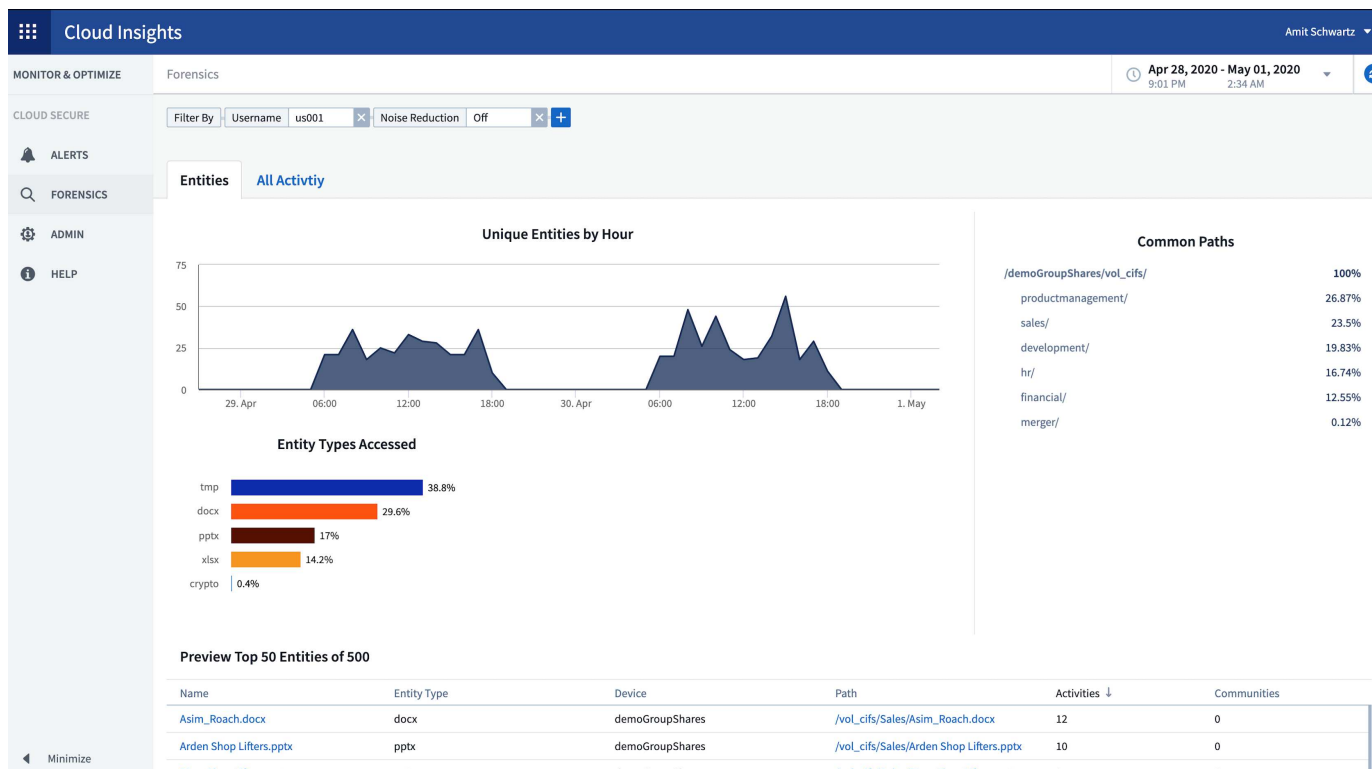
- Consumidores Cloud Insights: Pode executar e visualizar relatórios
- Autores do Cloud Insights: Podem executar as funções de consumidor, bem como criar e gerenciar relatórios e painéis
- Administradores do Cloud Insights: Pode executar as funções do autor, bem como todas as tarefas administrativas

Atualizações do Cloud Secure

O Cloud Insights inclui as seguintes alterações recentes do Cloud Secure.

Na página Forensics > Activity Forensics, fornecemos duas visualizações para analisar e investigar a atividade do usuário:

- Vista de atividade, focada na atividade do utilizador (que operação? Onde se realizou?)
- Visualização de entidades, focada em quais arquivos o usuário acessou.



Além disso, a notificação por e-mail de alerta agora contém um link direto para a página de alerta.

Agrupamento do tablier

O agrupamento de painéis permite que você seja melhor "gestão de dashboards" relevante. Você pode adicionar painéis relacionados a um grupo para gerenciamento "one-stop" de, por exemplo, seu armazenamento ou máquinas virtuais.

Os grupos são personalizados por usuário, então os grupos de uma pessoa podem ser diferentes dos de outra pessoa. Você pode ter quantos grupos precisar, com quantos painéis quiser ou quantos painéis quiser em cada grupo.

Dashboard Groups (3)



Search groups..

All Dashboards (60)

My Dashboards (11)

Storage Group (7) ⋮

Dashboards (7)



Name ↑

Dashboard - Storage Cost

Dashboard - Storage IO Detail

Dashboard - Storage Overview

Gauges Storage Performance

Storage Admin - Which nodes are in high demand?

Storage Admin - Which pools are in high demand?

Storage IOPs

Fixação do painel de instrumentos

É possível fixar painéis para que os favoritos apareçam sempre no topo da lista.

Dashboards (7)



Name ↑



Dashboard - Storage Overview



Storage Admin - Which nodes are in high demand?



Storage IOPs

Dashboard - Storage Cost

Dashboard - Storage IO Detail

Gauges Storage Performance

Storage Admin - Which pools are in high demand?

Modo de TV e Atualização automática

"[Modo de TV e Atualização automática](#)" permitir a exibição de dados quase em tempo real em um painel ou página de ativos:

- **Modo de TV** fornece uma exibição organizada; o menu de navegação está oculto, proporcionando mais espaço de tela para a exibição de dados.
- Dados em widgets em painéis e páginas de destino de ativos **Atualização automática** de acordo com um intervalo de atualização (a cada 10 segundos) determinado pelo intervalo de tempo do Painel selecionado

(ou intervalo de tempo do widget, se definido para substituir o tempo do painel).

Combinados, o modo TV e a Atualização automática fornecem uma visualização em tempo real dos seus dados Cloud Insights, perfeita para demonstrações contínuas ou monitorização interna.

Abril de 2020

Novas opções de intervalo de tempo do painel de instrumentos

As opções de intervalo de tempo para painéis e outras páginas do Cloud Insights agora incluem *Last 1 Hour* e *Last 15 minutes*.

Atualizações do Cloud Secure

O Cloud Insights inclui as seguintes alterações recentes do Cloud Secure.

- Melhores metadados de arquivos e pastas mudam o reconhecimento para detetar se o usuário alterou a permissão, proprietário ou propriedade de Grupo.
- Exportar relatório de atividades do usuário para CSV.

O Cloud Secure monitora e audita todas as operações de acesso do usuário em arquivos e pastas. A auditoria de atividades permite que você cumpra políticas de segurança internas, atenda a requisitos de conformidade externos, como PCI, GDPR e HIPAA, e conduza investigações de incidentes de segurança e violação de dados.

Hora predefinida do painel de instrumentos

O intervalo de tempo padrão para painéis é agora de 3 horas em vez de 24 horas.

Tempos de agregação otimizados

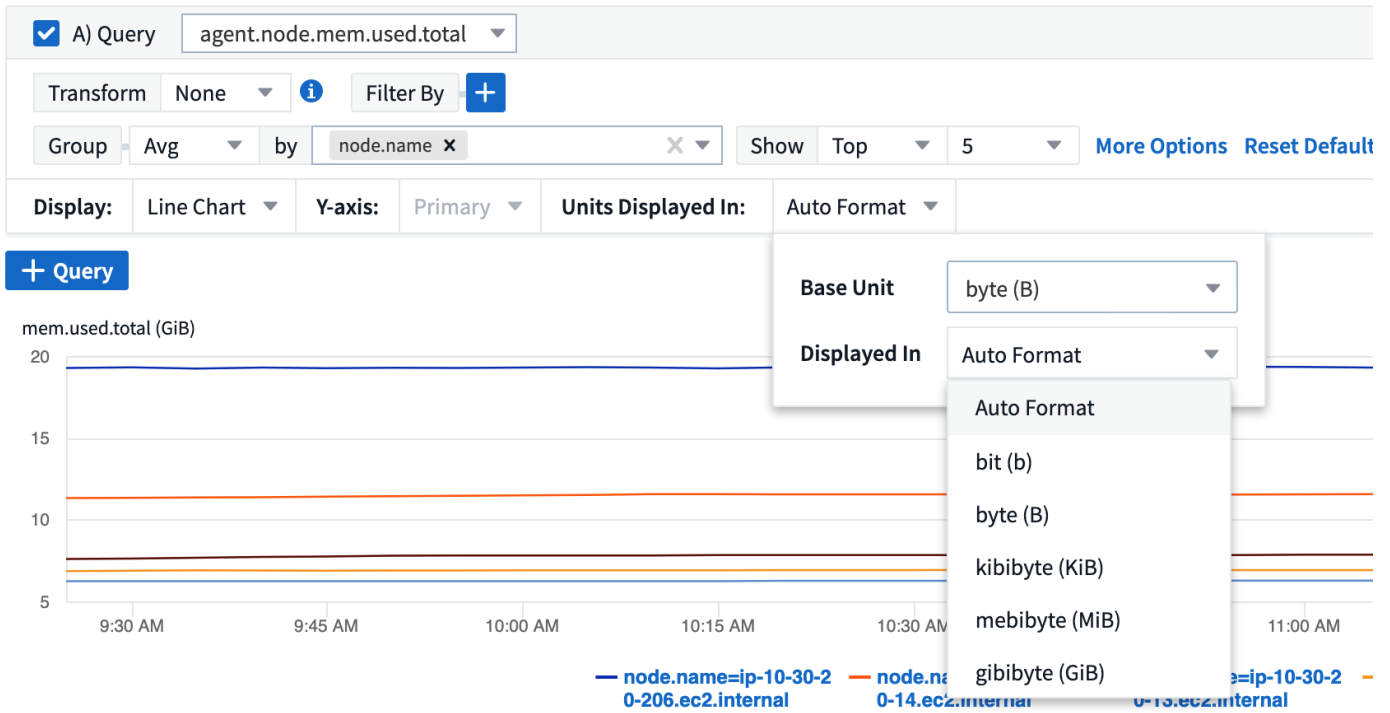
Intervalos otimizados "[agregação de tempo](#)" em widgets de séries temporais (gráficos de linha, spline, Area e Stacked Area) são mais frequentes para intervalos de tempo de painel/widget de 3 horas e 24 horas, permitindo gráficos mais rápidos de dados.

- o intervalo de tempo de 3 horas otimiza para um intervalo de agregação de 1 minutos. Anteriormente, isso era de 5 minutos.
- o intervalo de tempo de 24 horas otimiza para um intervalo de agregação de 30 minutos. Anteriormente era 1 hora.

Você ainda pode substituir a agregação otimizada definindo um intervalo personalizado.

Apresentar formato automático da unidade

Na maioria dos widgets, o Cloud Insights conhece a unidade base para exibir valores, por exemplo *megabytes*, *milhares*, *porcentagem*, *milissegundos (ms)*, etc., e agora "[formata automaticamente](#)" o widget para a unidade mais legível. Por exemplo, um valor de dados de 1.234.567.890 bytes seria formatado automaticamente para 1,23 gibibytes. Em muitos casos, o Cloud Insights sabe o melhor formato para os dados que estão sendo adquiridos. Nos casos em que o melhor formato não é conhecido, ou em widgets onde você deseja substituir a formatação automática, você pode escolher o formato desejado.



Importar anotações usando API

Com a poderosa API do Cloud Insights, agora você pode "importar anotações" atribuí-los a objetos usando um arquivo .CSV. Você também pode importar aplicativos e atribuir entidades de negócios da mesma maneira.

ASSETS.import

PUT /assets/import Import assets from a CSV file.

Import annotations and applications from the given CSV file. The format of the CSV file is following:

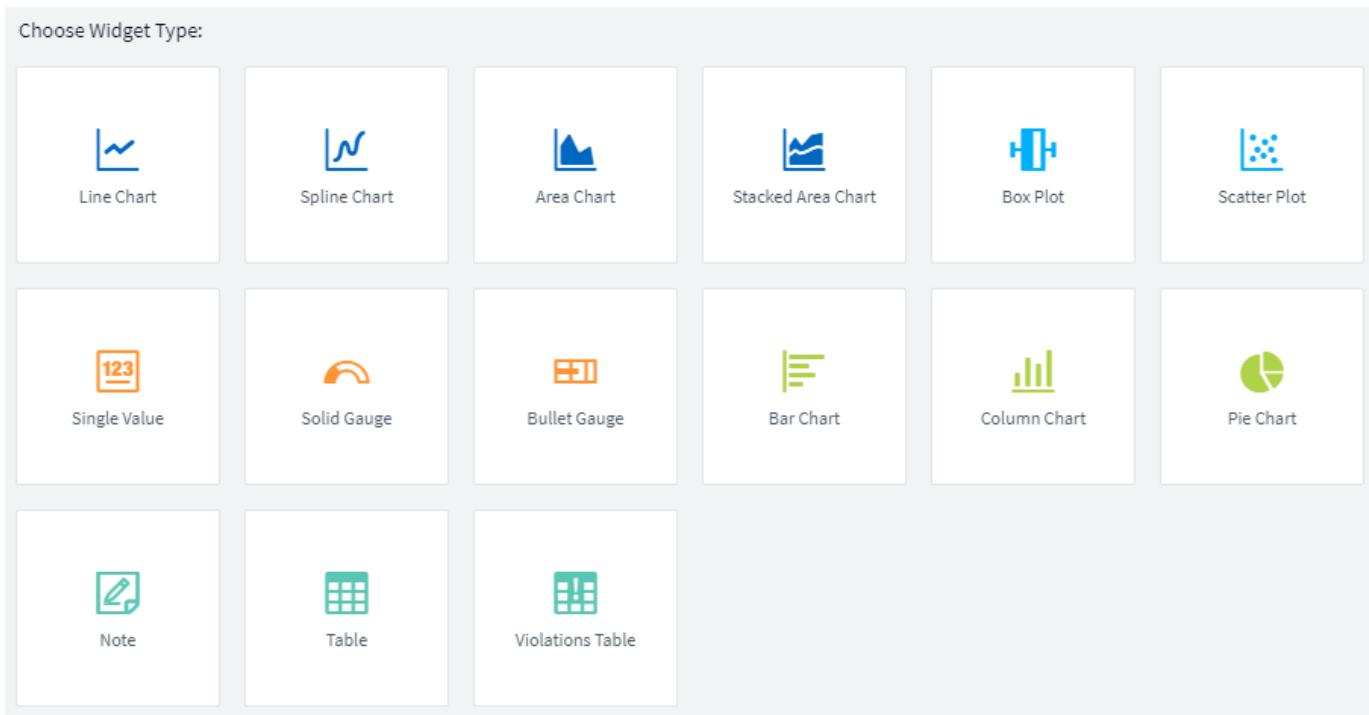
```

Project]
, <Annotation Type> [, <Annotation Type> ...] [, Application] [, Tenant] [, Line_Of_Business] [, Business_Unit] [,
<Object Type Value 1>, <Object Name or Key 1>, <Annotation Value> [, <Annotation Value> ...] [, <Application>] [, <Tenant>] [, <Line_Of_Business>] [, <Business_Unit>] [,
<Project>]
<Object Type Value 2>, <Object Name or Key 2>, <Annotation Value> [, <Annotation Value> ...] [, <Application>] [, <Tenant>] [, <Line_Of_Business>] [, <Business_Unit>] [,
<Project>]
<Object Type Value 3>, <Object Name or Key 3>, <Annotation Value> [, <Annotation Value> ...] [, <Application>] [, <Tenant>] [, <Line_Of_Business>] [, <Business_Unit>] [,
<Project>]
...
<Object Type Value N>, <Object Name or Key N>, <Annotation Value> [, <Annotation Value> ...] [, <Application>] [, <Tenant>] [, <Line_Of_Business>] [, <Business_Unit>] [,
<Project>]

```

Seletor Widget mais simples

Adicionar widgets a dashboards e páginas de destino de ativos é mais fácil com um novo seletor de widgets que mostra todos os tipos de widget em uma única exibição tudo ao mesmo tempo, para que o usuário não precise mais rolar por uma lista de tipos de widget para encontrar o que deseja adicionar. Widgets relacionados são coordenados por cores e agrupados por proximidade no novo seletor.



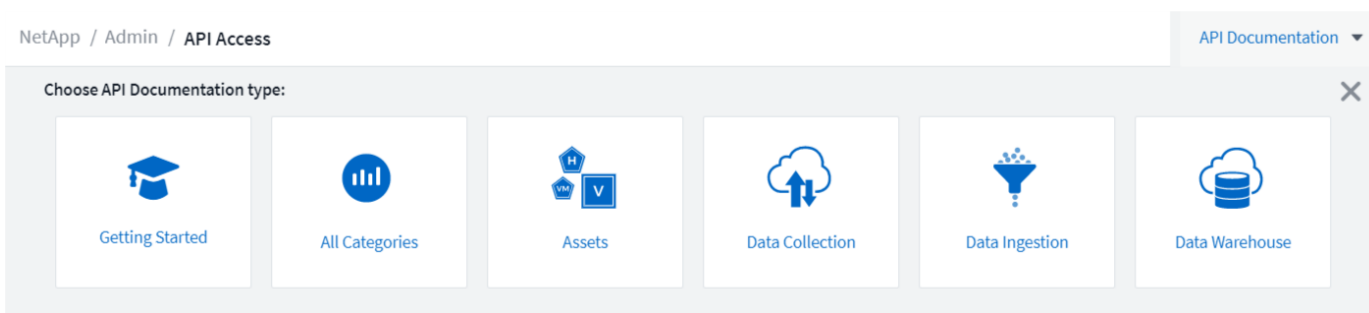
Fevereiro de 2020

API com Premium Edition

O Cloud Insights Premium Edition vem com um "API poderosa" que pode ser usado para integrar o Cloud Insights com outros aplicativos, como CMDB ou outros sistemas de emissão de bilhetes.

Informações detalhadas baseadas em Swagger são encontradas em **Admin > Acesso à API**, sob o link **Documentação da API**. O Swagger fornece uma breve descrição e informações de uso para a API e permite que você experimente cada API em seu ambiente.

A API Cloud Insights usa tokens de acesso para fornecer acesso baseado em permissão a categorias de API, como ATIVOS ou COLEÇÃO.



Sondagem inicial depois de adicionar Um coletor de dados

Anteriormente, depois de configurar um novo coletor de dados, o Cloud Insights pesquisaria o coletor de dados imediatamente para coletar dados *inventário*, mas aguardaria até o intervalo de enquete de desempenho configurado (normalmente 15 minutos) para reunir dados *performance* iniciais. Ele então

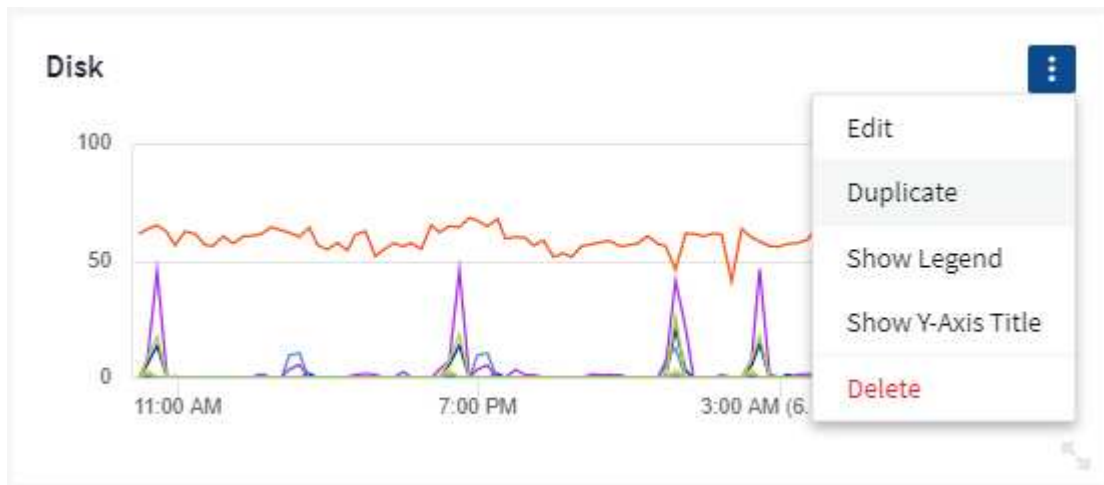
esperaria por outro intervalo antes de iniciar a segunda pesquisa de desempenho, o que significava que levaria até *30 minutos* antes que dados significativos fossem adquiridos de um novo coletor de dados.

O coletor de dados "**polling**" foi muito melhorado, de modo que a pesquisa de desempenho inicial ocorre imediatamente após a pesquisa de inventário, com a segunda pesquisa de desempenho ocorrendo dentro de alguns segundos após a conclusão da primeira pesquisa de desempenho. Isso permite que o Cloud Insights comece a mostrar dados úteis em painéis e gráficos em um tempo muito curto.

Esse comportamento de enquete também ocorre depois de editar a configuração de um coletor de dados existente.

Duplicação de Widget mais fácil

É mais fácil do que nunca criar uma cópia de um widget em um painel ou página de destino. No modo de edição do dashboard, clique no menu no widget e selecione **duplicar**. O editor de widget é iniciado, pré-preenchido com a configuração original do widget e com um sufixo "copy" no nome do widget. Você pode facilmente fazer todas as alterações necessárias e salvar o novo widget. O widget será colocado na parte inferior do seu painel de controle, e você pode posicioná-lo conforme necessário. Lembre-se de salvar seu painel quando todas as alterações estiverem concluídas.



Logon único (SSO)

Com o Cloud Insights Premium Edition, os administradores podem habilitar "**Logon único**" (SSO) o acesso ao Cloud Insights para todos os usuários em seu domínio corporativo, sem ter que convidá-los individualmente. Com o SSO ativado, qualquer usuário com o mesmo endereço de e-mail de domínio pode fazer login no Cloud Insights usando suas credenciais corporativas.



O SSO só está disponível no Cloud Insights Premium Edition e deve ser configurado antes de poder ser ativado para o Cloud Insights. A configuração SSO inclui "**Federação de identidade**" através do NetApp Cloud Central. A federação permite que usuários de logon único acessem suas contas do NetApp Cloud Central usando credenciais de seu diretório corporativo.

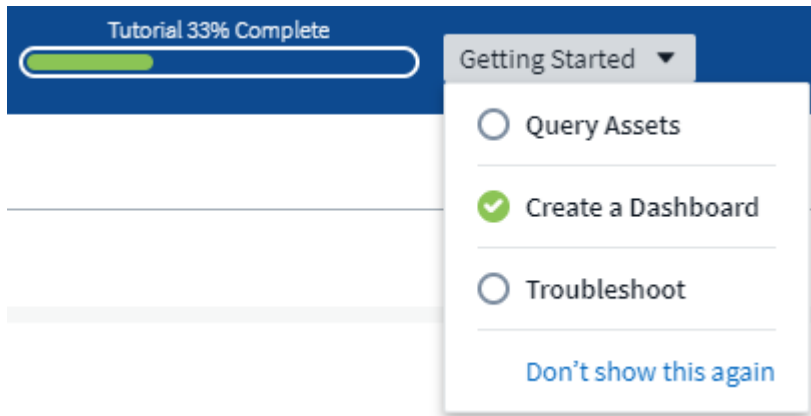
Janeiro de 2020

Documentação do Swagger para API REST

Swagger explica cada API REST disponível no Cloud Insights, bem como seu uso e sintaxe. As informações sobre APIs do Cloud Insights estão disponíveis no "[documentação](#)".

Barra de progresso dos tutoriais de funcionalidades

A lista de verificação de tutoriais de recursos foi movida para o banner superior e agora apresenta um indicador de progresso. Tutoriais estão disponíveis para cada usuário até serem descartados e estão sempre disponíveis no Cloud Insights "[documentação](#)".



Alterações da Unidade de aquisição

Ao instalar uma unidade de aquisição (AU) em um host ou VM que tenha o mesmo nome de uma AU já instalada, o Cloud Insights garante um nome exclusivo anexando o nome AU com "_1", "_2", etc. este também é o caso ao desinstalar e reinstalar uma AU da mesma VM sem primeiro removê-la do Cloud Insights. Quer um nome AU diferente completamente? Não há problema; os AU podem ser renomeados após a instalação.

Agregação de tempo otimizada em Widgets

Em widgets, você pode escolher entre um intervalo de agregação de tempo *otimizado* ou um intervalo *Custom* definido por você. A agregação otimizada seleciona automaticamente o intervalo de tempo certo com base no intervalo de tempo do painel selecionado (ou intervalo de tempo do widget, se substituir o tempo do painel). O intervalo muda dinamicamente à medida que o painel ou o intervalo de tempo do widget é alterado.

Processo simplificado de "Introdução ao Cloud Insights"

O processo para começar a usar o Cloud Insights foi simplificado para tornar a sua configuração inicial mais fácil e suave. Basta selecionar um coletor de dados inicial e seguir as instruções. O Cloud Insights irá orientá-lo através da configuração do coletor de dados e de qualquer agente ou unidade de aquisição necessária. Na maioria dos casos, até mesmo importará um ou mais painéis iniciais para que você possa começar a obter insights sobre seu ambiente rapidamente (mas aguarde até 30 minutos para que o Cloud Insights colete dados significativos).

Melhorias adicionais:

- A instalação da unidade de aquisição é mais simples e é executada mais rápido.
- As escolhas de coletores de dados alfabéticos facilitam a localização daquele que você está procurando.
- As instruções de configuração melhoradas do Data Collector são mais fáceis de seguir.

- Usuários experientes podem ignorar o processo de introdução com o clique de um botão.
- Uma nova barra de progresso mostra onde você está no processo.



Dezembro de 2019

Entidade de negócio pode ser usada em filtros

As anotações de entidades empresariais podem ser usadas em filtros para consultas, widgets, políticas de desempenho e páginas de destino.

Disponível para widgets Single-Value e Gauge, e quaisquer widgets rolados para "All"

Clicar no valor em um widget de valor único ou indicador abre uma página de consulta mostrando os resultados da primeira consulta usada no widget. Além disso, clicar na legenda de qualquer widget cujos dados são agrupados por "todos" também abrirá uma página de consulta mostrando os resultados da primeira consulta usada no widget.

Período experimental prolongado

Os novos usuários que se inscrevem para uma avaliação gratuita do Cloud Insights agora têm 30 dias para avaliar o produto. Este é um aumento em relação ao período experimental anterior de 14 dias.

Cálculo Unidade gerenciada

O cálculo de unidades gerenciadas (MUs) no Cloud Insights foi alterado para o seguinte:

- 1 Unidade gerenciada: 2 hosts (qualquer máquina virtual ou física)
- 1 Unidade gerenciada: 4 TB de capacidade não formatada de discos físicos ou virtuais

Essa alteração dobra com eficiência a capacidade do ambiente que você pode monitorar com a assinatura atual do Cloud Insights.

Novembro de 2019

Outubro de 2019

Relatórios

"[Relatório Cloud Insights](#)" é uma ferramenta de business intelligence que permite visualizar relatórios predefinidos ou criar relatórios personalizados. Com o Reporting, você pode executar as seguintes tarefas:

- Execute um relatório predefinido
- Crie um relatório personalizado
- Personalize o formato do relatório e o método de entrega
- Programe relatórios para serem executados automaticamente
- Relatórios por e-mail
- Use cores para representar limites nos dados

Os relatórios do Cloud Insights podem gerar relatórios personalizados para áreas como chargeback, análise de consumo e previsão, e podem ajudar a responder a perguntas como:

- Que inventário tenho?
- Onde está o meu inventário?
- Quem está usando nossos ativos?
- Qual é o chargeback para storage alocado para uma unidade de negócios?
- Por quanto tempo até que eu precise adquirir capacidade de armazenamento adicional?
- As unidades de negócios estão alinhadas ao longo das camadas de storage adequadas?
- Como a alocação de storage muda ao longo de um mês, trimestre ou ano?

Os relatórios estão disponíveis com o Cloud Insights **Premium Edition**.

Melhorias no Active IQ

"Riscos da Active IQ" agora estão disponíveis como objetos que podem ser consultados, bem como usados em widgets de tabela do painel. Os seguintes atributos de objeto de riscos estão incluídos: * Categoria * Categoria de mitigação * impacto potencial * Detalhe de risco * gravidade * origem * armazenamento * nó de armazenamento * Categoria de UI

Setembro de 2019

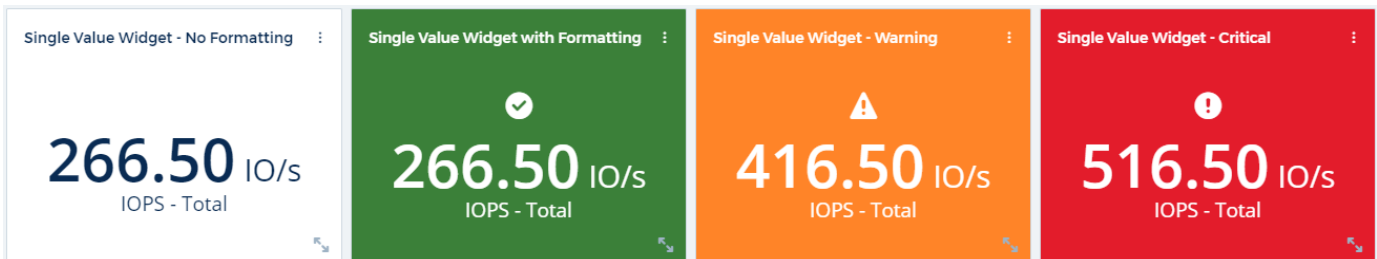
Novos Widgets de calibre

Dois novos widgets estão disponíveis para exibir dados de valor único em seus painéis em cores atraentes com base nos limites especificados. Você pode exibir valores usando um **Solid Gauge** ou **Bullet Gauge**. Os valores que chegam dentro do intervalo de aviso são apresentados a laranja. Os valores no intervalo crítico são apresentados a vermelho. Os valores abaixo do limiar de aviso são apresentados a verde.



Formatação de cores condicionais para Widget de valor único

Agora você pode exibir o widget de valor único com um fundo colorido com base nos limites definidos.



Convide usuários durante o Onboarding

A qualquer momento durante o processo de integração, você pode clicar em Admin > Gerenciamento de usuários > Usuário para convidar usuários adicionais para o seu ambiente Cloud Insights. Esteja ciente de que os usuários com funções *Guest* ou *User* terão maior benefício quando a integração for concluída e os dados forem coletados.

Melhoria da página de detalhes do coletor de dados

A página de detalhes do coletor de dados foi melhorada para exibir erros em um formato mais legível. Os erros são agora exibidos em uma tabela separada na página, com cada erro exibido em uma linha separada no caso de vários erros para o coletor de dados.

Agosto de 2019

Todos vs. Coletores de dados disponíveis

Ao adicionar coletores de dados ao seu ambiente, você pode definir um filtro para mostrar apenas os coletores de dados disponíveis para você com base no seu nível de assinatura, ou todos os coletores de dados.

Integração com ActiveIQ

O Cloud Insights coleta dados do NetApp ActiveIQ, que fornece uma série de visualizações, análises e outros serviços relacionados ao suporte para clientes da NetApp e seus sistemas de hardware/software. O Cloud Insights se integra aos sistemas de gerenciamento de dados do ONTAP. Consulte ["Active IQ"](#) para obter mais informações.

Julho de 2019

Melhorias no painel de instrumentos

Painéis e Widgets foram melhorados com as seguintes alterações:

- Além de soma, Mín, Máx e Méd, **Count** é agora uma opção para rolagem em widgets de valor único. Ao rolar por "contagem", o Cloud Insights verifica se um objeto está ativo ou não, e apenas adiciona os ativos à contagem. O número resultante está sujeito a agregação e filtros.
- No widget de valor único, agora você tem a opção de exibir o número resultante com 0, 1, 2, 3 ou 4 casas decimais.
- Os gráficos de linha mostram uma etiqueta de eixo e unidades quando um único contador está sendo traçado.
- **A opção Transform** está disponível para dados de integração de Serviços agora em todos os widgets de séries temporais para todas as métricas. Para qualquer contador de integração de serviços (Telegraf) ou métrica em widgets de séries temporais (linha, spline, Area, Stacked Area), você pode escolher como deseja ["Transforme os valores"](#). Nenhum (valor de exibição como está), soma, Delta, cumulativo, etc.

Downgrade para Basic Edition

O downgrade para a Edição básica falha com uma mensagem de erro se não houver nenhum dispositivo NetApp disponível configurado que tenha concluído com êxito uma pesquisa nos últimos 7 dias.

Coletando métricas Kube-State

O ["Kubernetes Data Collector"](#) agora coleta objetos e contadores do plugin kube-state-metrics, expandindo consideravelmente o número e o escopo das métricas disponíveis para monitoramento no Cloud Insights.

Junho de 2019

Edições Cloud Insights

O Cloud Insights está disponível em diferentes edições para atender às suas necessidades de orçamento e negócios. Os clientes NetApp existentes com uma conta de suporte NetApp ativa podem desfrutar de 7 dias de retenção de dados e acesso a coletores de dados NetApp com a **Edição básica** gratuita, ou obter maior retenção de dados, acesso a todos os coletores de dados suportados, suporte técnico especializado e muito mais com **Edição padrão**. Para obter mais informações sobre os recursos disponíveis, consulte o site do NetApp "[Cloud Insights](#)".

Novo coletor de dados de infraestrutura: NetApp HCI

- "[Centro Virtual da NetApp HCI](#)" Foi adicionado como um coletor de dados de infraestrutura. O coletor de dados do Centro Virtual HCI coleta informações do host do NetApp HCI e requer Privileges somente leitura em todos os objetos do Centro Virtual.

Observe que o coletor de dados da HCI somente adquire do HCI Virtual Center. Para coletar dados do sistema de armazenamento, você também deve configurar o coletor de dados NetApp "[SolidFire](#)".

Maio de 2019

Novo coletor de dados de serviço: Kapacitor

- "[Kapacitor](#)" foi adicionado como um coletor de dados para serviços.

Integração com Serviços via Telegraf

Além da aquisição de dados de dispositivos de infraestrutura, como switches e armazenamento, o Cloud Insights agora coleta dados de uma variedade de sistemas operacionais e Serviços, usando "[Telegraf como seu agente](#)" para coleta de dados de integração. Telegraf é um agente orientado a plugins que pode ser usado para coletar e relatar métricas. Plugins de entrada são usados para coletar as informações desejadas no agente acessando o sistema/os diretamente, chamando APIs de terceiros ou ouvindo fluxos configurados.

A documentação para integrações atualmente suportadas pode ser encontrada no menu à esquerda em **Referência e suporte**.

Storage Virtual Machine Assets

- As máquinas virtuais de storage (SVMs) estão disponíveis como ativos no Cloud Insights. Os SVMs têm suas próprias páginas de destino de ativos e podem ser exibidos e usados em pesquisas, consultas e filtros. Os SVMs também podem ser usados em widgets de painel, bem como associados a anotações.

Requisitos do sistema da unidade de aquisição reduzida

- Os requisitos de CPU e memória do sistema para o software da unidade de aquisição (AU) foram reduzidos. Os novos requisitos são:

Componente	* Requisito antigo *	* Novo requisito*
Núcleos de CPU	4	2
Memória	16 GB	8 GB

Plataformas adicionais suportadas

- As seguintes plataformas foram adicionadas às plataformas atualmente ["Compatível com Cloud Insights"](#):

Linux	Windows
CentOS 7,3 64-bit CentOS 7,4 64-bit CentOS 7,6 64-bit Debian 9 64-bit Red Hat Enterprise Linux 7,3 64-bit Red Hat Enterprise Linux 7,4 64-bit Ubuntu Server 18,04 LTS 7,6 64-bit	Microsoft Windows 10 64-bit Microsoft Windows Server 2008 R2 Microsoft Windows Server 2019

Abril de 2019

Filtrar máquinas virtuais por Tags

Ao configurar os seguintes coletores de dados, você pode filtrar para incluir ou excluir máquinas virtuais da coleta de dados de acordo com suas Tags ou rótulos.

- ["Amazon EC2"](#)
- ["Azure"](#)
- ["Google Cloud Platform"](#)

Março de 2019

Notificações por e-mail para eventos relacionados com assinaturas

- Você pode selecionar destinatários para e-mail ["notificações"](#) quando eventos relacionados à assinatura ocorrerem, como expiração da avaliação ou alterações na conta subscrita. Você pode escolher destinatários para essas notificações entre os seguintes:
 - Todos os proprietários de contas
 - Todos os administradores
 - Endereços de e-mail adicionais que você especificar

Painéis adicionais

- Os seguintes novos focos da AWS ["dashboards"](#) foram adicionados à galeria e estão disponíveis para importação:
 - AWS Admin - quais EC2 estão em alta demanda?
 - Desempenho de instância do AWS EC2 por região

Fevereiro de 2019

Coleta de contas AWS Child

- O Cloud Insights é compatível "[Coleta de contas filhas da AWS](#)" com um único coletor de dados. Seu ambiente da AWS deve estar configurado para permitir que o Cloud Insights colete de contas menores.

Nome do coletor de dados

- Os nomes do coletor de dados agora podem incluir pontos (.), hífen (-) e espaços (), além de letras, números e sublinhados. Os nomes não podem começar ou terminar com um espaço, ponto ou hífen.

Unidade de aquisição para Windows

- Você pode configurar uma Unidade de aquisição do Cloud Insights em um servidor/VM do Windows. Revise o Windows "[pré-requisitos](#)" antes de instalar o "[Software da unidade de aquisição](#)".

Janeiro de 2019

O campo "proprietário" é mais legível

- Nas listas Dashboard e Query, os dados do campo "Owner" anteriormente eram uma string de ID de autorização, em vez de um nome de proprietário amigável. O campo "proprietário" agora mostra um nome de proprietário mais simples e legível.

Divisão da Unidade gerenciada na Página de assinatura

- Para cada coletor de dados listado na página **Admin > Subscription**, agora você pode ver um detalhamento das contagens de unidades gerenciadas (MU) para hosts e armazenamento, bem como o total.

Dezembro de 2018

Melhoria do tempo de carregamento da IU

- O tempo de carregamento inicial para a interface de usuário (UI) do Cloud Insights foi significativamente melhorado. O tempo de atualização da IU também se beneficia dessa melhoria em circunstâncias em que os metadados são carregados.

Edição em massa coletores de dados

- Você pode editar informações para vários coletores de dados ao mesmo tempo. Na página **observabilidade > coletores**, selecione os coletores de dados a serem modificados marcando a caixa à esquerda de cada um e clique no botão **ações em massa**. Escolha **Editar** e modifique os campos necessários.

Os coletores de dados selecionados devem ser do mesmo fornecedor e modelo e residir na mesma

Unidade de aquisição.

As páginas de suporte e assinatura estão disponíveis durante o Onboarding

- Durante o fluxo de trabalho de integração, você pode navegar para as páginas **Ajuda > suporte** e **Admin > assinatura**. O retorno dessas páginas retorna ao fluxo de trabalho de integração, desde que você não tenha fechado a guia do navegador.

Novembro de 2018

Inscreva-se por meio do NetApp Sales ou do AWS Marketplace

- A subscrição e faturação do Cloud Insights estão agora disponíveis diretamente através do NetApp. Isso é além da assinatura de autoatendimento disponível no AWS Marketplace. Um novo link **Contact Sales** é apresentado na página **Admin > Subscription**. Para clientes cujos ambientes têm ou se espera que tenham 1.000 ou mais unidades gerenciadas (MUs), recomenda-se entrar em Contato com as vendas da NetApp através do link vendas de Contato.

Hiperligações de anotação de texto

- As anotações do tipo texto podem agora incluir hiperligações.

Walkthrough de integração

- O Cloud Insights agora apresenta um passo a passo de integração para o primeiro usuário (administrador ou proprietário da conta) a fazer login em um novo ambiente. O passo a passo leva você através da instalação de uma Unidade de aquisição, configuração de um coletor de dados inicial e seleção de um ou mais painéis úteis.

Importar painéis da Galeria

- Além de selecionar painéis durante a integração, você pode importar painéis via **painéis > Mostrar todos os painéis** e clicar em * na Galeria*.

Duplicação de Dashboards

- A capacidade de duplicar um painel foi adicionada à página de lista de painéis como uma escolha no menu de opções para cada painel e na própria página principal de um painel no menu *Salvar*.

Menu de produtos Cloud Central

- O menu que permite alternar para outros produtos da NetApp Cloud Central foi movido para o canto superior direito da tela.

Integração do Data Infrastructure Insights

Antes de começar a trabalhar com o Insights de infraestrutura de dados, você deve se inscrever no portal **NetApp BlueXP** . Se você já tiver um login no NetApp BlueXP , poderá iniciar uma avaliação gratuita do Insights de infraestrutura de dados com algumas etapas rápidas.

Criando sua conta do NetApp BlueXP

Para começar a usar os serviços de nuvem da NetApp, "**NetApp BlueXP** "acesse e clique em **Get Started**.

- Se ainda não se inscreveu, selecione **Inscrever-se**
- Introduza um endereço de correio eletrônico comercial válido e escolha uma palavra-passe.
- Introduza o nome da sua empresa e o seu nome completo.
- Aceite os termos e condições e selecione **continuar**.
- BlueXP irá guiá-lo através de começar.

E se eu já tiver um login no NetApp BlueXP ?

Depois de ter uma conta no NetApp BlueXP , basta escolher **entrar** na "**NetApp BlueXP** " página do portal.

Introduza o seu endereço de e-mail e palavra-passe. Você será levado para a página de ofertas de nuvem da NetApp.

Selecione Data Infrastructure Insights.



Cloud Insights
Start Free Trial

Iniciando a avaliação gratuita do Data Infrastructure Insights

Se esta for a primeira vez que fizer login no Data Infrastructure Insights, na oferta Data Infrastructure Insights, clique em **Start Free Trial**. O Data Infrastructure Insights guiará você pela criação do locatário da sua empresa, incluindo a seleção da região onde você deseja que seu locatário resida.

Please choose your AWS region.



Quando a criação do seu locatário estiver concluída, você poderá usar suas credenciais do BlueXP para fazer

login e iniciar seu teste gratuito de 30 dias do Insights de infraestrutura de dados. Durante esse teste, você pode explorar os recursos que o Data Infrastructure Insights tem a oferecer.

Durante a avaliação gratuita, você pode "[inicie a sua subscrição](#)" acessar o Data Infrastructure Insights a qualquer momento. Ao assinar, você pode usar os recursos do Data Infrastructure Insights com base na assinatura atual.

Inicie sessão e vá

Uma vez que seu locatário tenha sido criado, você pode simplesmente fazer login no Portal do NetApp BlueXP e clicar em **ir para informações de infraestrutura de dados**. Você será levado diretamente ao seu locatário do Data Infrastructure Insights.

Você também pode abrir um navegador diretamente no URL do locatário do Data Infrastructure Insights, por exemplo:

```
\https://<tenant-prefix>.c01.cloudinsights.netapp.com/
```

O URL também será incluído no e-mail de convite de cada usuário para acesso simples e marcação de livros. Se o usuário ainda não estiver conectado ao BlueXP, ele será solicitado a fazer login.



Os novos usuários ainda precisam se inscrever para acessar o BlueXP antes que possam acessar o URL do locatário.

Na primeira vez que você fizer login em um novo locatário, você será orientado através da configuração até "[comece a recolher dados](#)".

Terminar sessão

Para terminar sessão no Data Infrastructure Insights, clique no seu **Nome de utilizador** e selecione **Terminar sessão**. Você será levado de volta para a tela de login do BlueXP.



Fazer logout do Insights da infraestrutura de dados faz o logout do BlueXP. Você também será desconectado de outros serviços da NetApp Cloud que usam o login do BlueXP.

Tempo limite de inatividade

Por padrão, o BlueXP fará logout de um usuário se não houver atividade por seis horas (360 minutos). Independentemente da atividade, os usuários serão desconectados após sete dias.

Segurança

Segurança do Insights da infraestrutura de dados

A segurança de dados de produtos e clientes é de extrema importância na NetApp. O Data Infrastructure Insights segue as práticas recomendadas de segurança ao longo do ciclo de vida da versão para garantir que as informações e os dados do cliente estejam protegidos da melhor maneira possível.

Visão geral de segurança

Segurança física

A infraestrutura de produção do Data Infrastructure Insights é hospedada na Amazon Web Services (AWS). Os controles físicos e ambientais relacionados à segurança dos servidores de produção do Data Infrastructure Insights, que incluem edifícios, bem como fechaduras ou chaves usadas nas portas, são gerenciados pela AWS. De acordo com a AWS: "O acesso físico é controlado tanto no perímetro quanto no estabelecimento de pontos de entrada pela equipe de segurança profissional que utiliza vigilância por vídeo, sistemas de detecção de intrusão e outros meios eletrônicos. A equipe autorizada utiliza mecanismos de autenticação multifator para acessar andares do data center."

O Data Infrastructure Insights segue as práticas recomendadas do "[Modelo de responsabilidade compartilhada](#)" descrito pela AWS.

Segurança do produto

O Data Infrastructure Insights segue um ciclo de vida de desenvolvimento em linha com os princípios ágeis, permitindo-nos, assim, abordar quaisquer defeitos de software orientados para a segurança mais rapidamente, em comparação com metodologias de desenvolvimento de ciclo de lançamento mais longo. Usando metodologias de integração contínua, somos capazes de responder rapidamente às mudanças funcionais e de segurança. Os procedimentos e políticas de gerenciamento de mudanças definem quando e como as mudanças ocorrem e ajudam a manter a estabilidade do ambiente de produção. Quaisquer alterações com impactos são formalmente comunicadas, coordenadas, adequadamente revisadas e aprovadas antes de sua liberação no ambiente de produção.

Segurança da rede

O acesso à rede a recursos no ambiente Data Infrastructure Insights é controlado por firewalls baseados em host. Cada recurso (como um balanceador de carga ou instância de máquina virtual) tem um firewall baseado em host que restringe o tráfego de entrada apenas às portas necessárias para que esse recurso execute sua função.

O Data Infrastructure Insights usa vários mecanismos, incluindo serviços de detecção de intrusão para monitorar o ambiente de produção em busca de anomalias de segurança.

Avaliação de risco

A equipe Data Infrastructure Insights segue um processo formalizado de avaliação de risco para fornecer uma maneira sistemática e repetível de identificar e avaliar os riscos para que eles possam ser gerenciados adequadamente por meio de um Plano de tratamento de riscos.

Proteção de dados

O ambiente de produção Data Infrastructure Insights é configurado em uma infraestrutura altamente redundante, utilizando várias zonas de disponibilidade para todos os serviços e componentes. Além da utilização de uma infraestrutura de computação redundante e altamente disponível, o backup de dados críticos em intervalos regulares e as restaurações são testadas periodicamente. Políticas e procedimentos formais de backup minimizam o impacto das interrupções das atividades de negócios e protegem os processos de negócios contra os efeitos de falhas de sistemas de informação ou desastres e garantem sua retomada oportuna e adequada.

Autenticação e gerenciamento de acesso

Todo o acesso do cliente ao Data Infrastructure Insights é feito por meio de interações da interface do usuário do navegador por https. A autenticação é realizada através do serviço de terceiros 3rd, Auth0. A NetApp centralizou-se nisso como a camada de autenticação para todos os serviços de dados de nuvem.

O Data Infrastructure Insights segue as práticas recomendadas do setor, incluindo "menos privilégio" e "controle de acesso baseado em função", sobre o acesso lógico ao ambiente de produção do Data Infrastructure Insights. O acesso é controlado com base em necessidade estrita e só é concedido para pessoal autorizado selecionado usando mecanismos de autenticação multifator.

Coleta e proteção de dados do cliente

Todos os dados do cliente são criptografados em trânsito em redes públicas e criptografados em repouso. O Data Infrastructure Insights utiliza criptografia em vários pontos do sistema para proteger os dados dos clientes usando tecnologias que incluem Transport Layer Security (TLS) e o algoritmo AES-256 padrão do setor.

Desprovisionamento do cliente

As notificações por e-mail são enviadas em vários intervalos para informar o cliente que sua assinatura está expirando. Uma vez que a assinatura expirou, a IU é restrita e um período de carência começa para a coleta de dados. O cliente é então notificado por e-mail. As assinaturas de teste têm um período de carência de 14 dias e as contas de assinatura pagas têm um período de carência de 28 dias. Após o término do período de carência, o cliente é notificado por e-mail de que a conta será excluída em 2 dias. Um cliente pago também pode solicitar diretamente para estar fora do serviço.

Os locatários expirados e todos os dados associados do cliente são excluídos pela equipe de operações do Data Infrastructure Insights Operations (SRE) no final do período de carência ou mediante confirmação da solicitação do cliente para encerrar sua conta. Em ambos os casos, a equipe SRE executa uma chamada de API para excluir a conta. A chamada API exclui a instância do locatário e todos os dados do cliente. A exclusão do cliente é verificada chamando a mesma API e verificando se o status do locatário do cliente é "EXCLUÍDO".

Gerenciamento de incidentes de segurança

O Insights de infraestrutura de dados é integrado ao processo da equipe de resposta a incidentes de Segurança de Produtos (PSIRT) da NetApp para localizar, avaliar e resolver vulnerabilidades conhecidas. O PSIRT coleta informações de vulnerabilidades de vários canais, incluindo relatórios de clientes, engenharia interna e fontes amplamente reconhecidas, como o banco de dados CVE.

Se um problema for detectado pela equipe de engenharia do Data Infrastructure Insights, a equipe iniciará o processo PSIRT, avaliará e potencialmente corrigirá o problema.

Também é possível que um cliente ou pesquisador do Insights de infraestrutura de dados possa identificar um

problema de segurança com o produto Insights de infraestrutura de dados e relatar o problema ao suporte técnico ou diretamente à equipe de resposta a incidentes da NetApp. Nesses casos, a equipe de Data Infrastructure Insights iniciará o processo PSIRT, avaliará e potencialmente corrigirá o problema.

Teste de vulnerabilidade e penetração

O Data Infrastructure Insights segue as melhores práticas do setor e executa testes regulares de vulnerabilidade e penetração usando profissionais e empresas de segurança internas e externas.

Treinamento de conscientização sobre segurança

Todos os funcionários do Data Infrastructure Insights passam por treinamento de segurança, desenvolvido para funções individuais, para garantir que cada funcionário esteja equipado para lidar com os desafios específicos voltados à segurança de suas funções.

Conformidade

O Data Infrastructure Insights realiza auditorias e validações independentes de terceiros de sua segurança, processos e serviços, incluindo a conclusão da Auditoria SOC 2.

Consultores de Segurança da NetApp

Pode visualizar os avisos de segurança disponíveis do NetApp ["aqui"](#).

Informação e região

A NetApp leva a segurança das informações dos clientes muito a sério. Veja como e onde o Data Infrastructure Insights armazena suas informações.

Quais informações o Data Infrastructure Insights armazena?

O Data Infrastructure Insights armazena as seguintes informações:

- Dados de performance

Os dados de desempenho são dados de séries temporais que fornecem informações sobre o desempenho do dispositivo/fonte monitorado. Isso inclui, por exemplo, o número de iOS fornecido por um sistema de armazenamento, a taxa de transferência de uma porta FibreChannel, o número de páginas entregues por um servidor da Web, o tempo de resposta de um banco de dados e muito mais.

- Dados de inventário

Os dados de inventário consistem em metadados que descrevem o dispositivo/fonte monitorado e como ele é configurado. Isso inclui, por exemplo, versões de hardware e software instaladas, discos e LUNs em um sistema de armazenamento, núcleos de CPU, RAM e discos de uma máquina virtual, os espaços de tabela de um banco de dados, o número e tipo de portas em um switch SAN, nomes de diretório/arquivo (se o Storage Workload Security estiver ativado), etc.

- Dados de configuração

Isso resume os dados de configuração fornecidos pelo cliente usados para gerenciar o inventário e as operações do cliente, por exemplo, nomes de host ou endereços IP dos dispositivos monitorados, intervalos de polling, valores de tempo limite, etc.

- Segredos

Os segredos consistem nas credenciais usadas pela Unidade de aquisição do Data Infrastructure Insights para acessar dispositivos e serviços do cliente. Essas credenciais são criptografadas usando criptografia assimétrica forte e as chaves privadas são armazenadas somente nas unidades de aquisição e nunca saem do ambiente do cliente. Mesmo os SREs privilegiados do Insights de infraestrutura de dados não conseguem acessar segredos do cliente em texto simples devido a esse design.

- Dados funcionais

Esses são dados gerados como resultado do NetApp que fornece o Serviço de dados em nuvem, que informa a NetApp no desenvolvimento, implantação, operações, manutenção e proteção do Serviço de dados em nuvem. Os dados funcionais não contêm informações do Cliente ou informações pessoais.

- Dados de acesso do usuário

Informações de autenticação e acesso que permitem que o NetApp BlueXP se comunique com sites regionais de informações de infraestrutura de dados, incluindo dados relacionados à autorização do usuário.

- Dados do diretório do usuário de segurança do workload de armazenamento

Nos casos em que a funcionalidade de Segurança de carga de trabalho está ativada E o cliente optar por ativar o coletor do diretório de utilizadores, o sistema armazenará nomes de apresentação de utilizadores, endereços de correio eletrônico empresariais e outras informações recolhidas no ativo Directory.



Os dados do diretório do usuário referem-se às informações do diretório do usuário coletadas pelo coletor de dados do diretório do usuário do Workload Security, e não aos dados sobre os usuários do Data Infrastructure Insights/Workload Security.

Nenhum dado pessoal explícito é coletado de recursos de infraestrutura e serviços. As informações coletadas consistem apenas em métricas de performance, informações de configuração e metadados da infraestrutura, assim como muitos telefônicas dos fornecedores, incluindo suporte automático da NetApp e ActiveIQ. No entanto, dependendo das convenções de nomenclatura de um cliente, os dados para compartilhamentos, volumes, VMs, qtrees, aplicativos, etc. podem conter informações de identificação pessoal.

Se o Workload Security estiver ativado, o sistema também examinará os nomes de arquivos e diretórios em SMB ou outros compartilhamentos, que podem conter informações pessoalmente identificáveis. Quando os clientes ativam o Coletor do diretório de usuários de Segurança de carga de trabalho (que mapeia essencialmente os SIDs do Windows para nomes de usuário por meio do ativo Directory), o nome de exibição, o endereço de e-mail corporativo e quaisquer atributos adicionais selecionados serão coletados e armazenados pelo Data Infrastructure Insights.

Além disso, os logs de acesso ao Data Infrastructure Insights são mantidos e contêm os endereços IP e de e-mail dos usuários usados para fazer login no serviço.

Onde minhas informações são armazenadas?

O Data Infrastructure Insights armazena informações de acordo com a região em que seu ambiente é criado.

As seguintes informações são armazenadas na região do host:

- Informações de telemetria e de ativos/objetos, incluindo contadores e métricas de desempenho

- Informações da Unidade de aquisição
- Dados funcionais
- Faça auditoria de informações sobre as atividades do usuário dentro do Data Infrastructure Insights
- Informações sobre o ativo Directory de segurança da carga de trabalho
- Informações de auditoria de segurança de carga de trabalho

As informações a seguir residem nos Estados Unidos, independentemente da região que hospeda seu ambiente Data Infrastructure Insights:

- Informações do site do ambiente (às vezes chamado de "locatário"), como o proprietário do site/conta.
- Informações que permitem que o NetApp BlueXP se comunique com sites regionais de informações de infraestrutura de dados, incluindo qualquer coisa a ver com autorização do usuário.
- Informações relacionadas à relação entre o usuário do Data Infrastructure Insights e o locatário.

Regiões de acolhimento

As regiões de host incluem:

- EUA: US-East-1
- EMEA: eu-central-1
- APAC: ap-sudeste-2

Mais informações

Você pode ler mais sobre a privacidade e segurança do NetApp nos seguintes links:

- ["Centro de confiança"](#)
- ["Transferências de dados transfronteiriças"](#)
- ["Regras corporativas vinculativas"](#)
- ["Resposta a solicitações de dados de terceiros"](#)
- ["Princípios de Privacidade da NetApp"](#)

Ferramenta SecurityAdmin

O Data Infrastructure Insights inclui recursos de segurança que permitem que seu ambiente opere com segurança aprimorada. Os recursos incluem melhorias na criptografia, hash de senha e a capacidade de alterar senhas internas de usuário, bem como pares de chaves que criptografam e descriptografam senhas.

Para proteger dados confidenciais, o NetApp recomenda que você altere as chaves padrão e a senha do usuário *Acquisition* após uma instalação ou atualização.

As senhas criptografadas de origem de dados são armazenadas no Data Infrastructure Insights, que usa uma chave pública para criptografar senhas quando um usuário as insere em uma página de configuração de coletor de dados. O Data Infrastructure Insights não tem as chaves privadas necessárias para descriptografar as senhas do coletor de dados; somente as unidades de aquisição (AUS) têm a chave privada do coletor de dados necessária para descriptografar as senhas do coletor de dados.

Considerações sobre atualização e instalação

Quando o sistema Insight contiver configurações de segurança não predefinidas (ou seja, se tiver palavras-passe recodificadas), tem de efetuar uma cópia de segurança das suas configurações de segurança. Instalar um novo software ou, em alguns casos, atualizar o software, reverte o sistema para uma configuração de segurança padrão. Quando o sistema voltar para a configuração padrão, você deve restaurar a configuração não padrão para que o sistema funcione corretamente.

Gestão da segurança na unidade de aquisição

A ferramenta SecurityAdmin permite gerenciar opções de segurança para o Data Infrastructure Insights e é executada no sistema da unidade de aquisição. O gerenciamento de segurança inclui o gerenciamento de chaves e senhas, salvar e restaurar configurações de segurança que você cria ou restaura as configurações padrão.

Antes de começar

- Tem de ter admin Privileges no sistema AU para instalar o software da Unidade de aquisição (que inclui a ferramenta SecurityAdmin).
- Se você tiver usuários não administradores que posteriormente precisarão acessar a ferramenta SecurityAdmin, eles devem ser adicionados ao grupo *cisys*. O grupo *cisys* é criado durante a instalação da AU.

Após a instalação da AU, a ferramenta SecurityAdmin encontra-se no sistema da unidade de aquisição em qualquer uma destas localizações:

```
Windows - C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat  
Linux - /bin/oci-securityadmin.sh
```

Usando a ferramenta SecurityAdmin

Inicie a ferramenta SecurityAdmin no modo interativo (-i).



Recomenda-se usar a ferramenta SecurityAdmin no modo interativo, para evitar passar segredos na linha de comando, que pode ser capturada em logs.

São apresentadas as seguintes opções:

```
[root@ci-qa-xitij-cis2-285941inaw bin]# ./securityadmin -i
Select Action:

1 - Backup
2 - Restore
3 - Register / Update External Key Retrieval Script
4 - Rotate Encryption Keys
5 - Reset to Default Keys
6 - Change Truststore Password
7 - Change Keystore Password
8 - Encrypt Collector Password
9 - Exit

Enter your choice: █
```

1. Backup

Cria um arquivo zip de backup do Vault contendo todas as senhas e chaves e coloca o arquivo em um local especificado pelo usuário ou nos seguintes locais padrão:

```
Windows - C:\Program Files\SANscreen\backup\vault
Linux - /var/log/netapp/oci/backup/vault
```

Recomenda-se que os backups do Vault sejam mantidos seguros, pois incluem informações confidenciais.

2. Restaurar

Restaura o backup zip do Vault que foi criado. Uma vez restaurado, todas as senhas e chaves são revertidas para valores existentes no momento da criação do backup.

A restauração pode ser usada para sincronizar senhas e chaves em vários servidores, por exemplo, usando estas etapas: 1) alterar chaves de criptografia na AU. 2) criar um backup do cofre. 3) Restaurar o backup do Vault para cada um dos AUS.

3. Register / Update External Key Retrieval Script

Use um script externo para Registrar ou alterar as chaves de criptografia da AU usadas para criptografar ou descriptografar senhas de dispositivos.

Ao alterar as chaves de criptografia, você deve fazer backup da nova configuração de segurança para que possa restaurá-la após uma atualização ou instalação.

Nota esta opção só está disponível no Linux.

Ao usar seu próprio script de recuperação de chave com a ferramenta SecurityAdmin, tenha em mente o seguinte:

- O algoritmo suportado atual é RSA com um mínimo de 2048 bits.
- O script deve retornar as chaves privadas e públicas em texto simples. O script não deve retornar chaves privadas e públicas criptografadas.
- O script deve retornar conteúdo codificado em bruto (somente formato PEM).
- O script externo deve ter permissões *execute*.

4. **Rotate Encryption Keys** (rodar chaves de encriptação)

Gire suas chaves de criptografia (desRegistra chaves atuais e Registra novas chaves). Para usar uma chave de um sistema de gerenciamento de chaves externo, você deve especificar o ID da chave pública e o ID da chave privada.

5. * Redefinir para as chaves padrão*

Repõe a palavra-passe do utilizador de aquisição e as chaves de encriptação do utilizador de aquisição para valores predefinidos; os valores predefinidos são os fornecidos durante a instalação.

6. * Alterar senha de armazenamento de confiança*

Altere a senha do armazenamento de confiança.

7. **Altere a senha do Keystore**

Altere a senha do keystore.

8. **Encrypt Collector Password**

Encripte a palavra-passe do coletor de dados.

9. **Saída**

Saia da ferramenta SecurityAdmin.

Escolha a opção que deseja configurar e siga as instruções.

Especificando um usuário para executar a ferramenta

Se você estiver em um ambiente controlado e com consciência de segurança, talvez você não tenha o grupo *cisys*, mas ainda queira que usuários específicos executem a ferramenta SecurityAdmin.

Você pode conseguir isso instalando manualmente o software AU e especificando o usuário/grupo para quem deseja acessar.

- Usando a API, baixe o Instalador de CI para o sistema AU e descompacte-o.
 - Você precisará de um token de autorização única. Consulte a documentação do Swagger da API (*Admin > API Access* e selecione o link *API Documentation*) e localize a seção *GET /au/oneTimeToken* API.
 - Depois de ter o token, use a API `_GET /au/instaladores/` Você precisará fornecer a plataforma (Linux

ou Windows), bem como a versão do instalador.

- Copie o arquivo do instalador baixado para o sistema AU e descompacte-o.
- Navegue até a pasta que contém os arquivos e execute o instalador como root, especificando o usuário e o grupo:

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

Se o usuário e/ou grupo especificado não existir, eles serão criados. O usuário terá acesso à ferramenta SecurityAdmin.

Atualizando ou removendo proxy

A ferramenta SecurityAdmin pode ser usada para definir ou remover informações de proxy para a Unidade de aquisição executando a ferramenta com o parâmetro *-pr*:

```
[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.)
```

Por exemplo, para remover o proxy, execute este comando:

```
[root@ci-eng-linau bin]# ./securityadmin -pr -rp
Tem de reiniciar a Unidade de aquisição depois de executar o comando.
```

Para atualizar um proxy, o comando é

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

Recuperação de chave externa

Se você fornecer um script de shell UNIX, ele pode ser executado pela unidade de aquisição para recuperar a

chave privada e a **chave pública** do seu sistema de gerenciamento de chaves.

Para recuperar a chave, o Data Infrastructure Insights executará o script, passando dois parâmetros: *Key id* e *key type*. *Key id* pode ser usado para identificar a chave em seu sistema de gerenciamento de chaves. *Tipo de chave* é "pública" ou "privada". Quando o tipo de chave é "pública", o script deve retornar a chave pública. Quando o tipo de chave é "privado", a chave privada deve ser retornada.

Para enviar a chave de volta para a unidade de aquisição, o script deve imprimir a chave para a saída padrão. O script deve imprimir *only* a chave para a saída padrão; nenhum outro texto deve ser impresso na saída padrão. Uma vez que a chave solicitada é impressa na saída padrão, o script deve sair com um código de saída de 0; qualquer outro código de retorno é considerado um erro.

O script deve ser registrado na unidade de aquisição usando a ferramenta SecurityAdmin, que executará o script juntamente com a unidade de aquisição. O script deve ter permissão *read* e *execute* para o usuário root e "cisys". Se o script shell for modificado após o Registro, o script shell modificado deve ser re-registrado na unidade de aquisição.

parâmetro de entrada: id da chave	Identificador de chave usado para identificar a chave no sistema de gerenciamento de chaves dos clientes.
parâmetro de entrada: tipo de chave	público ou privado.
saída	A chave solicitada deve ser impressa na saída padrão. A chave RSA de 2048 bits é atualmente suportada. As chaves devem ser codificadas e impressas no seguinte formato - formato de chave privada - PEM, PKCS8 PrivateKeyInfo RFC 5958 formato de chave pública - PEM, X,509 subjectPublicKeyInfo RFC 5280 codificado POR DER
código de saída	Código de saída de zero para o sucesso. Todos os outros valores de saída são considerados falha.
permissões de script	O script deve ter permissão de leitura e execução para o usuário root e "cisys".
registros	As execuções de script são registradas. Os logs podem ser encontrados em - /var/log/NetApp/cloudinsights/securityadmin/securityadmin.log /var/log/NetApp/cloudinsights/acq/acq.log

Encriptar uma palavra-passe para utilização na API

A opção 8 permite criptografar uma senha, que você pode passar para um coletor de dados via API.

Inicie a ferramenta SecurityAdmin no modo interativo e selecione a opção 8: *Encrypt Password*.

```
securityadmin.sh -i
```

É-lhe pedido que introduza a palavra-passe que pretende encriptar. Observe que os caracteres digitados não são exibidos na tela. Digite novamente a senha quando solicitado.

Alternativamente, se você usar o comando em um script, em uma linha de comando use *securityadmin.sh* com o parâmetro "-enc", passando sua senha não criptografada:

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

A palavra-passe encriptada é apresentada no ecrã. Copie toda a cadeia, incluindo quaisquer símbolos à esquerda ou à direita.

```
[root@ci-eng-srivardh-learn bin]# securityadmin.sh -i
Select Action:

1 - Backup
2 - Restore
3 - Change Encryption Keys
4 - Reset to Default Keys
5 - Check for Default Encryption Keys
6 - Change Truststore Password
7 - Change Keystore Password
8 - Encrypt Password
9 - Exit

Enter your choice: 8
Please enter your password to encrypt:
Please confirm your password to encrypt:

Your Encrypted Password below

ciYJAMpdEncBsLQwF2gobbiERL4Jrwb7tLW0FYhu0dERGZUZ3L+uWfcCXdNSXTWr6SFuumwsWVFib3h78vnM0s6vM7G/2k1Bd8ggJiQ+tS/LZkmJ6XKgTdcf3LGn8UqzQy
Rn0v5jJ8Gip6nCysrt9dapsEiRVHrMJVr8btGYbb4Zoz62qudMfW9uQdm3qyzSKbIY0L0An89yDPC0kDkaXreyLfpju0G5UmeZz1KGCt0aBTggri/JIYyrr4w2ZLnG0w21
LGM59vor70GU0iKZYabLd+7LpsdCCBi1eF86BCj2RkxX0of891sHN+E7zTvZEofdGVWepc7b/HNah5XiXgV1viCZ/WqkyQ==
```

Para enviar a senha criptografada para um coletor de dados, você pode usar a API de coleta de dados. O Swagger para esta API pode ser encontrado em **Admin > API Access** e clique no link "API Documentation". Selecione o tipo de API "coleta de dados". No título *data_collection.data_collector*, escolha a API */Collector/datasources* POST para este exemplo.

The screenshot shows the Swagger UI for the `data_collection.data_collector` API. The endpoint is `POST /collector/datasources` with the description "Create a data collector".

Parameters:

Name	Description
<code>preEncrypted</code> boolean (query)	Optional, defaults to false. If <code>preEncrypted</code> query parameter set to true, directs server to treat all passed secret values as already encrypted. Default value : false

The `preEncrypted` parameter is currently set to `false`.

Request body: required, type `application/json`.

Example Value:

```
{
  "acquisitionUnit": {
    "additionalProp1": "string",
    "additionalProp2": "string"
```

Se você definir a opção *preEncrypted* como *true*, qualquer senha que você passar pelo comando API será tratada como **já criptografada**; a API não irá criptografar novamente a(s) senha(s). Ao criar sua API, basta colar a senha criptografada anteriormente no local apropriado.

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":
            "J8bepjwz9oNknfs6mcqzb3zuEThZQp1VyTk+1wE05gWwmmj1u0CB688nfOnB1xnIBVsAWyLmORxFAw
            vcDCvGbTraqp/+nT0k94LO8Z7Q04I5KqhHfTvINGU54S4IVLWiMIFj8kSU4RhMvNNNq5Tarz0gJZhWR+
            4RoNF+84R/uFFGwKebIrwfHxWZZMoW7pEJ2kzLFBtBzx2mUvRP0kn6AFbyS4+DM2YTPQkSk3W2Gzc
            +nfPDDyH8Tq6AM5WsVCKqnZAa2ZIY1FxMkKT7iFt5oiYnl93ka7OrQlmM9QAYpoyw/JT0nXHDuf683uE
            K32yn9CgxNGXy5NcNzRurdFNb5w=="
        }
      },
      {
        "id": "storageperformance",
        "displayName": "Array Performance",
        "isMandatory": false,
        "attributes": {
          "password": "this will not be encrypted on the server side"
        }
      }
    ]
  },
  "acquisitionUnit": {
    "id": "1"
  }
}
```


Como começar

Tutoriais de recursos

O Data Infrastructure Insights é carregado com recursos úteis que permitem localizar dados de forma rápida e fácil, solucionar problemas e fornecer insights sobre seu ambiente corporativo. Encontre dados facilmente com consultas avançadas, visualize dados em painéis e envie alertas por e-mail para os limites de dados definidos.

O Data Infrastructure Insights inclui vários tutoriais em vídeo para ajudá-lo a entender esses recursos e implementar melhor suas estratégias de insights de negócios. Todos os usuários que têm acesso ao seu locatário do Data Infrastructure Insights podem aproveitar esses tutoriais.

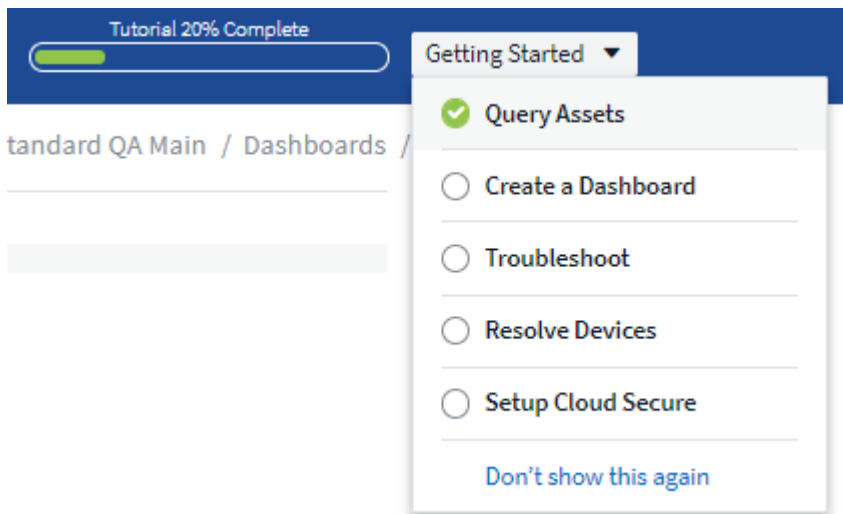
Introdução

Assista a um breve tutorial explicando como o Data Infrastructure Insights funciona.


► <https://docs.netapp.com/pt-br/data-infrastructure-insights//media/howTo.mp4> (video)

Lista de verificação e tutoriais em vídeo

A **Lista de verificação de arranque** apresentada no seu site Data Infrastructure Insights contém uma lista de várias tarefas e conceitos úteis. A seleção de um item na lista de verificação leva você à página de Insights de infraestrutura de dados apropriada para esse conceito. Por exemplo, clicar no item *criar um Dashboard* abre a página Data Infrastructure Insights **Dashboards**.



Na parte superior da página há um link para um tutorial em vídeo mostrando como criar um painel. Você pode ver o vídeo quantas vezes quiser até clicar no botão *Get It! Não mostrar novamente este link* para esse vídeo. O vídeo estará disponível toda vez que você for para a página Dashboards, até que você o rejeite.

 [Learn How to Create a Dashboard](#) [Watch Video](#) [Got it! Don't show this again.](#)

Depois de assistir ao vídeo pelo menos uma vez, o item *Create a Dashboard* na lista de verificação é

desmarcado, indicando que você concluiu o tutorial. Você pode então prosseguir para o próximo tutorial.



Você pode ver os tutoriais em qualquer ordem que você gosta, quantas vezes quiser até ser demitido.

A lista de verificação está em falta

A lista de verificação de arranque é apresentada no seu site até clicar no link *não mostrar novamente* na parte inferior da lista de verificação. Mesmo depois de descartar a lista de verificação, os tutoriais ainda estão disponíveis em cada página apropriada do Data Infrastructure Insights até que você ignore cada um da barra de cabeçalho da mensagem.

Veja os tutoriais

A consultar dados

▶ <https://docs.netapp.com/pt-br/data-infrastructure-insights//media/Queries.mp4> (video)

Criando um Dashboard

▶ <https://docs.netapp.com/pt-br/data-infrastructure-insights//media/Dashboards.mp4> (video)

Solução de problemas

▶ <https://docs.netapp.com/pt-br/data-infrastructure-insights//media/Troubleshooting.mp4> (video)

Resolver dispositivos

▶ https://docs.netapp.com/pt-br/data-infrastructure-insights//media/AHR_small.mp4 (video)

Coleta de dados

Começando a coletar dados

Depois de se inscrever no Data Infrastructure Insights e fazer login no seu ambiente pela primeira vez, você será guiado pelas etapas a seguir para começar a coletar e gerenciar dados.

Os coletores de dados descobrem informações de suas fontes de dados, como dispositivos de armazenamento, switches de rede e máquinas virtuais. As informações recolhidas são utilizadas para análise, validação, monitorização e resolução de problemas.

O Data Infrastructure Insights tem três tipos de coletores de dados disponíveis:

- Infraestrutura (dispositivos de armazenamento, switches de rede, infraestrutura de computação)
- Sistemas operacionais (como VMware ou Windows)
- Serviços (como Kafka)

Selecione seu primeiro coletor de dados entre os fornecedores e modelos compatíveis disponíveis. Você pode facilmente adicionar coletores de dados adicionais mais tarde.

Instale uma unidade de aquisição

Se você selecionou um coletor de dados *Infrastructure*, uma Unidade de aquisição será necessária para injetar dados no Data Infrastructure Insights. Terá de transferir e instalar o software da Unidade de aquisição num servidor ou VM no centro de dados a partir do qual irá recolher. Uma única unidade de aquisição pode ser usada para vários coletores de dados.



ONTAP Data
Management
Software

Install Acquisition Unit

Cloud Insights collects device data via one or more Acquisition Units installed on local servers. Each Acquisition Unit can host multiple Data Collectors, which send device metrics to Cloud Insights for analysis.

What Operating System or Platform Are You Using?

Linux

[Linux Versions Supported](#) ⓘ

[Production Best Practices](#) ⓘ

Installation Instructions

[Need Help?](#)

1 [Copy Installer Snippet](#)

This snippet has a unique key valid for 24 hours for this Acquisition Unit only.

[+ Reveal Installer Snippet](#)

2 Paste the snippet into a bash shell to run the installer.

3 Waiting for Acquisition Unit to connect...

- Siga o "instruções" apresentado para instalar a sua unidade de aquisição. Assim que o software da unidade de aquisição estiver instalado, o botão continuar é apresentado e pode avançar para o passo seguinte.

3 [Continue](#) **New acquisition unit detected!**

Pode configurar unidades de aquisição adicionais mais tarde, se necessário. Por exemplo, você pode querer que diferentes unidades de aquisição colem informações de data centers em diferentes regiões.

Configure o coletor de dados - infraestrutura

Para coletores de dados *Infrastructure*, você será solicitado a preencher os campos de coletor de dados apresentados:

- Dê ao coletor de dados um nome único e significativo.
- Insira as credenciais (nome de usuário e senha) para se conectar ao dispositivo, conforme apropriado.
- Preencha quaisquer outros campos obrigatórios nas seções *Configuration* e *Advanced Configuration*.
- Clique em **Add Collector** para salvar o coletor de dados.

Você será capaz de configurar coletores de dados adicionais mais tarde.

Configure o Data Collector - sistemas operacionais e Serviços

Sistema operativo:

Para coletores de dados *sistema operacional*, escolha uma plataforma (Linux, Windows) para instalar um Data Infrastructure Insights Agent. Você deve ter pelo menos um agente para coletar dados dos Serviços. O agente também coleta dados do próprio host, para uso no Data Infrastructure Insights. Estes dados são categorizados como dados "Node" em widgets, etc.

- Abra uma janela de terminal ou comando no host ou VM do agente e cole o comando exibido para instalar o agente.
- Quando a instalação estiver concluída, clique em **Complete Setup**.

Serviços:

Para coletores de dados *Service*, clique em um bloco para abrir a página de instruções para esse serviço.

- Escolha uma plataforma e uma chave de acesso ao agente.
- Se você não tiver um agente instalado nessa plataforma, siga as instruções para instalar o agente.
- Clique em **continuar** para abrir a página de instruções do coletor de dados.
- Siga as instruções para configurar o coletor de dados.
- Quando a configuração estiver concluída, clique em **Complete Setup**.

Adicione painéis

Dependendo do tipo de coletor de dados inicial que você selecionou para configurar (armazenamento, switch, etc.), um ou mais painéis relevantes serão importados. Por exemplo, se você configurou um coletor de dados de armazenamento, um conjunto de painéis relacionados ao armazenamento será importado e um será definido como sua Página inicial do Data Infrastructure Insights. Pode alterar a página inicial a partir da lista **painéis > Mostrar todos os painéis**.

Você pode importar painéis adicionais mais tarde "[crie o seu próprio](#)" ou .

Isso é tudo o que há para ele

Depois de concluir o processo de configuração inicial, seu ambiente começará a coletar dados.

Se o processo de configuração inicial for interrompido (por exemplo, se você fechar a janela do navegador), você precisará seguir os passos manualmente:

- Escolha um Data Collector
- Instale um Agente ou Unidade de aquisição, se solicitado
- Configure o coletor de dados

Definições úteis

As definições a seguir podem ser úteis quando se fala sobre coletores de dados ou recursos do Data Infrastructure Insights:

- Ciclo de vida do coletor: Um coletor pertencerá a um dos seguintes estados em seu ciclo de vida:
 - **Preview**: Disponível em uma capacidade limitada ou para um público limitado. "[Recursos de](#)

visualização" Espera-se que os coletores de dados se tornem GA após o período de pré-visualização. Os períodos de visualização variam de acordo com o público ou a funcionalidade.

- **GA:** Um recurso ou coletor de dados que geralmente está disponível para todos os clientes, com base no Edition ou no conjunto de recursos.
- **Deprecated:** Aplica-se a coletores de dados que são, ou são esperados para se tornar, não mais funcionalmente sustentáveis. Os coletores de dados obsoletos são frequentemente substituídos por coletores de dados mais recentes e funcionalmente atualizados.
- **Deleted:** Um coletor de dados que foi removido e não está mais disponível.
- **Unidade de aquisição:** Um computador dedicado à hospedagem de coletores de dados, normalmente uma Máquina Virtual. Esse computador normalmente está localizado no mesmo data center/VPC que os itens monitorados.
- **Fonte de dados:** Um módulo para comunicação com uma pilha de hardware ou software. Ele consiste em uma configuração e código que são executados no computador da AU para se comunicar com o dispositivo.

Requisitos da Unidade de aquisição

Você deve instalar uma Unidade de aquisição (AU) para adquirir informações de seus coletores de dados de infraestrutura (storage, VM, porta, EC2, etc.). Antes de instalar a Unidade de aquisição, você deve garantir que o locatário atenda aos requisitos do sistema operacional, CPU, memória e espaço em disco.

Requisitos

Componente	Requisito Linux	Requisitos do Windows
Sistema operacional	Um computador executando uma versão licenciada de um dos seguintes: * CentOS (64 7,9 9,1 9,4 15 SP5 22,04-bit): 64 8,1 9,4 15 18,04 a 8,1 7,2 8,10 9,0 15 SP2 20,04, 7,5 a 8,4, Stream 64, Stream 15,1 * AlmaLinux 15,5 e 9,4 * Debian (64-bit): 9 e 10 * OpenSUSE Leap 9 a 9,3 * Oracle Enterprise Linux (8-bit): 8,1 a 7,9, 7,9 a 8,8 * Red Hat Enterprise Linux (7,2 Recomenda-se um servidor dedicado. Se você estiver executando com o SELinux, é recomendável executar os seguintes comandos no sistema de unidade de aquisição: Sudo semanage fcontext -a -t usr_t "/opt/NetApp/cloudinsights(/.*)?" sudo restorecon -R /opt/NetApp/cloudinsights	Um computador com uma versão licenciada de um dos seguintes: * Microsoft Windows 10 64-bit * Microsoft Windows Server 2012 * Microsoft Windows Server 2012 R2 * Microsoft Windows Server 2016 * Microsoft Windows Server 2019 * Microsoft Windows Server 2022 * Microsoft Windows 11 este computador não deve estar executando nenhum outro software de nível de aplicativo. Recomenda-se um servidor dedicado.
CPU	2 núcleos de CPU	O mesmo
Memória	8 GB DE RAM	O mesmo

Espaço disponível em disco	50 GB (100 GB recomendados) para Linux, o espaço em disco deve ser alocado desta maneira: /Opt/NetApp 10 GB (20 GB para ambientes grandes) /var/log/NetApp 40 GB (80 GB para ambientes grandes) /tmp pelo menos 1 GB disponíveis durante a instalação	50 GB
Rede	É necessária uma ligação Ethernet de 100 Mbps/1 Gbps, endereço IP estático e conectividade de porta 80 ou 443 (saída) da Unidade de aquisição para *.cloudinsights.NetApp.com ou o seu inquilino de informações de infra-estrutura de dados (isto é, <a href="https://<tenant_id>.C01.cloudsights.NetApp.com">https://<tenant_id>.C01.cloudsights.NetApp.com). Para obter os requisitos entre a Unidade de aquisição e cada Coletor de dados, consulte as instruções para a "Coletor de dados". Se a sua organização exigir o uso de proxy para acesso à Internet, talvez seja necessário entender o comportamento de proxy da sua organização e buscar certas exceções para que o Data Infrastructure Insights funcione. Por exemplo, sua organização bloqueia o acesso por padrão e só permite o acesso a sites/domínios específicos por exceção? Se assim for, você precisará adicionar o seguinte domínio à lista de exceções: *.cloudinsights.NetApp.com para obter mais informações, leia sobre Proxies " Aqui (Linux) " ou " Aqui (Windows) ".	O mesmo
Permissões	Permissões sudo no servidor da Unidade de aquisição. /tmp deve ser montado com recursos exec.	Permissões de administrador no servidor da Unidade de aquisição
Verificação de vírus		Durante a instalação, você deve desativar completamente todos os scanners de vírus. Após a instalação, os caminhos utilizados pelo software da Unidade de aquisição têm de ser excluídos da verificação de vírus.

Recomendações adicionais

- Para uma auditoria precisa e relatórios de dados, é altamente recomendável sincronizar o tempo na máquina da unidade de aquisição usando **Network Time Protocol (NTP)** ou **Simple Network Time Protocol (SNTP)**.

Em relação ao dimensionamento

Você pode começar a usar uma Unidade de aquisição de dados Infrastructure Insights com apenas 8GB GB de memória e 50GB GB de espaço em disco. No entanto, para ambientes maiores, você deve fazer as seguintes perguntas:

Você espera:

- Descubra mais de 2500 máquinas virtuais ou 10 clusters ONTAP grandes (> 2 nós), Symmetrix ou matrizes HDS/HPE VSP/XP nesta Unidade de aquisição?
- Implantar 75 ou mais coletores de dados totais nesta Unidade de aquisição?

Para cada resposta "Sim" acima, recomenda-se adicionar 8 GB de memória e 50 GB de espaço em disco à AU. Então, por exemplo, se você respondeu "Sim" para ambos, você deve implantar um sistema de memória 24GB com 150GBMB ou mais de espaço em disco. No Linux, o espaço em disco a ser adicionado ao local do log.

Para perguntas adicionais sobre o dimensionamento, entre em Contato com o suporte da NetApp.

Configurar unidades de aquisição

O Data Infrastructure Insights coleta dados do dispositivo usando uma ou mais unidades de aquisição instaladas em servidores locais. Cada Unidade de aquisição pode hospedar vários coletores de dados, que enviam métricas de dispositivo para o Data Infrastructure Insights para análise.

Este tópico descreve como adicionar unidades de aquisição e descreve as etapas adicionais necessárias quando seu ambiente usa um proxy.



Para uma auditoria precisa e relatórios de dados, é altamente recomendável sincronizar o tempo na máquina da unidade de aquisição usando **Network Time Protocol (NTP)** ou **Simple Network Time Protocol (SNTP)**.

Leia sobre segurança do Data Infrastructure Insights ["aqui"](#).

Adicionando uma Unidade de aquisição Linux

Antes de começar

- Se o sistema estiver usando um proxy, você deverá definir as variáveis de ambiente proxy antes que a unidade de aquisição seja instalada. Para obter mais informações, [Configurando variáveis de ambiente proxy](#) consulte .

Etapas para a instalação da Unidade de aquisição do Linux

1. Faça login como Administrador ou proprietário de conta no seu ambiente Data Infrastructure Insights.
2. Clique em **Observability > Collectors > Acquisition Units > Acquisition Unit**

O sistema exibe a caixa de diálogo *Install Acquisition Unit*. Escolha Linux.




ONTAP Data
Management
Software

Install Acquisition Unit

Cloud Insights collects device data via one or more Acquisition Units installed on local servers. Each Acquisition Unit can host multiple Data Collectors, which send device metrics to Cloud Insights for analysis.

What Operating System or Platform Are You Using?

 Linux

Linux Versions Supported  Production Best Practices 

Installation Instructions

[Need Help?](#)

1 Copy Installer Snippet

This snippet has a unique key valid for 24 hours for this Acquisition Unit only.

 Reveal Installer Snippet

2 Paste the snippet into a bash shell to run the installer.

3 Waiting for Acquisition Unit to connect...

1. Verifique se o servidor ou VM que hospeda a Unidade de aquisição atende aos requisitos de sistema recomendados.
2. Verifique se o servidor está executando uma versão suportada do Linux. Clique em *as versões suportadas* (*i*) para obter uma lista de versões suportadas.
3. Copie o snippet de comando Installation na caixa de diálogo para uma janela de terminal no servidor ou na VM que hospedará a unidade de aquisição.
4. Cole e execute o comando no shell Bash.

Depois de terminar

- Clique em **Observability > Collectors > Acquisition Units** (observabilidade > coletores > unidades de aquisição) para verificar o estado das unidades de aquisição.
- Pode aceder aos registos da Unidade de aquisição em `/var/log/NetApp/cloudinsights/acq/acq.log`
- Use o seguinte script para controlar a Unidade de aquisição:
 - `cloudinsights-service.sh` (parar, iniciar, reiniciar, verificar o estado)
- Use o seguinte script para desinstalar a Unidade de aquisição:
 - `cloudinsights-uninstall.sh`

Configurando variáveis de ambiente proxy

Para ambientes que usam um proxy, você deve definir as variáveis de ambiente proxy antes de adicionar a Unidade de aquisição. As instruções para configurar o proxy são fornecidas na caixa de diálogo *Adicionar unidade de aquisição*.

1. Clique em *have a Proxy Server?*
2. Copie os comandos para um editor de texto e defina suas variáveis de proxy conforme necessário.

Nota: Esteja ciente de restrições em caracteres especiais nos campos de nome de usuário e senha do proxy: '%' e '!' são permitidos no campo de nome de usuário. ':', '%' e '!' são permitidos no campo de senha.

3. Execute o comando editado em um terminal usando o shell Bash.
4. Instale o software da unidade de aquisição.

Configuração do proxy

A Unidade de aquisição usa autenticação de 2 vias/mútua para se conectar ao servidor Data Infrastructure Insights. O certificado de cliente deve ser passado para o servidor Data Infrastructure Insights para ser autenticado. Para isso, o proxy deve ser configurado para encaminhar a solicitação https para o servidor Data Infrastructure Insights sem descriptografar os dados.

A maneira mais simples de fazer isso é especificar a configuração curinga em seu proxy/firewall para se comunicar com o Data Infrastructure Insights, por exemplo:

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



O uso de um asterisco (*) para curinga é comum, mas sua configuração de proxy/firewall pode usar um formato diferente. Verifique com a documentação do proxy para garantir a especificação correta do curinga em seu ambiente.

Mais informações sobre a configuração do proxy podem ser encontradas no NetApp "[Knowledgebase](#)".

Exibindo URLs de proxy

Você pode visualizar seus URLs de endpoint proxy clicando no link **Configurações de proxy** ao escolher um coletor de dados durante a integração ou no link em *Configurações de proxy* na página **Ajuda > suporte**. Uma tabela como a seguinte é exibida.

Hostname	Port	Protocol	Methods	Endpoint URL Purpose
qtrjkso.proxyserver.cloudinsights-dev.netapp.com	443	https	GET, POST, PATCH, PUT, DELETE	Tenant
00b1100.1234.abcd.12bc.a1b2c3ef56a7.proxyserver.cloudinsights-dev.netapp.com	443	https	GET, POST, PATCH, PUT, DELETE	Acquisition Unit Ingestion
aulogin.proxyserver.cloudinsights-dev.netapp.com	443	https	GET, POST, PATCH, PUT, DELETE	Acquisition Unit Authentication
portal.proxy.cloud.netapp.com	443	https	GET, POST, PATCH, PUT, DELETE	Gateway

Se você tiver o Workload Security no locatário, os URLs de endpoint configurados também serão exibidos nesta lista.

Adicionar uma Unidade de aquisição do Windows

Passos para a instalação da unidade de aquisição do Windows

1. Inicie sessão no servidor/VM da Unidade de aquisição como um utilizador com permissões de

Administrador.


2. Nesse servidor, abra uma janela do navegador e faça login no seu ambiente Data Infrastructure Insights como Administrador ou proprietário da conta.
3. Clique em **observabilidade > coletores > unidades de aquisição > Unidade de aquisição** .

O sistema exibe a caixa de diálogo *Install Acquisition Unit*. Escolha Windows.

Install Acquisition Unit

Cloud Insights collects device data via one or more Acquisition Units installed on local servers. Each Acquisition Unit can host multiple Data Collectors, which send device metrics to Cloud Insights for analysis.

What Operating System or Platform Are You Using?

 Windows ▼

Windows Versions Supported ⓘ

Production Best Practices ⓘ

Installation Instructions

[Need Help?](#)

1 [Download Installer \(Windows 64-bit\)](#)

2 [Copy Access Key](#)

This access key is a unique key valid for 24 hours for this Acquisition Unit only.

[+ Reveal Access Key](#)

3 **Paste access key into installer when prompted.**

4 **Please ensure you have copied and pasted the access key into the installer.**

[+ Have a Proxy Server?](#)

1. Verifique se o servidor ou VM que hospeda a Unidade de aquisição atende aos requisitos de sistema recomendados.
2. Verifique se o servidor está executando uma versão suportada do Windows. Clique em *as versões suportadas (i)* para obter uma lista de versões suportadas.
3. Clique no botão **Download Installer (Windows 64-bit)**.
4. Copie a chave de acesso. Você precisará disso durante a instalação.
5. No servidor/VM da Unidade de aquisição, execute o instalador transferido.
6. Cole a chave de acesso no assistente de instalação quando solicitado.
7. Durante a instalação, você terá a oportunidade de fornecer suas configurações de servidor proxy.

Depois de terminar

- Clique em * > observabilidade > coletores > unidades de aquisição* para verificar o estado das unidades de aquisição.
- Pode aceder ao registo da unidade de aquisição no <install dir>/Cloud Insights/Unidade de aquisição/log/acq.log
- Use o script a seguir para parar, iniciar, reiniciar ou verificar o status da Unidade de aquisição:

```
cloudinsights-service.sh
```

Configuração do proxy

A Unidade de aquisição usa autenticação de 2 vias/mútua para se conectar ao servidor Data Infrastructure Insights. O certificado de cliente deve ser passado para o servidor Data Infrastructure Insights para ser autenticado. Para isso, o proxy deve ser configurado para encaminhar a solicitação https para o servidor Data Infrastructure Insights sem descriptografar os dados.

A maneira mais simples de fazer isso é especificar a configuração curinga em seu proxy/firewall para se comunicar com o Data Infrastructure Insights, por exemplo:

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



O uso de um asterisco (*) para curinga é comum, mas sua configuração de proxy/firewall pode usar um formato diferente. Verifique com a documentação do proxy para garantir a especificação correta do curinga em seu ambiente.

Mais informações sobre a configuração do proxy podem ser encontradas no NetApp "[Knowledgebase](#)".

Exibindo URLs de proxy

Você pode visualizar seus URLs de endpoint proxy clicando no link **Configurações de proxy** ao escolher um coletor de dados durante a integração ou no link em *Configurações de proxy* na página **Ajuda > suporte**. Uma tabela como a seguinte é exibida.

Proxy Settings					×
<p>i If your organization requires proxy usage for internet access, you need to understand your organization's proxy behavior and seek certain exceptions for Cloud Insights to work. The simplest way is to add the following domains to the exception list:</p>					
Hostname	Port	Protocol	Methods	Endpoint URL Purpose	
qtrjks0.proxyserver.cloudinsights-dev.netapp.com	443	https	GET, POST, PATCH, PUT, DELETE	Tenant	
00b1100.1234.abcd.12bc.a1b2c3ef56a7.proxyserver.cloudinsights-dev.netapp.com	443	https	GET, POST, PATCH, PUT, DELETE	Acquisition Unit Ingestion	
aulogin.proxyserver.cloudinsights-dev.netapp.com	443	https	GET, POST, PATCH, PUT, DELETE	Acquisition Unit Authentication	
portal.proxy.cloud.netapp.com	443	https	GET, POST, PATCH, PUT, DELETE	Gateway	

[Close](#)

Se você tiver o Workload Security no locatário, os URLs de endpoint configurados também serão exibidos nesta lista.

Desinstalar uma unidade de aquisição

Para desinstalar o software da unidade de aquisição, faça o seguinte:

Windows:

Se estiver a desinstalar uma unidade de aquisição **Windows**:

1. No servidor/VM da Unidade de aquisição, abra o Painel de Controle e escolha **Desinstalar um Programa**. Selecione o programa Data Infrastructure Insights Acquisition Unit para remoção.
2. Clique em Desinstalar e siga as instruções.

Linux:

Se você estiver desinstalando uma unidade de aquisição **Linux**:

1. No servidor/VM da Unidade de aquisição, execute o seguinte comando:

```
sudo cloudinsights-uninstall.sh -p  
. Para obter ajuda com a desinstalação, execute:
```

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

Windows e Linux:

Após desinstalação da AU:

1. Em Data Infrastructure Insights, vá para **Observability > Collectors** e **selecione a guia *Acquisition Units** (unidades de aquisição).
2. Clique no botão Opções à direita da Unidade de aquisição que deseja desinstalar e selecione *Delete*. Só pode eliminar uma unidade de aquisição se não houver coletores de dados atribuídos a ela.



Não é possível eliminar uma unidade de aquisição (AU) que tenha coletores de dados ligados a ela. Mova todos os coletores de dados da AU para outra AU (edite o coletor e simplesmente selecione uma AU diferente) antes de excluir a AU original.

Uma unidade de aquisição com uma estrela próxima a ela está sendo usada para resolução do dispositivo. Antes de remover esta AU, tem de selecionar outra AU para utilizar para a Resolução do dispositivo. Passe o Mouse sobre uma AU diferente e abra o menu "três pontos" para selecionar "usar para resolução do dispositivo".

cbc-cloudinsights-au  

10.65.57.18

This Acquisition Unit is used for Device Resolution.

Reinstalar uma unidade de aquisição

Para reinstalar uma Unidade de aquisição no mesmo servidor/VM, siga estes passos:

Antes de começar

Você deve ter uma Unidade de aquisição temporária configurada em um servidor/VM separado antes de reinstalar uma Unidade de aquisição.

Passos

1. Inicie sessão no servidor/VM da unidade de aquisição e desinstale o software AU.
2. Faça login no seu ambiente Data Infrastructure Insights e acesse **Observability > Collectors**.
3. Para cada coletor de dados, clique no menu Opções à direita e selecione *Editar*. Atribua o coletor de dados à Unidade de aquisição temporária e clique em **Save**.

Você também pode selecionar vários coletores de dados do mesmo tipo e clicar no botão **ações em massa**. Escolha *Edit* e atribua os coletores de dados à Unidade de aquisição temporária.

4. Depois de todos os coletores de dados terem sido movidos para a Unidade de aquisição temporária, vá para **Observability > Collectors** e selecione a guia **Acquisition Units** (unidades de aquisição).
5. Clique no botão Opções à direita da unidade de aquisição que deseja reinstalar e selecione *Delete*. Só pode eliminar uma unidade de aquisição se não houver coletores de dados atribuídos a ela.
6. Agora você pode reinstalar o software da Unidade de aquisição no servidor/VM original. Clique em * Unidade de aquisição* e siga as instruções acima para instalar a Unidade de aquisição.
7. Uma vez que a unidade de aquisição tenha sido reinstalada, atribua os coletores de dados à unidade de aquisição.

Ver detalhes AU

A página de detalhes da unidade de aquisição (AU) fornece detalhes úteis para uma UA, bem como informações para ajudar na resolução de problemas. A página de detalhes da AU contém as seguintes seções:

- Uma seção **summary** que mostra o seguinte:
 - **Nome e IP** da Unidade de aquisição
 - Conexão atual **Status** da AU
 - **Último relatório** tempo de enquete bem-sucedido do coletor de dados
 - O **sistema operacional** da máquina AU
 - Qualquer **Nota** atual para a UA. Utilize este campo para introduzir um comentário para a UA. O campo exibe a nota adicionada mais recentemente.
- Uma tabela dos **coletores de dados** da UA mostrando, para cada coletor de dados:
 - **Nome** - clique neste link para detalhar a página de detalhes do coletor de dados com informações adicionais
 - **Status** - informações de sucesso ou erro
 - **Tipo** - Fornecedor/modelo
 - **Endereço IP** do coletor de dados
 - Nível de **impacto** atual
 - **Último tempo adquirido** - quando o coletor de dados foi analisado com sucesso pela última vez

Acquisition Unit Summary

Name xp-linux	Connection Status OK - Need Help?	Operating System Linux	Note
IP 10.197.120.145	Last Reported 2 minutes ago		

Data Collectors (3) + Data Collector Bulk Actions Filter...

<input type="checkbox"/>	Name ↑	Status	Type	IP	Impact	Last Acquired	
<input type="checkbox"/>	foo	! Inventory failed	NetApp Data ONTAP 7-Mode	foo	Low	Never	⋮
<input type="checkbox"/>	xp-cisco	All successful	Cisco MDS Fabric Switches	10.197.136.66		2 minutes ago	⋮
<input type="checkbox"/>	xpcdot26	All successful	NetApp ONTAP Data Management Software	10.197.136.26		8 minutes ago	⋮

Para cada coletor de dados, você pode clicar no menu "três pontos" para clonar, Editar, Poll ou Excluir o coletor de dados. Você também pode selecionar vários coletores de dados nesta lista para executar ações em massa neles.

Para reiniciar a Unidade de aquisição, clique no botão **Restart** na parte superior da página. Solte este botão para tentar **Restaurar conexão** para a AU em caso de problema de conexão.

Configurando um agente para coletar dados (Windows/Linux)

O Data Infrastructure Insights usa "**Telegraf**" como seu agente para a coleta de dados de integração. Telegraf é um agente de servidor baseado em plugins que pode ser usado para coletar e relatar métricas, eventos e logs. Plugins de entrada são usados para coletar as informações desejadas no agente acessando o sistema/os diretamente, chamando APIs de terceiros ou ouvindo fluxos configurados (ou seja, Kafka, statsD, etc). Os plugins de saída são usados para enviar as métricas, eventos e logs coletados do agente para o Data Infrastructure Insights.

A versão atual do Telegraf para Data Infrastructure Insights é **1.24.0**.

Para obter informações sobre como instalar no Kubernetes, consulte a "[Operador de monitoramento do Kubernetes do NetApp](#)" página.



Para uma auditoria precisa e relatórios de dados, é altamente recomendável sincronizar a hora na máquina do agente usando **Network Time Protocol (NTP)** ou **Simple Network Time Protocol (SNTP)**.



Se você quiser verificar os arquivos de instalação antes de instalar o Agente, consulte a seção abaixo em [Verificando somas de verificação](#).

Instalando um agente

Se você estiver instalando um coletor de dados de serviço e ainda não tiver configurado um agente, será solicitado que você instale primeiro um agente para o sistema operacional apropriado. Este tópico fornece instruções para instalar o agente Telegraf nos seguintes sistemas operacionais:

- [Windows](#)
- [RHEL e CentOS](#)
- [Ubuntu e Debian](#)

Para instalar um agente, independentemente da plataforma que você estiver usando, primeiro faça o seguinte:

1. Faça login no host que você usará para seu agente.
2. Faça login no seu ambiente Data Infrastructure Insights e navegue até **Observability > Collectors**.
3. Clique em * Data Collector* e escolha um coletor de dados para instalar.
4. Escolha a plataforma apropriada para o seu host (Windows, Linux)
5. Siga as etapas restantes para cada plataforma.



Depois de instalar um agente em um host, você não precisa instalar um agente novamente nesse host.



Depois de instalar um agente em um servidor/VM, o Data Infrastructure Insights coleta métricas desse sistema, além de coletar de qualquer coletor de dados que você configurar. Essas métricas são reunidas como "[Métricas de "nó"](#)".



Se você estiver usando um proxy, leia as instruções de proxy da sua plataforma antes de instalar o agente Telegraf.

Locais de registro

As mensagens de log do Telegraf são redirecionadas do stdout para os seguintes arquivos de log são padrão:

- RHEL/CentOS: `/Var/log/telegraf/telegraf.log`
- Ubuntu/Debian: `/Var/log/telegraf/telegraf.log`
- Windows: `C: Arquivos de programas / telegraf / telegraf.log`

Windows

Pré-requisitos:

- O PowerShell deve ser instalado
- Se você estiver atrás de um proxy, siga as instruções na seção **Configurando o suporte Proxy para Windows**.

Configurando o suporte Proxy para Windows



Se o seu ambiente usar um proxy, leia esta seção antes de instalar.



As etapas abaixo descrevem as ações necessárias para definir as variáveis de ambiente `http_proxy/https_proxy`. Para alguns ambientes proxy, os usuários também podem precisar definir a variável `no_proxy environment`.

Para sistemas que residem atrás de um proxy, execute o seguinte para definir a(s) variável(s) de ambiente `https_proxy` e/ou `http_proxy` **ANTES** para instalar o agente Telegraf:

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

Instalando o agente



Install Agent

Quickly setup an agent in your environment and immediately start monitoring data

Select existing API Access Token or create a new one

KEY1 (...Zqlk0c)

+ API Access Token

Installation Instructions

[Need Help?](#)

1 Copy Agent Installer Snippet

This snippet has a unique key and is valid for 24 hours. Already have an agent in your environment? [View Troubleshooting](#)

Reveal Agent Installer Snippet

2 Open a PowerShell window as administrator and paste the snippet

3 Complete Setup

Etapas para instalar o agente no Windows:

1. Escolha uma chave de acesso ao agente.
2. Copie o bloco de comandos da caixa de diálogo de instalação do agente. Você pode clicar no ícone da área de transferência para copiar rapidamente o comando para a área de transferência.
3. Abra uma janela do PowerShell
4. Cole o comando na janela do PowerShell e pressione Enter.
5. O comando fará o download do instalador do agente apropriado, instalá-lo e definirá uma configuração padrão. Quando terminar, ele reiniciará o serviço do agente. O comando tem uma chave única e é válido por 24 horas.
6. Clique em **Finish** ou **Continue**

Depois que o agente estiver instalado, você poderá usar os seguintes comandos para iniciar/parar o serviço:

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

Desinstalar o agente

Para desinstalar o agente no Windows, faça o seguinte em uma janela do PowerShell:

1. Parar e eliminar o serviço Telegraf:

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

2. Remova o certificado da trustore:

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

3. Exclua a pasta *C:/Program Files/telegraf* para remover os arquivos binários, logs e configurações

4. Remova a chave *SYSTEM_CurrentControlSet/Services/EventLog/Application/telegraf* do Registro

Atualizando o agente

Para atualizar o agente telegraf, faça o seguinte:

1. Parar e eliminar o serviço telegraf:

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

2. Exclua a chave *SYSTEM_CurrentControlSet/Services/EventLog/Application/telegraf* do Registro

3. Excluir arquivos *_C*

4. Excluir arquivos *_C*

5. ["Instale o novo agente"](#).

RHEL e CentOS

Pré-requisitos:

- Os seguintes comandos devem estar disponíveis: Curl, sudo, ping, sha256sum, openssl e dmidecode
- Se você estiver atrás de um proxy, siga as instruções na seção **Configurando o suporte Proxy para RHEL/CentOS**.

Configurando o suporte de proxy para RHEL/CentOS



Se o seu ambiente usar um proxy, leia esta seção antes de instalar.



As etapas abaixo descrevem as ações necessárias para definir as variáveis de ambiente *http_proxy/https_proxy*. Para alguns ambientes proxy, os usuários também podem precisar definir a variável *no_proxy environment*.

Para sistemas que residem atrás de um proxy, execute as seguintes etapas **ANTES** para instalar o agente

Telegraf:

1. Defina a(s) variável(s) de ambiente `https_proxy` e/ou `http_proxy` para o usuário atual:

```
export https_proxy=<proxy_server>:<proxy_port>
. Crie _etc/default/telegraf_ e insira definições para as variáveis
_https_proxy_ e/ou _http_proxy_:
```

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

Instalando o agente



Install Agent

Quickly setup an agent in your environment and immediately start monitoring data

Select existing API Access Token or create a new one

default_ingestion_api_key1 (...xEKVyK)

+ API Access Token

Production Best Practices ?

Installation Instructions

[Need Help?](#)

- 1 For environments operating behind a proxy server, follow the instructions to [configure proxy support to install and run Telegraf](#).
- 2 [Copy Agent Installer Snippet](#)
This snippet has a unique key and is valid for 24 hours. Already have an agent in your environment? [View Troubleshooting](#)
[Reveal Agent Installer Snippet](#)
- 3 Open a terminal window and paste the snippet in a Bash shell (requires `curl`, `sudo`, `ping`, `sha256sum`, and `dmidecode`).
- 4 [Complete Setup](#)

Etapas para instalar o agente no RHEL/CentOS:

1. Escolha uma chave de acesso ao agente.
2. Copie o bloco de comandos da caixa de diálogo de instalação do agente. Você pode clicar no ícone da área de transferência para copiar rapidamente o comando para a área de transferência.
3. Abra uma janela Bash
4. Cole o comando na janela Bash e pressione Enter.
5. O comando fará o download do instalador do agente apropriado, instalá-lo e definirá uma configuração padrão. Quando terminar, ele reiniciará o serviço do agente. O comando tem uma chave única e é válido por 24 horas.
6. Clique em **Finish** ou **Continue**

Depois que o agente estiver instalado, você poderá usar os seguintes comandos para iniciar/parar o serviço:

Se o sistema operacional estiver usando systemd (CentOS 7 e RHEL 7):

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

Se o sistema operacional não estiver usando systemd (CentOS 7 e RHEL 7):

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

Desinstalar o agente

Para desinstalar o agente no RHEL/CentOS, em um terminal Bash, faça o seguinte:

1. Pare o serviço Telegraf:

```
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. Remova o agente Telegraf:

```
yum remove telegraf
. Remova qualquer configuração ou arquivos de log que possam ser
deixados para trás:
```

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

Atualizando o agente

Para atualizar o agente telegraf, faça o seguinte:

1. Pare o serviço telegraf:

```
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. Remova o agente telegraf anterior:

```
yum remove telegraf
. xref:{relative_path}#rhel-and-centos["Instale o novo agente"].
```

Ubuntu e Debian

Pré-requisitos:

- Os seguintes comandos devem estar disponíveis: Curl, sudo, ping, sha256sum, openssl e dmidecode
- Se você está atrás de um proxy, você deve seguir as instruções na seção **Configurando o suporte Proxy para Ubuntu/Debian**.

Configurando o suporte Proxy para Ubuntu/Debian



Se o seu ambiente usar um proxy, leia esta seção antes de instalar.



As etapas abaixo descrevem as ações necessárias para definir as variáveis de ambiente *http_proxy/https_proxy*. Para alguns ambientes proxy, os usuários também podem precisar definir a variável *no_proxy environment*.

Para sistemas que residem atrás de um proxy, execute as seguintes etapas **ANTES** para instalar o agente Telegraf:

1. Defina a(s) variável(s) de ambiente *https_proxy* e/ou *http_proxy* para o usuário atual:

```
export https_proxy=<proxy_server>:<proxy_port>
. Crie /etc/default/telegraf e insira definições para as variáveis
_https_proxy_ e/ou _http_proxy_:
```

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

Instalando o agente

Install Agent

Quickly setup an agent in your environment and immediately start monitoring data

Select existing API Access Token or create a new one

default_ingestion_api_key1 (...xEKVyK) ▼

+ API Access Token

Production Best Practices ?

Installation Instructions

[Need Help?](#)

1 For environments operating behind a proxy server, follow the instructions to [configure proxy support to install and run Telegraf](#).

2 [Copy Agent Installer Snippet](#)

This snippet has a unique key and is valid for 24 hours. Already have an agent in your environment? [View Troubleshooting](#)

Reveal Agent Installer Snippet

3 Open a terminal window and paste the snippet in a Bash shell (requires curl, sudo, ping, sha256sum, and dmidecode).

4 [Complete Setup](#)

Passos para instalar o agente no Debian ou Ubuntu:

1. Escolha uma chave de acesso ao agente.
2. Copie o bloco de comandos da caixa de diálogo de instalação do agente. Você pode clicar no ícone da área de transferência para copiar rapidamente o comando para a área de transferência.
3. Abra uma janela Bash
4. Cole o comando na janela Bash e pressione Enter.
5. O comando fará o download do instalador do agente apropriado, instalá-lo e definirá uma configuração padrão. Quando terminar, ele reiniciará o serviço do agente. O comando tem uma chave única e é válido por 24 horas.
6. Clique em **Finish** ou **Continue**

Depois que o agente estiver instalado, você poderá usar os seguintes comandos para iniciar/parar o serviço:

Se o seu sistema operacional estiver usando systemd:

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

Se o seu sistema operacional não estiver usando systemd:

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

Desinstalar o agente

Para desinstalar o agente no Ubuntu/Debian, em um terminal Bash, execute o seguinte:

1. Pare o serviço Telegraf:

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

2. Remova o agente Telegraf:

```
dpkg -r telegraf
. Remova qualquer configuração ou arquivos de log que possam ser
deixados para trás:
```

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

Atualizando o agente

Para atualizar o agente telegraf, faça o seguinte:

1. Pare o serviço telegraf:

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

2. Remova o agente telegraf anterior:

```
dpkg -r telegraf
. xref:{relative_path}#ubuntu-and-debian["Instale o novo agente"].
```

Verificando somas de verificação

O instalador do agente Data Infrastructure Insights executa verificações de integridade, mas alguns usuários podem querer executar suas próprias verificações antes de instalar ou aplicar artefatos baixados. Isso pode ser feito baixando o instalador e gerando uma soma de verificação para o pacote baixado e comparando a soma de verificação com o valor mostrado nas instruções de instalação.

Baixe o pacote de instalação sem instalar

Para executar uma operação somente de download (em oposição ao download-e-install padrão), os usuários podem editar o comando de instalação do agente obtido a partir da interface do usuário e remover a opção "install".

Siga estes passos:

1. Copie o snippet do Agent Installer como indicado.
2. Em vez de colar o snippet em uma janela de comando, cole-o em um editor de texto.
3. Remova o comando "--install" (Linux) ou "-install" (Windows).
4. Copie o comando inteiro do editor de texto.
5. Agora cole-o em sua janela de comando (em um diretório de trabalho) e execute-o.

Não Windows (estes exemplos são para o Kubernetes; os nomes de script reais podem variar):

- Transferir e instalar (predefinição):

```
installerName=cloudinsights-kubernetes.sh ... && sudo -E -H  
./$installerName --download --install  
* Apenas transferência:
```

```
installerName=cloudinsights-kubernetes.sh ... && sudo -E -H  
./$installerName --download
```

Windows:

- Transferir e instalar (predefinição):

```
!$(($installerName=".\\cloudinsights-windows.ps1") ... -and  
$(&$installerName -download -install)  
* Apenas transferência:
```

```
!$(($installerName=".\\cloudinsights-windows.ps1") ... -and  
$(&$installerName -download)
```

O comando somente download fará o download de todos os artefatos necessários do Data Infrastructure Insights para o diretório de trabalho. Os artefactos incluem, mas podem não estar limitados a:

- um script de instalação
- um arquivo de ambiente
- Ficheiros YAML
- um arquivo de checksum (terminando em sha256.signed ou sha256.ps1)

O script de instalação, o arquivo de ambiente e os arquivos YAML podem ser verificados usando a inspeção visual.

Gerar valor de soma de verificação

Para gerar o valor da soma de verificação, execute o seguinte comando para sua plataforma apropriada:

- RHEL/Ubuntu:

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

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

Verifique a soma de verificação

Extraia o checksum esperado do arquivo checksum

- Não janelas:

```
openssl smime -verify -in telegraf*.sha256.signed -CAfile  
netapp_cert.pem -purpose any -nosigs -noverify  
* Windows:
```

```
(Get-Content telegraf.zip.sha256.ps1 -First 1).ToUpper()
```

Instale o pacote transferido

Uma vez que todos os artefatos tenham sido verificados satisfatoriamente, a instalação do agente pode ser iniciada executando:

Não janelas:

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

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

Solução de problemas

Algumas coisas para tentar se você encontrar problemas para configurar um agente:

Problema:	Tente isto:
Depois de configurar um novo plugin e reiniciar o Telegraf, o Telegraf não consegue iniciar. Os logs indicam que um erro semelhante ao seguinte: "[telegraf] erro ao executar agente: Erro ao carregar arquivo de configuração /etc/telegraf/telegraf.d/cloudinsights-default.conf: Plugin outputs.http: Line <linenumber>: Configuration especificou os campos ["use_system_proxy"], mas eles não foram usados"	A versão instalada do Telegraf está desatualizada. Siga as etapas nesta página para Atualizar o Agente para sua plataforma apropriada.
Eu executei o script do instalador em uma instalação antiga e agora o agente não está enviando dados	Desinstale o agente telegraf e execute novamente o script de instalação. Siga as etapas Upgrade the Agent nesta página para sua plataforma apropriada.
Já instalei um agente usando o Data Infrastructure Insights	Se você já tiver instalado um agente em seu host/VM, não será necessário instalar o agente novamente. Nesse caso, basta escolher a Plataforma e chave apropriadas na tela Instalação do Agente e clicar em continuar ou concluir .
Já tenho um agente instalado, mas não usando o instalador Data Infrastructure Insights	Remova o agente anterior e execute a instalação do Data Infrastructure Insights Agent para garantir as configurações padrão adequadas do arquivo de configuração. Quando terminar, clique em continuar ou concluir .

Informações adicionais podem ser encontradas na "[Suporte](#)" página ou no "[Matriz de suporte do Data Collector](#)".

Configurando coletores de dados

Você configura os coletores de dados em seu ambiente Data Infrastructure Insights para coletar dados de dispositivos no data center.

Antes de começar

- Tem de ter configurado uma Unidade de aquisição antes de poder começar a recolher dados.
- Você precisa de credenciais para os dispositivos a partir dos quais você está coletando dados.
- Endereços de rede do dispositivo, informações de conta e senhas são necessários para todos os dispositivos dos quais você está coletando dados.

Passos

1. No menu Data Infrastructure Insights, clique em **observabilidade > coletores**

O sistema exibe os coletores de dados disponíveis organizados pelo fornecedor.

2. Clique em * Coletor* e selecione o coletor de dados a configurar.

Na caixa de diálogo, pode configurar o coletor de dados e adicionar uma unidade de aquisição.

3. Introduza um nome para o coletor de dados.

4. Clique em **Configuração avançada** para adicionar campos de configuração adicionais. (Nem todos os

coletores de dados exigem configuração avançada.)

5. Clique em **Configuração de teste** para verificar se o coletor de dados está configurado corretamente.
6. Clique em **Add Collector** para salvar a configuração e adicionar o coletor de dados ao seu locatário do Data Infrastructure Insights.

Pode levar até dois períodos de enquete antes que os dados do serviço sejam exibidos em painéis ou disponíveis para consulta.

- 1st pesquisa de inventário: imediatamente
- pesquisa de dados de desempenho 1st para estabelecer uma linha de base: imediatamente após a pesquisa de inventário
- enquete de desempenho 2nd: dentro de 15 segundos após a conclusão da enquete de desempenho 1st

A polling então prossegue de acordo com os intervalos de enquete de inventário e desempenho configurados.

Determinando o status de aquisição do coletor de dados

Como os coletores de dados são a principal fonte de informações do Data Infrastructure Insights, é imperativo garantir que eles permaneçam em um estado em execução.

O status do coletor de dados é exibido no canto superior direito de qualquer página de ativo como a mensagem "adquirido N minutos atrás", onde N indica o tempo de aquisição mais recente do(s) coletor(es) de dados do ativo. A hora/data de aquisição também é apresentada.

Ao clicar na mensagem, é apresentada uma tabela com o nome do coletor de dados, o estado e o último tempo de aquisição bem-sucedido. Se você estiver conectado como Administrador, clicar no link do nome do coletor de dados na tabela o levará à página de detalhes desse coletor de dados.

Gerenciamento de coletores de dados configurados

A página Installed Data Collectors (coletores de dados instalados) fornece acesso aos coletores de dados que foram configurados para Data Infrastructure Insights. Você pode usar esta página para modificar coletores de dados existentes.

Passos

1. No menu Data Infrastructure Insights, clique em **observabilidade > coletores**

É apresentado o ecrã Available Data Collectors (coletores de dados disponíveis).

2. Clique em **Installed Data Collectors**

É apresentada uma lista de todos os coletores de dados instalados. A lista fornece o nome do coletor, o status, o endereço IP que o coletor está acessando e quando os dados foram adquiridos pela última vez a partir do dispositivo A. A ação que pode ser executada nesta tela inclui:

- Controlar a polling
- Alterar credenciais do coletor de dados
- Clonar coletores de dados

Controlando a polling do coletor de dados

Depois de fazer uma alteração em um coletor de dados, você pode querer que ele pesquise imediatamente para verificar suas alterações, ou você pode querer adiar a coleta de dados em um coletor de dados por um, três ou cinco dias enquanto você trabalha em um problema.

Passos

1. No menu Data Infrastructure Insights, clique em **observabilidade > coletores**
2. Clique em **Installed Data Collectors**
3. Marque a caixa de seleção à esquerda do Coletor de dados que deseja alterar
4. Clique em **ações em massa** e selecione a ação de polling que deseja executar.

As ações em massa podem ser executadas simultaneamente em múltiplos coletores de dados. Selecione os coletores de dados e escolha a ação a ser executada no menu **Bulk Action**.

Editando informações do coletor de dados

Você pode editar as informações de configuração do coletor de dados existentes.

Para editar um único coletor de dados:

1. No menu Data Infrastructure Insights, clique em **observabilidade > coletores** para abrir a lista de coletores de dados instalados.
2. No menu de opções à direita do coletor de dados que você deseja modificar, clique em **Editar**.

A caixa de diálogo Editar Coletor é aberta.

3. Digite as alterações e clique em **Configuração de teste** para testar a nova configuração ou clique em **Salvar** para salvar a configuração.

Você também pode editar vários coletores de dados:

1. Selecione a caixa de verificação à esquerda de cada coletor de dados que pretende alterar.
2. Clique no botão **ações em massa** e escolha **Editar** para abrir a caixa de diálogo Editar coletor de dados.
3. Modifique os campos como acima.



Os coletores de dados selecionados devem ser do mesmo fornecedor e modelo e residir na mesma Unidade de aquisição.

Ao editar vários coletores de dados, o campo Nome do Coletor de dados mostra "Misto" e não pode ser editado. Outros campos, como nome de usuário e senha, mostram "Misto" e podem ser editados. Os campos que compartilham o mesmo valor entre os coletores de dados selecionados mostram os valores atuais e podem ser editados.

Ao editar vários coletores de dados, o botão **Configuração de teste** não está disponível.

Clonar coletores de dados

Usando a instalação de clone, você pode adicionar rapidamente uma fonte de dados com as mesmas credenciais e atributos de outra fonte de dados. A clonagem permite configurar facilmente várias instâncias do mesmo tipo de dispositivo.

Passos

1. No menu Data Infrastructure Insights, clique em **observabilidade > coletores**.
2. Clique em **Installed Data Collectors**.
3. Clique na caixa de verificação à esquerda do coletor de dados que pretende copiar.
4. No menu de opções à direita do coletor de dados selecionado, clique em **Clone**.

A caixa de diálogo Clone Data Collector é exibida.

5. Introduza novas informações nos campos obrigatórios.
6. Clique em **Salvar**.

Depois de terminar

A operação clone copia todos os outros atributos e configurações para criar o novo coletor de dados.

Realizar ações em massa em coletores de dados

Você pode editar simultaneamente algumas informações para vários coletores de dados. Esse recurso permite que você inicie uma enquete, adie a polling e retome a polling em vários coletores de dados. Além disso, você pode excluir vários coletores de dados.

Passos

1. No menu Data Infrastructure Insights, clique em **observabilidade > coletores**
2. Clique em **Installed Data Collectors**
3. Clique na caixa de verificação à esquerda dos coletores de dados que pretende modificar.
4. No menu de opções à direita, clique na opção que deseja executar.

Depois de terminar

A operação selecionada é realizada nos coletores de dados. Quando você escolheu excluir coletores de dados, uma caixa de diálogo é exibida exigindo que você ajuste a ação.

Pesquisando um coletor de dados com falha

Se um coletor de dados tiver uma mensagem de falha e um impacto Alto ou Médio, você precisará pesquisar esse problema usando a página de resumo do coletor de dados com suas informações vinculadas.

Siga as etapas a seguir para determinar a causa dos coletores de dados com falha. As mensagens de falha do coletor de dados são exibidas no menu **Admin** e na página **Installed Data Collectors**.

Passos

1. Clique em **Admin > coletores de dados > coletores de dados instalados**.
2. Clique no Nome vinculado do coletor de dados com falha para abrir a página Resumo.
3. Na página Resumo, verifique a área Comentários para ler quaisquer notas que possam ter sido deixadas por outro engenheiro que também possa estar investigando essa falha.
4. Anote todas as mensagens de desempenho.
5. Mova o ponteiro do Mouse sobre os segmentos do gráfico da linha de tempo do evento para exibir informações adicionais.

6. Selecione uma mensagem de erro para um dispositivo e exibida abaixo da linha do tempo do evento e clique no ícone Detalhes do erro que é exibido à direita da mensagem.

Os detalhes do erro incluem o texto da mensagem de erro, causas mais prováveis, informações em uso e sugestões do que pode ser tentado para corrigir o problema.

7. Na área dispositivos reportados por este coletor de dados, você pode filtrar a lista para exibir apenas os dispositivos de interesse, e você pode clicar no **Nome** vinculado de um dispositivo para exibir a página de ativos desse dispositivo.
8. Quando você retornar à página de resumo do coletor de dados, marque a área **Mostrar alterações recentes** na parte inferior da página para ver se as alterações recentes poderiam ter causado o problema.

Importar a partir da Galeria do Dashboard

O Data Infrastructure Insights fornece uma série de painéis recomendados para fornecer insights de negócios sobre seus dados. Cada painel contém widgets projetados para ajudar a responder a uma pergunta específica ou resolver um problema específico relevante para os dados que estão sendo coletados no seu local.

Para importar um painel da galeria, faça o seguinte:

1. Selecione **painéis > painéis**
2. Clique em * na Galeria*

Uma lista de **painéis recomendados** é exibida. Cada painel é nomeado com uma pergunta específica que o painel pode ajudá-lo a resolver. Os painéis estão disponíveis para ajudar a responder perguntas sobre diferentes tipos de objetos, incluindo AWS, NetApp, storage, VMware e outros

3. Selecione um ou mais painéis da lista e clique em **Adicionar painéis**. Esses painéis agora são exibidos na lista de painéis.

Além dos painéis recomendados, você também pode optar por importar **painéis adicionais** que não sejam relevantes para seus dados atuais. Por exemplo, se você não tiver coletores de dados de armazenamento atualmente instalados, mas estiver planejando configurar alguns no futuro, ainda poderá optar por importar os painéis relevantes para o armazenamento. Esses painéis estarão disponíveis para exibição, mas podem não mostrar nenhum dado relevante até que pelo menos um coletor de dados de armazenamento esteja configurado.

A importação a partir da galeria do painel está disponível para usuários com função Administrador ou proprietário da conta.

Contas de usuário e funções

O Data Infrastructure Insights oferece até quatro funções de conta de usuário: Proprietário de conta, Administrador, Usuário e convidado. Cada conta recebe níveis de permissão específicos, conforme indicado na tabela abaixo. Os usuários são **"convidado"** para o Data Infrastructure Insights e recebem uma função específica ou podem fazer login **"Autorização de logon único (SSO)"** com uma função padrão. A autorização SSO está disponível como um recurso no Data Infrastructure Insights Premium Edition.

Níveis de permissão

Você usa uma conta que tem Privileges de administrador para criar ou modificar contas de usuário. A cada conta de usuário é atribuída uma função para cada recurso Data Infrastructure Insights dos seguintes níveis de permissão.

Função	Observabilidade	Segurança da carga de trabalho	Relatórios	Administrador
Proprietário da conta	O mesmo que Administrador	O mesmo que Administrador	O mesmo que Administrador	O mesmo que o Administrador, bem como gerenciar autenticação SSO e configuração de Federação de identidade. Também pode atribuir proprietários adicionais.
Administrador	Pode executar todas as funções de observabilidade, bem como o gerenciamento de coletores de dados.	Pode executar todas as funções de Segurança, incluindo as de Alertas, Forensics, coletores de dados, políticas de resposta automatizadas e tokens de API para Segurança. Um Administrador também pode convidar outros usuários, mas só pode atribuir funções de Segurança.	Pode executar todas as funções de usuário/autor, incluindo o gerenciamento de tokens de API de relatórios, bem como todas as tarefas administrativas, como configuração de relatórios, e o desligamento e reinicialização de tarefas de relatório. Um administrador também pode convidar outros usuários, mas só pode atribuir funções de relatórios.	Pode convidar outros usuários, mas só pode atribuir funções de observabilidade. Pode exibir, mas não modificar a configuração SSO. Pode criar e gerenciar tokens de acesso à API. Pode visualizar informações de auditoria. Pode visualizar informações de subscrição, utilização e histórico. Pode gerenciar listas de destinatários de notificação de alerta global e notificação de assinatura.
Utilizador	Pode visualizar e modificar dashboards, consultas, alertas, anotações, regras de anotação e aplicativos, além de gerenciar a resolução do dispositivo.	Pode visualizar e gerir Alertas e visualizar Forensics. A função de usuário pode alterar o status de alerta, adicionar uma nota, tirar snapshots manualmente e gerenciar restringir o acesso do usuário.	Pode executar todas as funções de convidado/consumidor, bem como criar e gerenciar relatórios e painéis.	Não disponível

Função	Observabilidade	Segurança da carga de trabalho	Relatórios	Administrador
Convidado	Tem acesso somente leitura a páginas de ativos, painéis, alertas e pode exibir e executar consultas.	Pode visualizar Alertas e Forensics. A função convidado não pode alterar o status de alerta, adicionar uma nota, tirar snapshots manualmente ou restringir o acesso do usuário.	Pode visualizar, programar e executar relatórios e definir preferências pessoais, como as de idiomas e fusos horários. Os convidados/consumidores não podem criar relatórios ou executar tarefas administrativas.	Não disponível

A prática recomendada é limitar o número de usuários com permissões de Administrador. O maior número de contas deve ser contas de usuário ou convidado.

Permissões do Data Infrastructure Insights por função de usuário

A tabela a seguir mostra as permissões do Data Infrastructure Insights concedidas a cada função de usuário.

Recurso	Administrador/proprietário da conta	Utilizador	Convidado
Unidades de aquisição: Adicionar/Modificar/Eliminar	Y	N	N
Alertas*: Criar/Modificar/Excluir	Y	Y	N
Alertas*: Visualizar	Y	Y	Y
Regras de anotação: Criar/Executar/Modificar/Eliminar	Y	Y	N
Anotações: Criar/Modificar/atribuir/Ver/Remover/Eliminar	Y	Y	N
Acesso à API*: Criar/Renomear/Desativar/revogar	Y	N	N
Aplicações: Criar/Visualizar/Modificar/Eliminar	Y	Y	N
Páginas de ativos: Modificar	Y	Y	N
Páginas de ativos: Exibir	Y	Y	Y
Auditoria: Vista	Y	N	N

Custo de nuvem	Y	N	N
Segurança	Y	N	N
Painéis: Criar/Modificar/Excluir	Y	Y	N
Painéis: Exibir	Y	Y	Y
Coletores de dados: Adicionar/Modificar/Poll/Excluir	Y	N	N
Notificações: Vista	Y	Y	Y
Notificações: Modificar	Y	N	N
Consultas: Criar/Modificar/Excluir	Y	Y	N
Consultas: Exibir/Executar	Y	Y	Y
Resolução do dispositivo	Y	Y	N
Relatórios*: Exibir/Executar	Y	Y	Y
Relatórios*: Criar/Modificar/Excluir/Agendar	Y	Y	N
Subscrição: Visualizar/Modificar	Y	N	N
Gerenciamento de usuários: Convidar/Adicionar/Modificar/desativar	Y	N	N

*Requer Premium Edition

Criando contas convidando usuários

A criação de uma nova conta de usuário é obtida através do BlueXP . Um usuário pode responder ao convite enviado por e-mail, mas se o usuário não tiver uma conta no BlueXP , o usuário precisa se inscrever no BlueXP para que ele possa aceitar o convite.

Antes de começar

- O nome de usuário é o endereço de e-mail do convite.
- Entenda as funções de usuário que você estará atribuindo.
- As senhas são definidas pelo usuário durante o processo de inscrição.

Passos

1. Faça login no Data Infrastructure Insights
2. No menu, clique em **Admin > User Management**

É apresentado o ecrã User Management (Gestão de utilizadores). O ecrã contém uma lista de todas as

contas do sistema.

3. Clique em * Usuário*

É apresentado o ecrã **convidar utilizador**.

4. Insira um endereço de e-mail ou vários endereços para convites.

Observação: quando você insere vários endereços, todos eles são criados com a mesma função. Você só pode definir vários usuários para a mesma função.

5. Selecione a função do usuário para cada recurso do Data Infrastructure Insights.



Os recursos e funções que você pode escolher dependem de quais recursos você tem acesso em sua função de administrador específica. Por exemplo, se você tiver a função Admin apenas para relatórios, poderá atribuir usuários a qualquer função no Relatório, mas não poderá atribuir funções para observabilidade ou Segurança.

Invite Users [X]

You can invite people to join by sending them an invitation link. Inviting users is the easiest way to get your team to collaborate. Invitations expire after 14 days

test@net.com [X]

Monitor & Optimize Role
Guest [v]

Cloud Secure Role
Administrator [v]

[Cancel] [Invite]

6. Clique em **convidar**

O convite é enviado ao usuário. Os usuários terão 14 dias para aceitar o convite. Assim que um usuário aceitar o convite, ele será levado para o Portal de nuvem da NetApp, onde se inscreverá usando o endereço de e-mail do convite. Se eles já tiverem uma conta para esse endereço de e-mail, podem simplesmente fazer login e acessar seu ambiente Data Infrastructure Insights.

Modificando a função de um usuário existente

Para modificar a função de um usuário existente, incluindo adicioná-lo como um **proprietário de conta secundária**, siga estas etapas.

1. Clique em **Admin > User Management**. O ecrã apresenta uma lista de todas as contas do sistema.
2. Clique no nome de utilizador da conta que pretende alterar.
3. Modifique a função do usuário em cada conjunto de recursos do Data Infrastructure Insights, conforme necessário.
4. Clique em *Save changes*.

Para atribuir um proprietário de conta secundário

Você deve estar logado como proprietário de uma conta para observabilidade, a fim de atribuir a função de proprietário de conta a outro usuário.

1. Clique em **Admin > User Management**.
2. Clique no nome de utilizador da conta que pretende alterar.
3. Na caixa de diálogo Usuário, clique em **Assign as Owner** (atribuir como proprietário).
4. Salve as alterações.

Daniel ✕

Email	Last Login
user.name@netapp.com	a year ago

[Learn about the permissions provided by each role](#) 🔗

Owner Role

Monitor & Optimize Role

Cloud Secure Role

Você pode ter tantos proprietários de contas quanto desejar, mas a melhor prática é limitar a função de proprietário a apenas selecionar pessoas.

Eliminar utilizadores

Um usuário com a função Administrador pode excluir um usuário (por exemplo, alguém não mais com a empresa) clicando no nome do usuário e clicando em *Excluir usuário* na caixa de diálogo. O usuário será removido do ambiente Data Infrastructure Insights.

Observe que quaisquer painéis, consultas, etc. criados pelo usuário permanecerão disponíveis no ambiente Data Infrastructure Insights mesmo depois que o usuário for removido.

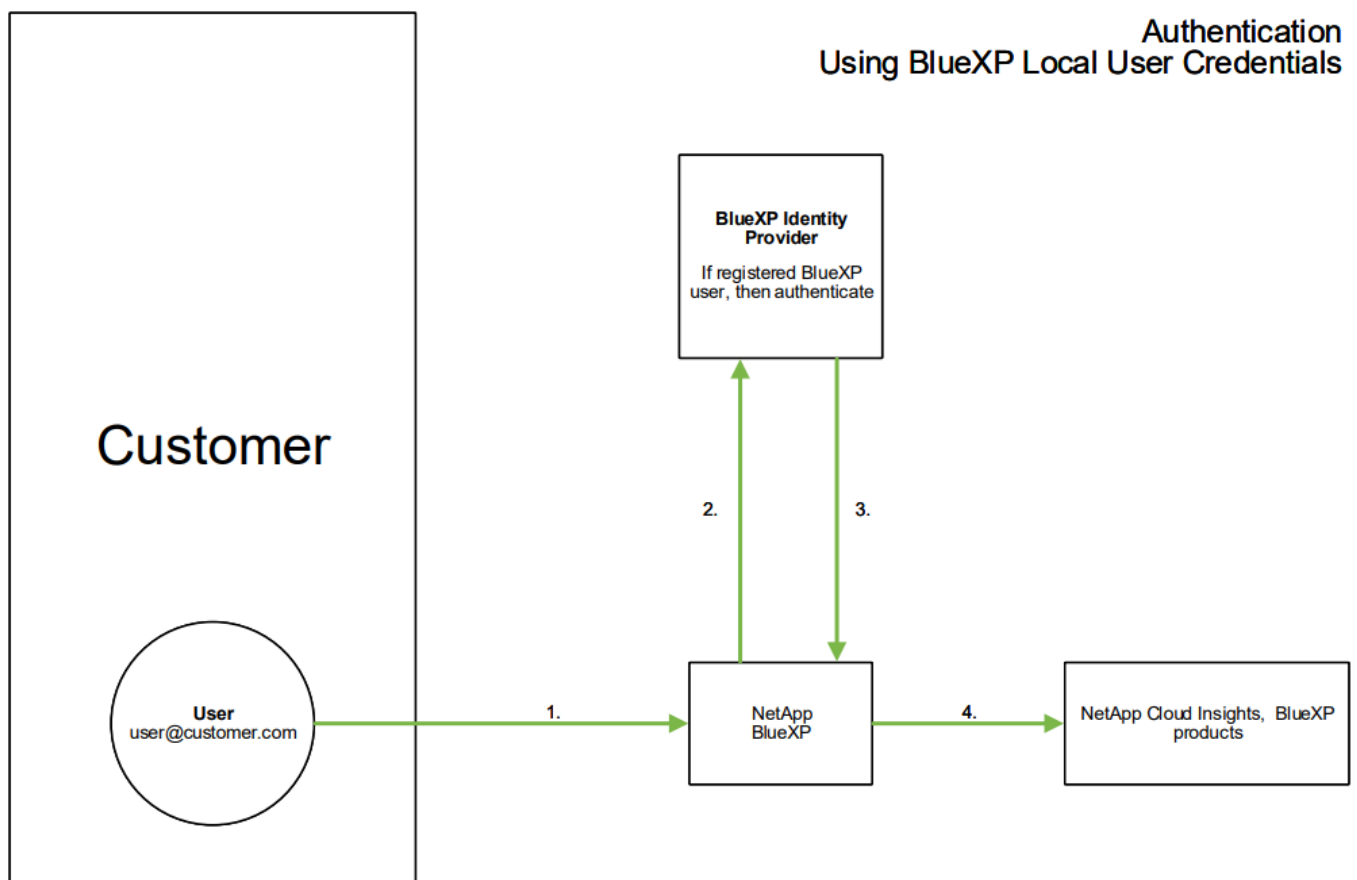
Logon único (SSO) e Federação de identidade

O que é a Federação de identidade?

Com a Federação de identidade:

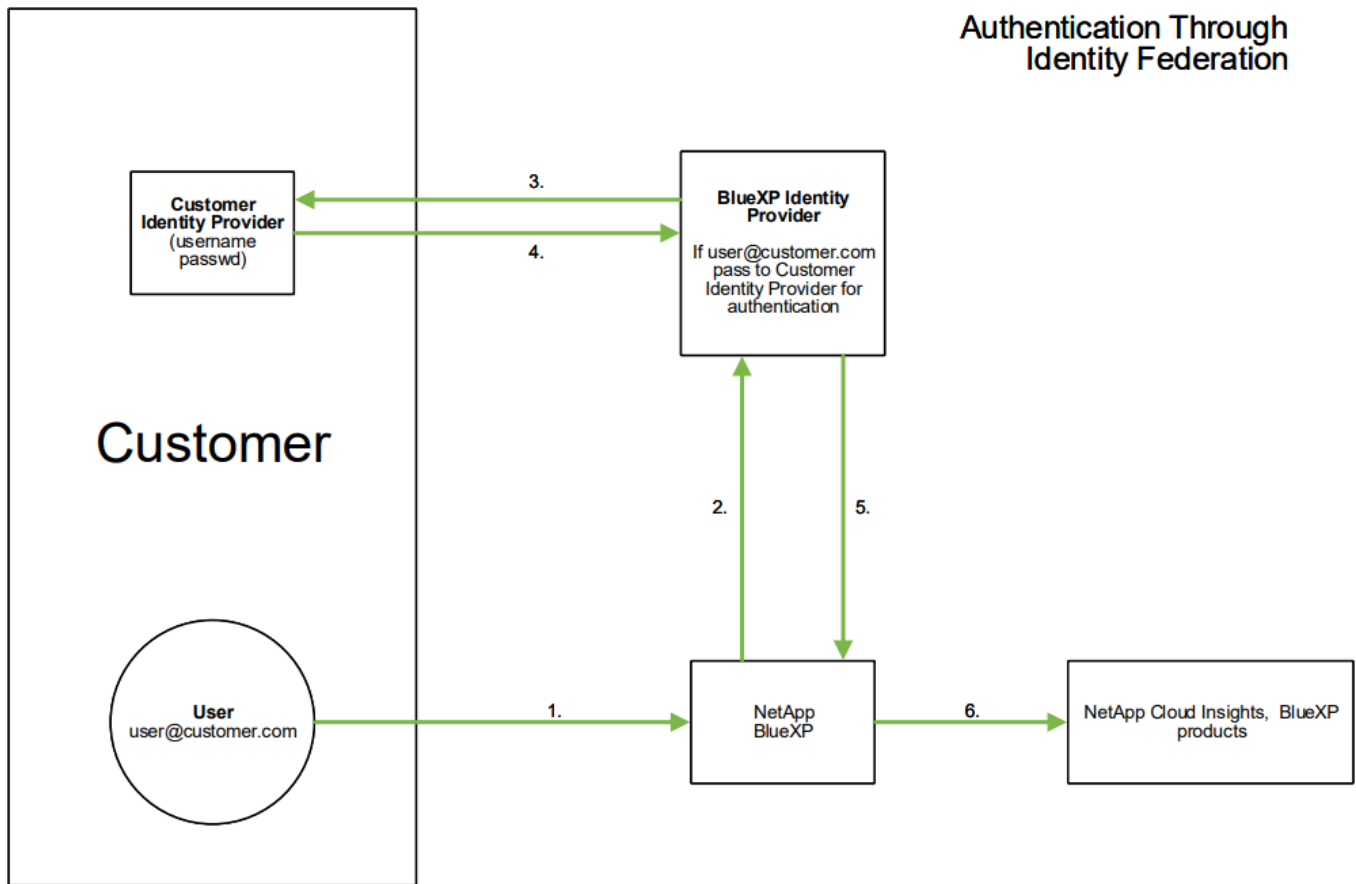
- A autenticação é delegada no sistema de gerenciamento de identidade do cliente, usando as credenciais do cliente de seu diretório corporativo e políticas de automação, como a Autenticação multifator (MFA).
- Os usuários fazem login uma vez em todos os Serviços do NetApp BlueXP (logon único).

As contas de usuário são gerenciadas no NetApp BlueXP para todos os serviços de nuvem. Por padrão, a autenticação é feita usando um perfil de usuário local do BlueXP. Abaixo está uma visão geral simplificada desse processo:



No entanto, alguns clientes gostariam de usar seu próprio provedor de identidade para autenticar seus usuários para Insights de infraestrutura de dados e seus outros Serviços NetApp BlueXP. Com a Federação de identidades, as contas do NetApp BlueXP são autenticadas usando credenciais do diretório corporativo.

O seguinte é um exemplo simplificado desse processo:



No diagrama acima, quando um usuário acessa o Data Infrastructure Insights, esse usuário é direcionado para o sistema de gerenciamento de identidade do cliente para autenticação. Depois que a conta for autenticada, o usuário será direcionado para o URL do locatário do Data Infrastructure Insights.

Habilitando a Federação de identidade

O BlueXP usa o Auth0 para implementar a Federação de identidades e integrar-se a serviços como os Serviços de Federação do Active Directory (ADFS) e o Microsoft Azure Active Directory (AD). Para configurar a Federação de identidade, consulte "[Instruções da Federação BlueXP](#)".



Você deve configurar a Federação de identidade do BlueXP antes de usar o SSO com Insights de infraestrutura de dados.

É importante entender que a federação de identidade em mudança no BlueXP se aplicará não apenas aos insights de infraestrutura de dados, mas a todos os serviços da NetApp BlueXP. O cliente deve discutir essa alteração com a equipe do NetApp de cada produto do BlueXP que possui para garantir que a configuração que está usando funcionará com a Federação de identidade ou se os ajustes precisarem ser feitos em qualquer conta. O cliente também precisará envolver sua equipe interna de SSO na federação de mudança de identidade.

Também é importante perceber que, uma vez ativada a federação de identidade, qualquer alteração no provedor de identidade da empresa (como passar de SAML para Microsoft AD) provavelmente exigirá solução de problemas/alterações/atenção no BlueXP para atualizar os perfis dos usuários.

Para este ou quaisquer outros problemas de federação, você pode abrir um ticket de suporte em

<https://mysupport.netapp.com/site/help> e selecionar a categoria **BlueXP .NetApp.com > problemas de Federação**.

Provisionamento automático de usuário de logon único (SSO)

Além de convidar os usuários, os administradores podem habilitar o acesso ao **Single Sign-On (SSO) User Auto-Provisioning** ao Data Infrastructure Insights para todos os usuários em seu domínio corporativo, sem ter que convidá-los individualmente. Com o SSO ativado, qualquer usuário com o mesmo endereço de e-mail de domínio pode fazer login no Data Infrastructure Insights usando suas credenciais corporativas.



O *provisionamento automático do usuário SSO* está disponível no Data Infrastructure Insights Premium Edition e deve ser configurado antes de poder ser habilitado para o Data Infrastructure Insights. A configuração de provisionamento automático do usuário SSO inclui "[Federação de identidade](#)" através do NetApp BlueXP, conforme descrito na seção acima. A Federação permite que usuários de logon único acessem suas contas do NetApp BlueXP usando credenciais de seu diretório corporativo, usando padrões abertos como a linguagem de marcação de asserção de Segurança 2,0 (SAML) e o OpenID Connect (OIDC).

Para configurar o *provisionamento automático do usuário SSO*, na página **Admin > Gerenciamento de usuário**, primeiro você deve configurar a Federação de identidade do BlueXP. Selecione o link **Configurar Federação** no banner para prosseguir para a Federação BlueXP. Uma vez configurado, os administradores do Data Infrastructure Insights podem habilitar o login do usuário SSO. Quando um administrador ativa *SSO User Auto-Provisioning*, ele escolhe uma função padrão para todos os usuários SSO (como convidado ou Usuário). Os usuários que fizerem login por meio do SSO terão essa função padrão.

Set up Identity Federation to sign in using your organization credentials.

[Dismiss](#) [Set Up Federation](#)

Ocasionalmente, um administrador desejará promover um único usuário fora da função SSO padrão (por exemplo, para torná-lo um administrador). Eles podem fazer isso na página **Admin > User Management** clicando no menu do lado direito do usuário e selecionando *Assign role*. Os usuários que recebem uma função explícita desta maneira continuam a ter acesso ao Data Infrastructure Insights, mesmo que *SSO User Auto-Provisioning* seja posteriormente desativado.

Se o usuário não precisar mais da função elevada, você pode clicar no menu para *Remover usuário*. O utilizador será removido da lista. Se *SSO User Auto-Provisioning* estiver ativado, o usuário poderá continuar fazendo login no Data Infrastructure Insights por meio do SSO, com a função padrão.

Você pode optar por ocultar usuários SSO desmarcando a caixa de seleção **Mostrar usuários SSO**.

No entanto, não ative *SSO User Auto-Provisioning* se qualquer um destes for verdadeiro:

- Sua organização tem mais de um locatário do Data Infrastructure Insights
- Sua organização não quer que nenhum/todos os usuários do domínio federado tenham algum nível de acesso automático ao locatário do Data Infrastructure Insights. *Neste momento, não temos a capacidade de usar grupos para controlar o acesso à função com esta opção.*


Restringindo o acesso por domínio

O Data Infrastructure Insights pode restringir o acesso do usuário apenas aos domínios especificados. Na página **Admin > User Management**, selecione "restringir domínios".

Restrict Domains



Select which domains have access to Cloud Insights:

- No restrictions (Cloud Insights available on all domains)
- Limit access to default domains (acme.com, gmail.com, netapp.com) 
- Limit access to defaults and following domains

legal.acme.com ✕

anvils.acme.com ✕

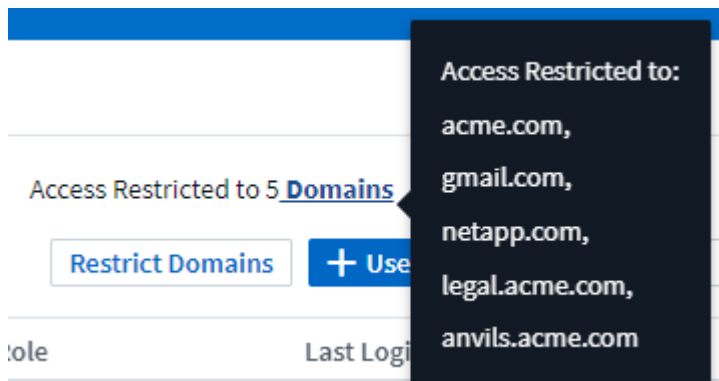
[Learn more about domain restriction.](#) 

Cancel

Save

Você é apresentado com estas escolhas:

- Sem restrições: O Data Infrastructure Insights permanece acessível aos usuários, independentemente de seu domínio.
- Limitar o acesso a domínios padrão: Os domínios padrão são aqueles usados pelos proprietários de contas de ambiente do Data Infrastructure Insights. Esses domínios são sempre acessíveis.
- Limite o acesso aos padrões mais domínios especificados. Liste todos os domínios que você deseja ter acesso ao seu ambiente Data Infrastructure Insights, além dos domínios padrão.



Access Restricted to 5 Domains

Restrict Domains + Use

Access Restricted to:

- acme.com,
- gmail.com,
- netapp.com,
- legal.acme.com,
- anvils.acme.com

Lista de coletores de dados do Insights de infraestrutura de dados

O Data Infrastructure Insights dá suporte a uma variedade de coletores de dados de muitos fornecedores e serviços.

Os coletores de dados são categorizados por estes tipos:

- **Infraestrutura:** Adquirida de dispositivos de fornecedores, como storage arrays, switches, hipervisores ou dispositivos de backup.
- **Serviço:** Adquirido de serviços como Kubernetes ou Docker. Também chamado *Integration*.

Lista alfabética de coletores de dados suportados pelo Data Infrastructure Insights:

Coletor de dados	Tipo
"Amazon EC2 e EBS"	Infraestrutura
"AWS S3 como storage"	Infra-estrutura
"Amazon FSX para NetApp ONTAP"	Infraestrutura
"Apache"	Serviço
"Azure NetApp Files"	Infraestrutura
"VMs Azure e VHD"	Infraestrutura
"Consultor de rede Brocade (BNA)"	Infraestrutura
"Switches Fibre Channel Brocade"	Infraestrutura
"Brocade FOS REST"	Infraestrutura
"Switches de malha Cisco MDS"	Infraestrutura
"Cônsul"	Serviço
"Couchbase"	Serviço
"CouchDB"	Serviço
"Cohesity SmartFiles"	Infraestrutura
"Dell EMC Data Domain"	Infraestrutura
"Dell EMC ECS"	Infraestrutura
"Dell EMC PowerScale (anteriormente Isilon)"	Infraestrutura
"Dell EMC Isilon / PowerScale REST"	Infraestrutura
"Dell EMC PowerStore"	Infraestrutura
"Ponto de recuperação da Dell EMC"	Infraestrutura
"Dell EMC ScaleIO/PowerFlex"	Infraestrutura
"Dell EMC Unity"	Infraestrutura
"Dell EMC Unisphere REST"	Infraestrutura

Coletor de dados	Tipo
"Família de dispositivos Dell EMC VMAX/Powermax"	Infraestrutura
"Armazenamento em bloco VNX da Dell EMC"	Infraestrutura
"Ficheiro VNX da Dell EMC"	Infraestrutura
"Dell EMC VNX Unified"	Infraestrutura
"Dell EMC VPLEX"	Infraestrutura
"Dell EMC XtremIO"	Infraestrutura
"Série XC da Dell"	Infraestrutura
"Docker"	Serviço
"Elasticsearch"	Serviço
"Flink"	Serviço
"Fujitsu ETERNUS DX"	Infraestrutura
"Google Compute e Storage"	Infraestrutura
"Hadoop"	Serviço
"HAProxy"	Serviço
"Plataforma de conteúdo Hitachi (HCP)"	Infraestrutura
"Hitachi Vantara Command Suite"	Infraestrutura
"Plataforma nas Hitachi Vantara"	Infraestrutura
"Hitachi Ops Center"	Infraestrutura
"Armazenamento HP Enterprise Alletra 6000 (anteriormente ágil)"	Infraestrutura
"Armazenamento HP Enterprise Alletra 9000 / Primera (anteriormente 3PAR)"	Infraestrutura
"HP Enterprise Command View"	Infraestrutura
"Huawei OceanStor e dispositivos Dorado"	Infraestrutura
"IBM Cleversafe"	Infraestrutura
"IBM CS Series"	Infraestrutura
"IBM PowerVM"	Infraestrutura
"IBM SAN volume Controller (SVC)"	Infraestrutura
"IBM System Storage DS8000 Series"	Infraestrutura
"Armazenamentos IBM XIV e A9000"	Infraestrutura
"Infinidat InfiniBox"	Infraestrutura
"Java"	Serviço
"Kafka"	Serviço
"Kapacitor"	Serviço

Coletor de dados	Tipo
"Kibana"	Serviço
"Kubernetes"	Serviço
"Série Lenovo HX"	Infraestrutura
"Memcached"	Serviço
"Microsoft Azure NetApp Files"	Infraestrutura
"Microsoft Hyper-V"	Infraestrutura
"MongoDB"	Serviço
"MySQL"	Serviço
"NetApp Cloud Volumes ONTAP"	Infraestrutura
"NetApp Cloud volumes Services para AWS"	Infraestrutura
"Conexão de nuvem NetApp para ONTAP 9.9 ou superior"	Infraestrutura
"NetApp Data ONTAP 7-Mode"	Infraestrutura
"NetApp e-Series"	Infraestrutura
"NetApp e-SERIES REST"	Infraestrutura
"Amazon FSX para NetApp ONTAP"	Infraestrutura
"Centro Virtual da NetApp HCI"	Infraestrutura
"Software de gerenciamento de dados NetApp ONTAP"	Infraestrutura
"Coletor de REPOUSO NetApp ONTAP"	Infraestrutura
"Coletor de array all-SAN NetApp ONTAP (ASA)"	Infraestrutura
"NetApp ONTAP Select"	Infraestrutura
"Array all-flash NetApp SolidFire"	Infraestrutura
"NetApp StorageGRID"	Infraestrutura
"Netstat"	Serviço
"Nginx"	Serviço
"Nó"	Serviço
"Série Nutanix NX"	Infraestrutura
"OpenStack"	Infraestrutura
"OpenZFS"	Serviço
"Oracle ZFS Storage Appliance"	Infraestrutura
"PostgreSQL"	Serviço
"Agente de fantoche"	Serviço
"Pure Storage FlashArray"	Infraestrutura

Coletor de dados	Tipo
"Virtualização da Red Hat"	Infraestrutura
"Redis"	Serviço
"RethinkDB"	Serviço
"RHEL CentOS"	Serviço
"Storage CDM da Rubrik"	Infraestrutura
"Ubuntu Debian"	Serviço
"Armazenamento de dados VASTO"	Infraestrutura
"VMware vSphere"	Infraestrutura
"Windows"	Serviço
"Zookeeper"	Serviço

Subscrever o Data Infrastructure Insights

Os primeiros passos do Data Infrastructure Insights são tão fáceis quanto três simples passos:


- Inscreva-se para "[NetApp BlueXP](#)" ter acesso a todas as ofertas da NetApp na nuvem.
- Inscreva-se em "[avaliação gratuita](#)" um dos Insights da infraestrutura de dados para explorar os recursos disponíveis.
- **Subscribe** to Data Infrastructure Insights para acesso contínuo e ininterrupto aos seus dados via "[Vendas da NetApp](#)" direto ou "[AWS Marketplace](#)".

Durante o processo de Registro, você pode escolher a região global para hospedar seu ambiente Data Infrastructure Insights. Para obter mais informações, leia sobre o Data Infrastructure Insights "[Informação e região](#)".

Para obter uma comparação completa dos recursos disponíveis nas edições Data Infrastructure Insights Basic e Premium, consulte a "[Preços do Data Infrastructure Insights](#)" página.



Os ambientes inativos do Data Infrastructure Insights Basic Edition são excluídos e seus recursos são recuperados. Um ambiente é considerado inativo se não houver atividade do usuário por 30 dias consecutivos, se não houver dados ingeridos por 7 dias consecutivos. O Data Infrastructure Insights enviará uma notificação e fornecerá um período de carência de quatro dias antes que um ambiente seja excluído.

Ao usar o Data Infrastructure Insights, se você vir um ícone de cadeado , isso significa que o recurso não está disponível em sua assinatura atual ou está disponível em um formulário limitado. Assine esse recurso para acesso total. Alguns recursos estão disponíveis como um [Avaliação do módulo](#) antes da assinatura.

Edição de avaliação

Quando você se inscreve no Data Infrastructure Insights e seu ambiente está ativo, entra em uma avaliação gratuita de 30 dias do Data Infrastructure Insights. Durante esse teste, você pode explorar os recursos que o Data Infrastructure Insights tem a oferecer em seu próprio ambiente.

A qualquer momento durante o período de teste, você pode se inscrever no Data Infrastructure Insights. A assinatura do Data Infrastructure Insights garante acesso ininterrupto aos seus dados, bem como opções estendidas "[suporte ao produto](#)".

O Data Infrastructure Insights exibe um banner quando sua avaliação gratuita está chegando ao fim. Dentro desse banner há um link *View Subscription*, que abre a página **Admin** → **Subscription**. Os usuários não administradores verão o banner, mas não poderão acessar a página de assinatura.



Se você precisar de tempo adicional para avaliar o Data Infrastructure Insights e sua avaliação estiver definida para expirar em 4 dias ou menos, poderá estender sua avaliação por mais 30 dias. Você pode estender o teste apenas uma vez. Você não pode estender se o seu teste expirou.

Teste pelo AWS Marketplace

Você também pode se inscrever para uma avaliação gratuita pelo AWS Marketplace. A avaliação gratuita do AWS Marketplace oferece acesso ao Data Infrastructure Insights por um período de teste de 33 dias e permite até 499 [Unidades gerenciadas](#) (MUs).

Nota: Se você configurar mais de 499 MUs, você entrará no estado "violado". Enquanto seu teste estiver em estado violado, você perderá o acesso a algumas funcionalidades do Data Infrastructure Insights até que a violação seja resolvida, reduzindo o número de MUs configuradas ou assinando o Data Infrastructure Insights.

A avaliação gratuita do AWS Marketplace não pode ser estendida. A qualquer momento durante a avaliação, você pode fazer o downgrade para uma assinatura do Data Infrastructure Insights Basic Edition ou alterar para uma assinatura paga do Data Infrastructure Insights, visitando a página **Admin** → **Subscription**.

E se o meu teste tiver expirado?

Se a sua avaliação gratuita expirou e você ainda não se inscreveu no Data Infrastructure Insights, você terá funcionalidade limitada até se inscrever. A ingestão de dados pode cessar e, após algumas semanas, seus dados serão excluídos de acordo com nossa política de retenção de dados.

E se a minha subscrição tiver expirado?

Se você tiver uma assinatura do Data Infrastructure Insights, mas essa assinatura expirou, você terá um período de carência de cinco dias para renovar sua assinatura. Toda a funcionalidade Data Infrastructure Insights permanecerá ativa durante esse período de carência.

Após o período de carência ter decorrido, a funcionalidade Data Infrastructure Insights é suspensa até que você seja renovado. Para renovar, consulte a página **Admin > Subscription** ou entre em Contato com as vendas da NetApp.



Os dados do Data Infrastructure Insights coletados até o fim do período de carência permanecem intactos por 30 dias após o período de carência. Se você renovar sua assinatura dentro desse tempo, todos os seus dados até o momento em que o período de carência terminar estarão disponíveis para você.

E se a minha subscrição tiver expirado?

Se você tiver uma assinatura do Data Infrastructure Insights, mas essa assinatura expirou, você terá um período de carência de cinco dias para renovar sua assinatura. Toda a funcionalidade Data Infrastructure Insights permanecerá ativa durante esse período de carência.

Após o período de carência ter decorrido, a funcionalidade Data Infrastructure Insights é suspensa até que você seja renovado. Para renovar, consulte a página **Admin > Subscription** ou entre em Contato com as vendas da NetApp.



Seus dados do Data Infrastructure Insights permanecem intactos por 30 dias após o período de carência. Se você renovar sua assinatura dentro desse tempo, todos os seus dados até o momento em que o período de carência terminar estarão disponíveis para você.

Avaliação do módulo

Você também pode aproveitar **avaliações de módulos**. Por exemplo, se você já estiver inscrito no Infrastructure Observability, mas estiver adicionando o Kubernetes ao seu ambiente, entrará automaticamente em uma avaliação de 30 dias da observabilidade do Kubernetes, a partir de quando instalar o Operador de monitoramento do Kubernetes da NetApp. Você só será cobrado pelo uso de unidade gerenciada de observabilidade do Kubernetes ao final do período de avaliação.



Tenha em mente que você será cobrado pelo uso de uma nova unidade gerenciada (MU) após a avaliação, então certifique-se de Planejar adequadamente. Quando a avaliação do seu módulo terminar, você será notificado se precisar adicionar mais MUs para evitar a interrupção do serviço.




Você pode monitorar o uso da unidade gerenciada na página **Admin > assinatura** na guia **uso**.



A *Module Evaluation* não é um *Trial* - usamos o período de avaliação de prazo quando fornecemos aos clientes um período de teste gratuito para usar o serviço Data Infrastructure Insights para confirmar a adequação e habilitar a compra. Uma avaliação de módulo é diferente - é quando permitimos que um cliente pago experimente um módulo de Data Infrastructure Insights que ele não usou nos últimos meses de sua assinatura paga. Quando a avaliação está ativa, as cobranças apenas para o módulo recém-configurado são dispensadas. O ambiente de trabalho dos clientes ainda está sob assinatura e não reverteu para a versão de avaliação gratuita. A subscrição não foi alterada.

Estimador

Durante uma avaliação do módulo, você não será cobrado o uso de um para os recursos consumidos para o módulo, mas você pode abrir o **Estimador** (na guia *Summary*) para ver como as MUs serão cobradas após a avaliação, bem como jogar com cenários "e se" com o número de MUs que você pode precisar no futuro. Reponha os números saindo do Estimador.

 Infrastructure Observability 	20 Hosts	20 Raw TiB	0 Object TiB	Current Usage	Managed Units = 15
 Kubernetes Observability 	40 vCPUs	Current Usage			Managed Units = 10

Marque a caixa de seleção ao lado de um módulo para adicionar ou remover todos os MU do módulo do custo estimado.

O Estimator também permite que você veja como os números se acumulam para um Add On - onde você mantém seu prazo de assinatura atual e aumenta o número de unidades gerenciadas licenciadas - ou uma opção de renovação para uma assinatura de renovação que você compraria quando seu prazo de assinatura atual terminar.

Observe que os clientes só são elegíveis para uma avaliação de módulo uma vez por assinatura.

Opções de subscrição

Para se inscrever, vá para **Admin** → **Subscription**. Além dos botões **Subscribe**, você poderá ver seus coletores de dados instalados e calcular sua medição estimada. Para um ambiente típico, você pode clicar no botão AWS Marketplace de autoatendimento. Se o seu ambiente incluir ou se espera que inclua 1.000 ou mais unidades gerenciadas, você estará qualificado para o preço de volume.

Medição de observabilidade

A capacidade de observação do Data Infrastructure Insights é avaliada de duas maneiras:

- Medição da capacidade
- Medição de unidade gerenciada (legado)

Sua assinatura será mensurada por um desses métodos, dependendo se você tem uma assinatura existente ou está iniciando uma nova assinatura.

Medição da capacidade

A observabilidade do Data Infrastructure Insights mede o uso de acordo com o nível de armazenamentos em seu localatário. Você pode ter armazenamentos que se enquadram em uma ou mais dessas categorias:

- Primário bruto
- Objeto bruto
- Nuvem consumida

Cada nível é medido a uma taxa diferente, com o todo calculado em conjunto para lhe dar um direito *efetivo*. A fórmula para calcular o uso eficaz é a seguinte:

```
Effective usage = Raw TiB + (0.1 x Object Tier Raw TiB) + (0.25 x Cloud Tier Provisioning TiB)
```



A soma de unidades gerenciadas pode diferir ligeiramente da contagem de coletores de dados na seção de resumo. Isso ocorre porque as contagens de unidades gerenciadas são arredondadas para a Unidade gerenciada mais próxima. A soma desses números na lista de coletores de dados pode ser ligeiramente maior do que o total de unidades gerenciadas na seção de status. A seção de resumo reflete sua contagem de unidades gerenciadas real para sua assinatura. Para facilitar isso, o DII calcula um único número de direito * efetivo* com base em quantidades *subscritas*; em seguida, calcula esse mesmo número com base no armazenamento *descoberto* e só declara violação se a capacidade efetiva descoberta for maior do que o direito efetivo. Isso oferece flexibilidade para monitorar quantidades que variam de acordo com os valores inscritos para cada nível, o que o DII permite, contanto que o storage total descoberto esteja dentro dos direitos efetivos inscritos.

Medição de unidade gerenciada (legado)

Observabilidade da infraestrutura de dados e uso do medidor de observabilidade do Kubernetes por **Unidade gerenciada**. O uso de suas unidades gerenciadas é calculado com base no número de **hosts ou máquinas virtuais** e na quantidade de **capacidade não formatada** sendo gerenciada em seu ambiente de infraestrutura.

- 1 Unidade gerenciada: 2 hosts (qualquer máquina virtual ou física)
- 1 Unidade gerenciada: 4 TIB de capacidade não formatada de discos físicos ou virtuais
- 1 Unidade gerenciada: 40 TIB de capacidade não formatada do armazenamento secundário selecionado: AWS S3, Cohesity SmartFiles, Dell EMC Data Domain, Hitachi Content Platform, IBM Cleversafe, NetApp StorageGRID, Rubrik.
- 1 Unidade gerenciada: 4 vCPUs de Kuberentes.
 - 1 Ajuste da Unidade gerenciada K8s: 2 nós ou hosts também monitorados pela infraestrutura.

Se o seu ambiente incluir ou for esperado que inclua 1.000 ou mais unidades gerenciadas, você estará qualificado para **preço por volume** e será solicitado a entrar em Contato com as vendas da NetApp para se inscrever. [abaixo](#) Consulte para obter mais detalhes.

Medição da segurança da carga de trabalho

A segurança do workload é medida pelo cluster usando a mesma abordagem que a medição de observabilidade.

Você pode exibir o uso do Workload Security na página **Admin > Subscription** na guia **Workload Security**.

Summary Usage History

Total Usage and Entitlement



Usage by Module



Infrastructure Observability Kubernetes Observability Workload Security

Last updated 07/18/2024 9:11:11 AM

Installed Data Collectors (17) Filter...

Name ↑	Type	High-end node	Mid-range node	Entry-level node	Software ONTAP	Unknown node	Metered MUs	MUs Adjustment	Billed MUs
CI_CIFS_SVM	ONTAP SVM	0	1	0	0	0	40.00	(40.00)	0.00
CL_SVM	ONTAP SVM	0	1	0	0	0	40.00	(40.00)	0.00
cluster11	ONTAP SVM	1	0	0	0	0	80.00	(80.00)	0.00
cluster_demo	Cloud Volumes ONTAP	0	0	0	1	0	10.00	(10.00)	0.00



As assinaturas existentes do Workload Security têm seu uso de MU ajustado para que o uso do nó não consuma unidades gerenciadas. O Data Infrastructure Insights mede o uso para garantir a conformidade com o uso licenciado.

Como faço para me inscrever?

Se sua contagem de unidades gerenciadas for inferior a 1.000, você poderá se inscrever por meio de vendas da NetApp ou [auto-subscrição](#) pelo mercado AWS.

Inscreva-se através do NetApp vendas diretas

Se a sua contagem de unidades geridas esperada for igual ou superior a 1.000, clique no "[Contato de vendas](#)" botão para subscrever a equipa de vendas da NetApp.

Você deve fornecer seus dados de informações de infraestrutura **número de série** ao seu representante de vendas da NetApp para que sua assinatura paga possa ser aplicada ao seu ambiente de informações de infraestrutura de dados. O número de série identifica exclusivamente o ambiente de avaliação do Data Infrastructure Insights e pode ser encontrado na página **Admin > Subscription**.

Inscreva-se automaticamente no AWS Marketplace



Você deve ser um proprietário ou administrador de conta para aplicar uma assinatura do AWS Marketplace à sua conta de avaliação existente do Data Infrastructure Insights. Além disso, você precisa ter uma conta do Amazon Web Services (AWS).

Clicar no link do Amazon Marketplace abre a página de assinatura da AWS "[Insights da infraestrutura de dados](#)", onde você pode concluir sua assinatura. Observe que os valores inseridos na calculadora não estão preenchidos na página de assinatura da AWS; você precisará inserir o total de unidades gerenciadas nessa página.

Depois de inserir a contagem total de unidades gerenciadas e escolher o prazo de assinatura de 12 meses ou 36 meses, clique em **Configurar sua conta** para concluir o processo de assinatura.

Depois que o processo de assinatura da AWS estiver concluído, você será levado de volta ao seu ambiente

Data Infrastructure Insights. Ou, se o ambiente não estiver mais ativo (por exemplo, você fez logout), você será levado para a página de login do NetApp BlueXP . Quando você entrar novamente no Data Infrastructure Insights, sua assinatura estará ativa.



Depois de clicar em **Configurar sua conta** na página do AWS Marketplace, você deve concluir o processo de assinatura da AWS em uma hora. Se você não o concluir dentro de uma hora, você precisará clicar em **Configurar sua conta** novamente para concluir o processo.

Se houver um problema e o processo de assinatura não for concluído corretamente, você ainda verá o banner "versão de avaliação" quando fizer login no seu ambiente. Neste caso, pode aceder a **Admin > subscrição** e repetir o processo de subscrição.

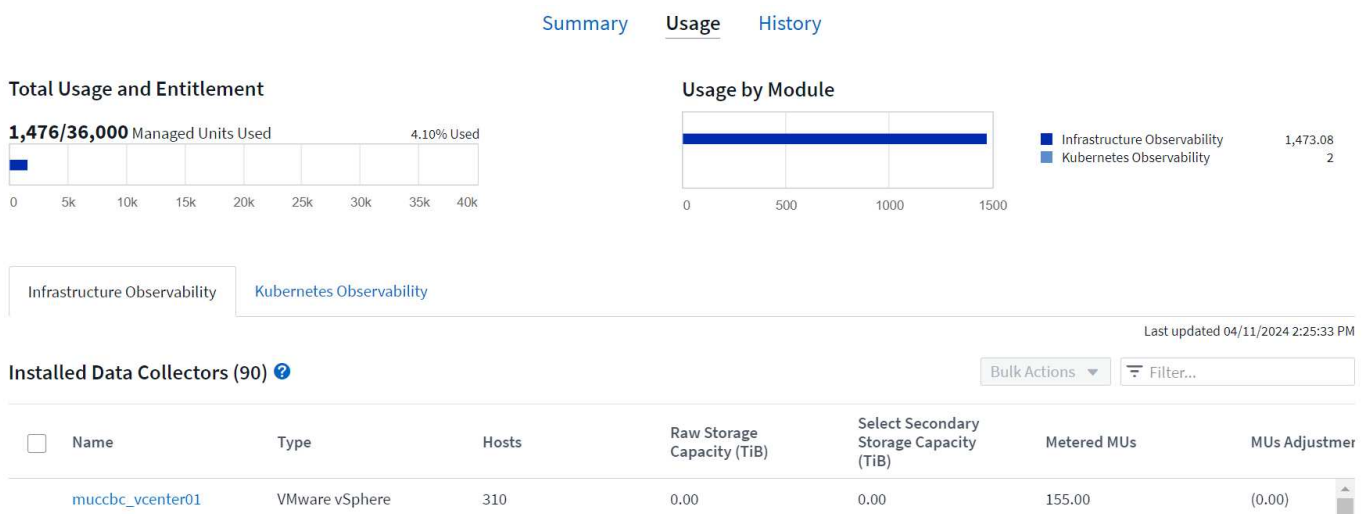
Veja o status da assinatura

Quando a sua subscrição estiver ativa, pode ver o estado da subscrição e a utilização da unidade gerida a partir da página **Admin > subscrição**.

A guia Subscription **Summary** (Resumo* da assinatura) exibe coisas como as seguintes:

- Edição atual
- Número de série da subscrição
- Direito de um atual

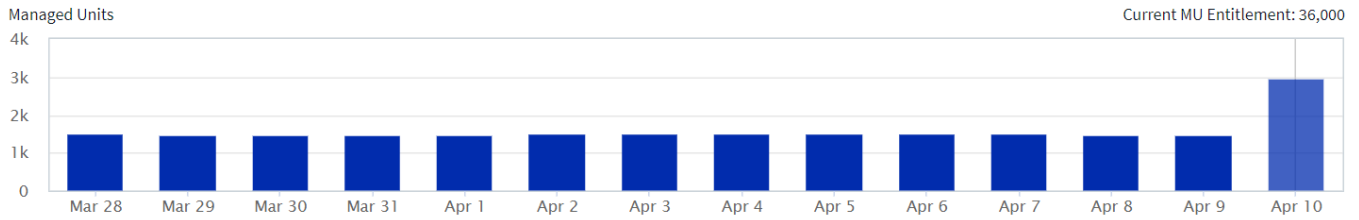
A guia **Usage** mostra seu uso atual de MU e como esse uso se divide pelo coletor de dados.



O separador **Histórico** dá-lhe informações sobre a sua utilização de MU nos últimos 7 a 90 dias. Passar o Mouse sobre uma coluna no gráfico dá a você um detalhamento por módulo (ou seja, observabilidade, Kubernetes).

🕒 Last 14 days ▼

Consumption by Module ?



Legend

04/10/2024	
Infrastructure Observability	2,939.53
Kubernetes Observability	11.00
Total Metered MUs (rounded)	2,951

Veja o seu Gerenciamento de uso

A guia Gerenciamento de uso mostra uma visão geral do uso da Unidade gerenciada, bem como guias que dividem o consumo de Unidade gerenciada por coletor ou cluster do Kubernetes.



A contagem de unidades gerenciadas de capacidade não formatada reflete uma soma da capacidade bruta total no ambiente e é arredondada para a Unidade gerenciada mais próxima.



A soma de unidades gerenciadas pode diferir ligeiramente da contagem de coletores de dados na seção de resumo. Isso ocorre porque as contagens de unidades gerenciadas são arredondadas para a Unidade gerenciada mais próxima. A soma desses números na lista de coletores de dados pode ser ligeiramente maior do que o total de unidades gerenciadas na seção de status. A seção de resumo reflete sua contagem de unidades gerenciadas real para sua assinatura.

Caso seu uso esteja chegando ou excedendo o valor inscrito, você poderá reduzir o uso excluindo coletores de dados ou interrompendo o monitoramento dos clusters do Kubernetes. Exclua um item nesta lista clicando no menu "três pontos" e selecionando *Excluir*.

O que acontece se eu exceder a minha utilização subscrita?

Os avisos são apresentados quando a utilização da unidade gerida exceder 80%, 90% e 100% do valor total subscrito:

Quando o uso excede:	Isto acontece/ação recomendada:
80%	É apresentado um banner informativo. Nenhuma ação é necessária.

Quando o uso excede:	Isto acontece/ação recomendada:
90%	É apresentado um banner de aviso. Você pode querer aumentar a contagem de unidades gerenciadas subscritas.
100%	Um banner de erro é exibido até que você execute um dos seguintes procedimentos: <ul style="list-style-type: none"> • Remova os coletores de dados para que o uso da Unidade gerenciada esteja em ou abaixo do valor inscrito • Modifique a sua subscrição para aumentar a contagem de unidades geridas subscritas

Inscriva-se diretamente e pule a avaliação

Você também pode se inscrever no Data Infrastructure Insights diretamente do ["AWS Marketplace"](#), sem primeiro criar um ambiente de teste. Assim que a subscrição estiver concluída e o ambiente estiver configurado, será imediatamente subscrito.

Adicionando um ID de direito

Se você possui um produto NetApp válido incluído no Insights de infraestrutura de dados, poderá adicionar esse número de série do produto à sua assinatura existente do Insights de infraestrutura de dados. Por exemplo, se você adquiriu o NetApp Astra Control Center, o número de série da licença do Astra Control Center poderá ser usado para identificar a assinatura no Insights de infraestrutura de dados. Insights de infraestrutura de dados refere-se a isso um *ID de direito*.

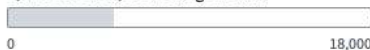
Para adicionar um ID de direito à sua assinatura do Data Infrastructure Insights, na página **Admin > Subscription**, clique em **_ ID de direito_**.

Subscription Summary

NetApp Serial Number: 95001014387268156333
Active Edition: Premium
[+ Entitlement ID](#)

Usage and Entitlement

5,122 out of 18,000 Managed Units



Hosts: 1,388 Managed Units (2,776 Hosts)

Unformatted Capacity: 3,734 Managed Units (14,934 TB)

Subscription Details

36 Months (Premium Edition)

Expires: March 3rd, 2022



[Modify Subscription](#)

[Estimate Cost](#)

Observabilidade

Criando painéis

Visão geral dos painéis

O Data Infrastructure Insights oferece aos usuários a flexibilidade para criar visualizações operacionais de dados de infraestrutura, permitindo que você crie painéis personalizados com uma variedade de widgets, cada um dos quais oferece ampla flexibilidade na exibição e criação de gráficos de seus dados.



Os exemplos nestas seções são apenas para fins de explicação e não cobrem todos os cenários possíveis. Os conceitos e etapas aqui podem ser usados para criar seus próprios painéis para destacar os dados específicos para suas necessidades específicas.

Criando um Dashboard

Você cria um novo dashboard em um de dois lugares:

- **Dashboards > novo painel]**
- **Painéis > Mostrar todos os painéis > clique no botão [-Painel]**

Controles do tablier

O ecrã Painel de instrumentos tem vários controles:

- *** Time seletor***: Permite visualizar os dados do painel durante um intervalo de tempo, desde os últimos 15 minutos até os últimos 30 dias, ou um intervalo de tempo personalizado de até 31 dias. Você pode optar por substituir esse intervalo de tempo global em widgets individuais.
- **Botão Editar**: Selecionar este irá ativar o modo Editar, que permite fazer alterações no painel de instrumentos. Novos painéis abrem no modo Editar por padrão.
- **Botão Salvar**: Permite salvar ou excluir o painel.

Você pode renomear o painel atual digitando um novo nome antes de clicar em **Salvar**.

- **Botão Adicionar Widget**, que permite adicionar qualquer número de tabelas, gráficos ou outros widgets ao painel.

Os widgets podem ser redimensionados e realocados para diferentes posições dentro do painel de controle, para lhe dar a melhor visualização de seus dados de acordo com suas necessidades atuais.

Tipos de widget

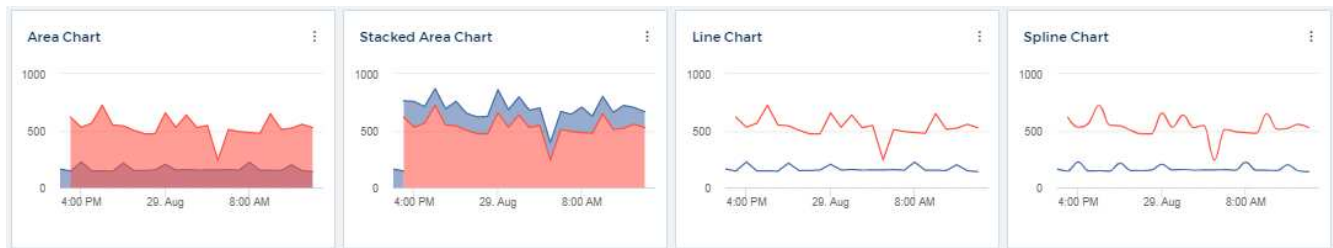
Você pode escolher entre os seguintes tipos de widget:

- *** Widget de tabela***: Uma tabela exibindo dados de acordo com filtros e colunas que você escolher. Os dados da tabela podem ser combinados em grupos que podem ser colapsados e expandidos.

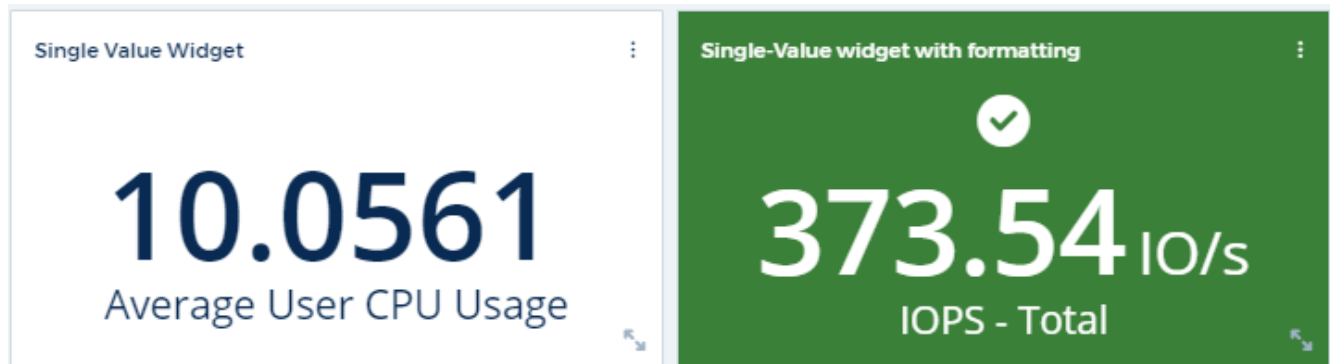
4 items found in 2 groups

Active Date	Storage Node	Cache Hit Ratio - Total (%)	IOPS - Total (IO...	IOPS - Write (L...	Latency
06/01/2020 (1)	ocinaneqa1-01	N/A	N/A	N/A	N/A
06/01/2020	ocinaneqa1-01	N/A	N/A	N/A	N/A
N/A (3)	--	N/A	N/A	N/A	N/A

- **Gráficos de linha, spline, Area, Stacked Area:** São widgets de gráficos de séries temporais nos quais você pode exibir desempenho e outros dados ao longo do tempo.



- * Widget de valor único*: Um widget que permite exibir um único valor que pode ser derivado diretamente de um contador ou calculado usando uma consulta ou expressão. Você pode definir limites de formatação de cores para mostrar se o valor está no intervalo esperado, aviso ou crítico.

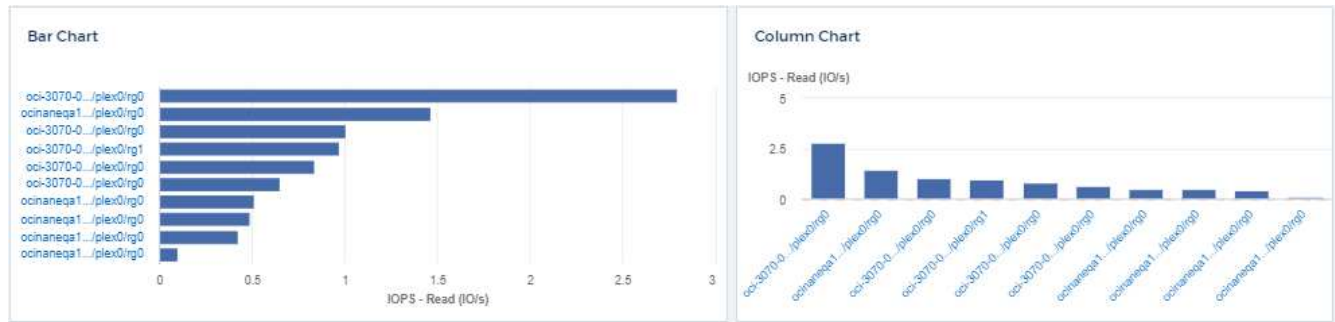


- * Widget de calibre*: Exibe dados de valor único em um medidor tradicional (sólido) ou calibre de bala, com cores baseadas em valores "Aviso" ou "crítico" você "[personalizar](#)".

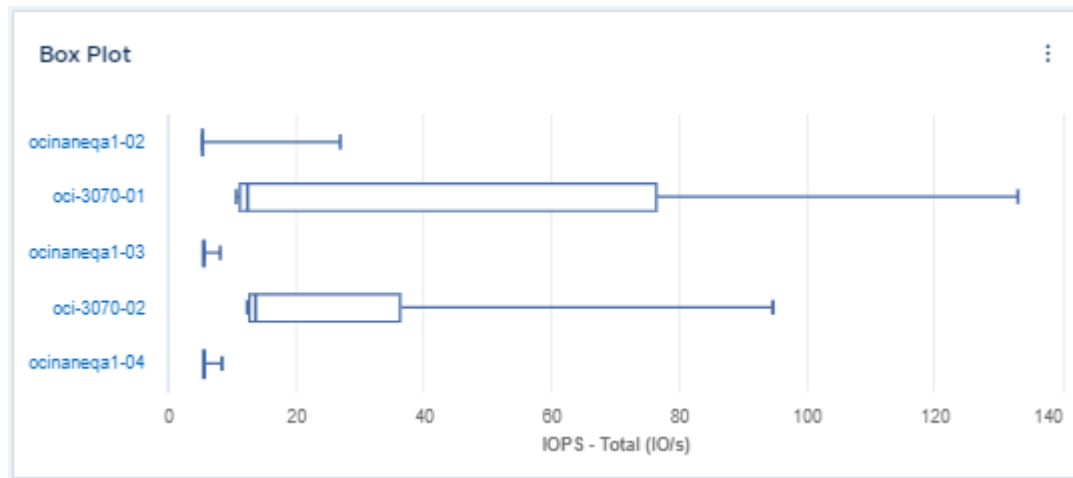


- **Bar, gráficos de colunas:** Exibe valores N superiores ou inferiores, por exemplo, armazenamentos Top

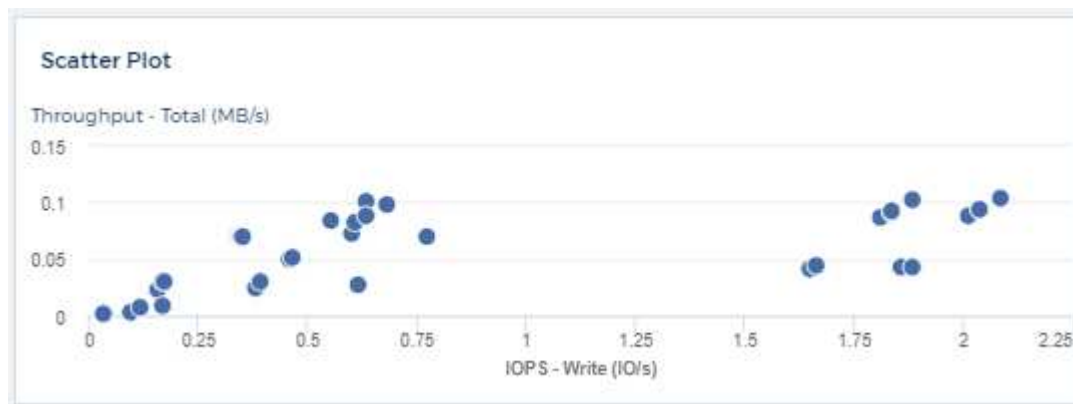
10 por capacidade ou volumes 5 inferiores por IOPS.



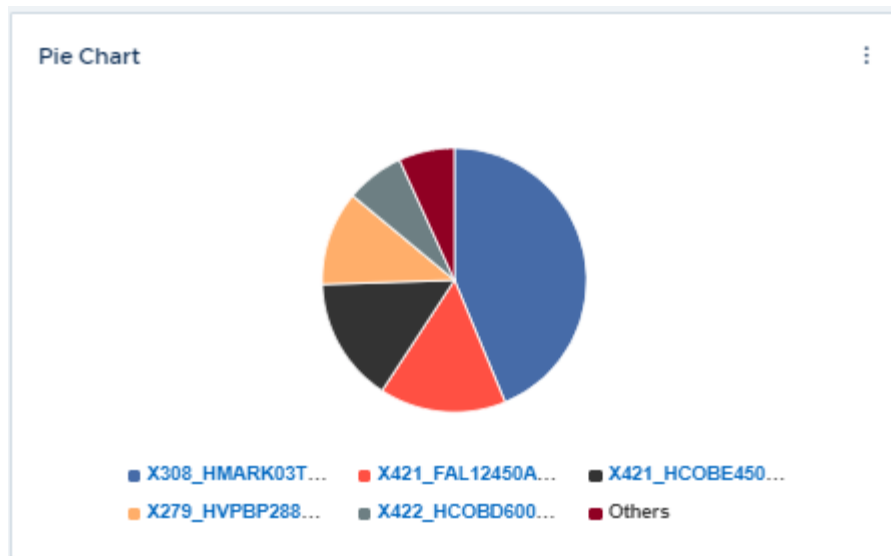
- * Gráfico de Gráfico de caixa*: Um gráfico do mínimo, máximo, mediana e o intervalo entre quartil inferior e superior de dados em um único gráfico.



- **Gráfico de plotagem de dispersão**: Gráficos de dados relacionados como pontos, por exemplo, IOPS e latência. Neste exemplo, você pode localizar rapidamente ativos com alta taxa de transferência e IOPS baixo.



- **Gráfico de pizza**: Um gráfico de pizza tradicional para exibir dados como um pedaço do total.



- * Observação widget*: Até 1000 caracteres de texto livre.



- **Tabela de alertas:** Exibe até os últimos 1.000 alertas.

Para obter explicações mais detalhadas sobre esses e outros recursos do Dashboard "[clique aqui](#)", .

Configurando um Dashboard como sua Home Page

Você pode escolher qual painel definir como a **home page** do seu locatário usando um dos seguintes métodos:

- Vá para **painéis > Mostrar todos os painéis** para exibir a lista de painéis no locatário. Clique no menu de opções à direita do painel desejado e selecione **Definir como Página Inicial**.
- Clique em um painel na lista para abrir o painel. Clique no menu suspenso no canto superior e selecione **Definir como Página Inicial**.

Funcionalidades do painel de instrumentos

Painéis e widgets permitem uma grande flexibilidade na forma como os dados são exibidos. Aqui estão alguns conceitos para ajudar você a aproveitar ao máximo seus painéis personalizados.

Nome do widget

Os widgets são nomeados automaticamente com base no objeto, métrica ou atributo selecionado para a primeira consulta de widget. Se você também escolher um agrupamento para o widget, os atributos "Agrupar por" serão incluídos na nomenclatura automática (método de agregação e métrica).

The screenshot shows the configuration interface for a widget. At the top, a text box contains the auto-generated name: "Maximum cpu.time_active by agent_node_ip". Below this, a configuration panel includes a "Query" section with "A) Query" checked, "Bar Chart" as the chart type, and "agent.node" as the object and "cpu.time_active" as the metric. The "Group by" field is set to "agent_node_ip" and the aggregation method is "Maximum".

Selecionar um novo objeto ou atributo de agrupamento atualiza o nome automático.

Se você não quiser usar o nome automático do widget, você pode simplesmente digitar um novo nome.

Posicionamento e tamanho do widget

Todos os widgets do painel podem ser posicionados e dimensionados de acordo com suas necessidades para cada painel específico.

Duplicando um Widget

No modo de edição do dashboard, clique no menu no widget e selecione **duplicar**. O editor de widget é iniciado, pré-preenchido com a configuração original do widget e com um sufixo "copy" no nome do widget. Você pode facilmente fazer todas as alterações necessárias e salvar o novo widget. O widget será colocado na parte inferior do seu painel de controle, e você pode posicioná-lo conforme necessário. Lembre-se de salvar seu painel quando todas as alterações estiverem concluídas.

Exibindo legendas do widget

A maioria dos widgets em painéis pode ser exibida com ou sem legendas. Legendas em widgets podem ser ativadas ou desativadas em um painel por um dos seguintes métodos:

- Ao exibir o painel, clique no botão **Opções** no widget e selecione **Mostrar Legendas** no menu.

À medida que os dados exibidos no widget mudam, a legenda desse widget é atualizada dinamicamente.

Quando legendas são exibidas, se a página de destino do ativo indicado pela legenda puder ser navegada, a legenda será exibida como um link para essa página de ativo. Se a legenda exibir "todos", clicar no link exibirá uma página de consulta correspondente à primeira consulta no widget.

Métricas transformadoras

O Insights de infraestrutura de dados fornece diferentes opções **Transform** para determinadas métricas em widgets (especificamente, aquelas métricas chamadas "personalizadas" ou métricas de integração, como do

Kubernetes, dados avançados do ONTAP, plugins do Telegraf, etc.), permitindo que você exiba os dados de várias maneiras. Ao adicionar métricas transformáveis a um widget, você é apresentado com uma lista suspensa fornecendo as seguintes opções de transformação:

Nenhum

Os dados são apresentados como estão, sem manipulação.

Taxa

Valor atual dividido pelo intervalo de tempo desde a observação anterior.

Cumulativo

A acumulação da soma dos valores anteriores e do valor atual.

Delta

A diferença entre o valor de observação anterior e o valor atual.

Taxa Delta

Valor Delta dividido pelo intervalo de tempo desde a observação anterior.

Taxa acumulada

Valor cumulativo dividido pelo intervalo de tempo desde a observação anterior.

Observe que transformar métricas não altera os dados subjacentes em si, mas apenas a maneira como os dados são exibidos.

Consultas e filtros de widgets do painel

Consultas

A consulta em um widget de painel é uma ferramenta poderosa para gerenciar a exibição de seus dados. Aqui estão algumas coisas a observar sobre consultas de widget.

Alguns widgets podem ter até cinco consultas. Cada consulta plotará seu próprio conjunto de linhas ou gráficos no widget. A configuração de rollup, agrupamento, resultados de cima/baixo, etc. em uma consulta não afeta nenhuma outra consulta para o widget.

Você pode clicar no ícone de olho para ocultar temporariamente uma consulta. O widget exibe atualizações automaticamente quando você oculta ou mostra uma consulta. Isso permite que você verifique seus dados exibidos para consultas individuais à medida que você cria seu widget.

Os seguintes tipos de widget podem ter várias consultas:

- Gráfico de área
- Gráfico de área empilhada
- Gráfico de linhas
- Gráfico de estrias
- Widget de valor único

Os restantes tipos de widget podem ter apenas uma única consulta:

- Tabela

- Gráfico de barras
- Gráfico de caixa
- Gráfico de dispersão

Filtragem em consultas de widget de painel

Aqui estão algumas coisas que você pode fazer para tirar o máximo proveito de seus filtros.

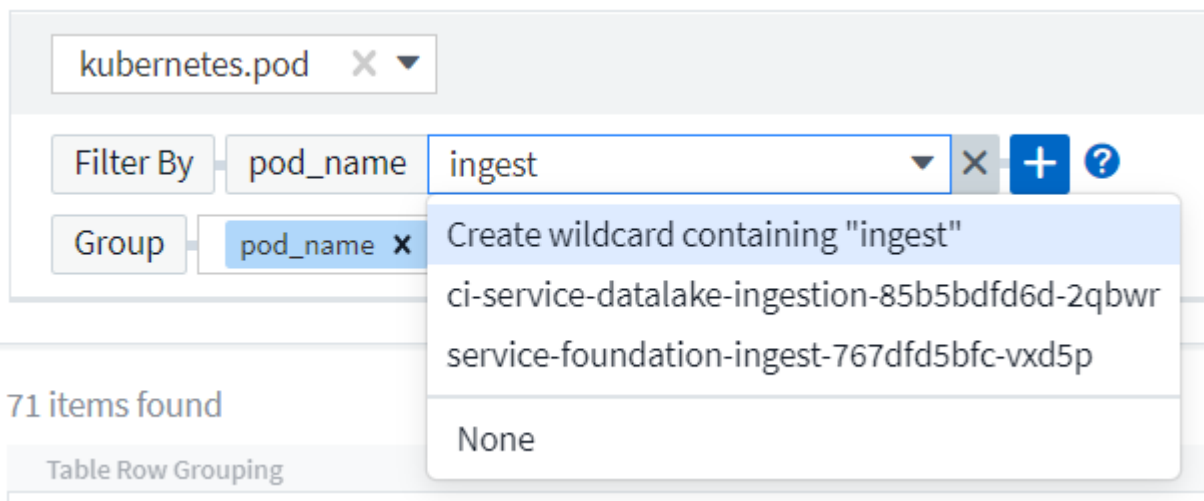
Filtragem de correspondência exata

Se você incluir uma string de filtro em aspas duplas, o Insight trata tudo entre a primeira e a última citação como uma correspondência exata. Quaisquer caracteres especiais ou operadores dentro das aspas serão tratados como literais. Por exemplo, a filtragem para "*" retornará resultados que são um asterisco literal; o asterisco não será tratado como um curinga neste caso. Os operadores E, OU, e NÃO também serão tratados como strings literais quando incluídos em aspas duplas.

Você pode usar filtros de correspondência exata para encontrar recursos específicos, por exemplo, nome de host. Se você quiser encontrar apenas o nome de host 'marketing', mas excluir 'arketing01', 'marketing-boston', etc., simplesmente inclua o nome "marketing" em aspas duplas.

Curingas e expressões

Quando você está filtrando valores de texto ou lista em consultas ou widgets de painel, à medida que você começa a digitar, você recebe a opção de criar um filtro * curinga* com base no texto atual. Selecionar esta opção irá retornar todos os resultados que correspondem à expressão curinga. Você também pode criar **expressões** usando NOT OU OU, ou pode selecionar a opção "nenhum" para filtrar valores nulos no campo.



Os filtros baseados em caracteres universais ou expressões (por exemplo, NÃO, OU, "nenhum", etc.) são exibidos em azul escuro no campo de filtro. Os itens que você selecionar diretamente da lista são exibidos em azul claro.

kubernetes.pod X ▼

Filter By pod_name *ingest* X ci-service-audit-5f775dd975-brfdc X X ▼ X + ?

Group pod_name X X ▼

3 items found

pod_name
ci-service-audit-5f775dd975-brfdc
ci-service-datalake-ingestion-85b5bdfd6d-2qbwr
service-foundation-ingest-767dfd5bfc-vxd5p

Observe que a filtragem de caracteres curinga e expressão funciona com texto ou listas, mas não com valores numéricos, datas ou booleanos.

Filtragem de texto avançada com sugestões contextuais de tipo à frente

A filtragem em consultas de widget é *contextual*; quando você seleciona um valor de filtro ou valores para um campo, os outros filtros dessa consulta mostrarão valores relevantes para esse filtro. Por exemplo, ao definir um filtro para um objeto específico *Name*, o campo a filtrar para *Model* mostrará apenas valores relevantes para esse nome de objeto.

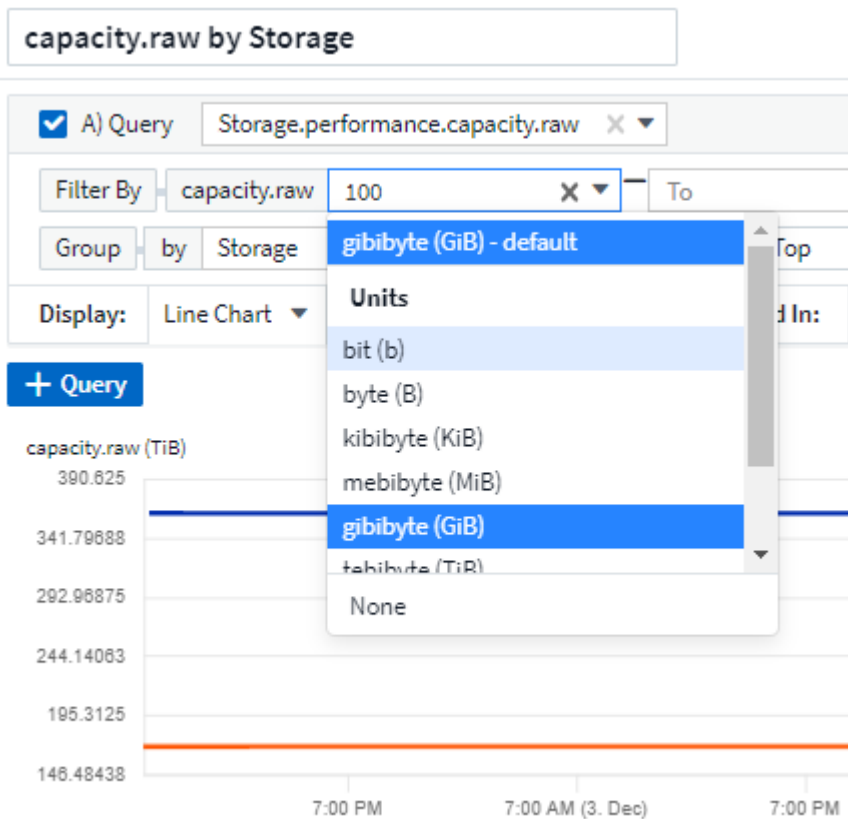
A filtragem contextual também se aplica a variáveis de página do painel (atributos de tipo de texto ou anotações somente). Quando você seleciona um valor de filter para uma variável, quaisquer outras variáveis que usam objetos relacionados só mostrarão possíveis valores de filtro com base no contexto dessas variáveis relacionadas.

Observe que somente filtros de texto mostrarão sugestões contextuais de tipo à frente. Data, Enum (lista), etc. não mostrará sugestões de tipo antecipada. Dito isto, você *pode* definir um filtro em um campo Enum (ou seja, lista) e ter outros campos de texto ser filtrados em contexto. Por exemplo, selecionar um valor em um campo Enum como o Data Center, em seguida, outros filtros mostrarão apenas os modelos/nomes nesse data center), mas não vice-versa.

O intervalo de tempo selecionado também fornecerá contexto para os dados mostrados nos filtros.

Escolher as unidades de filtro

Ao digitar um valor em um campo de filtro, você pode selecionar as unidades nas quais exibir os valores no gráfico. Por exemplo, você pode filtrar a capacidade bruta e optar por exibir no GiB surdez ou selecionar outro formato, como TIB. Isso é útil se você tiver vários gráficos no painel mostrando valores no TIB e quiser que todos os gráficos mostrem valores consistentes.



Refinamentos adicionais de filtragem

O seguinte pode ser usado para refinar ainda mais seus filtros.

- Um asterisco permite que você procure por tudo. Por exemplo,

```
vol*rhel
```

exibe todos os recursos que começam com "vol" e terminam com "rhel".

- O ponto de interrogação permite procurar um número específico de caracteres. Por exemplo,

```
BOS-PRD??-S12
```

Exibe *BOS-PRD12-S12*, *BOS-PRD13-S12* e assim por diante.

- O OPERADOR OU permite especificar várias entidades. Por exemplo,

```
FAS2240 OR CX600 OR FAS3270
```

encontra vários modelos de armazenamento.

- O operador NOT permite excluir texto dos resultados da pesquisa. Por exemplo,

NOT EMC*

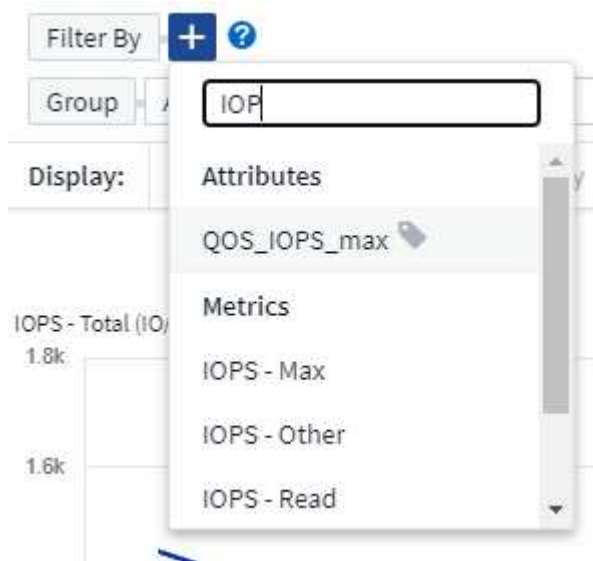
Encontra tudo o que não começa com "EMC". Você pode usar

NOT *

para exibir campos que não contêm nenhum valor.

Identificar objetos retornados por consultas e filtros

Os objetos retornados por consultas e filtros são semelhantes aos mostrados na ilustração a seguir. Objetos com 'tags' atribuídos a eles são anotações enquanto os objetos sem tags são contadores de desempenho ou atributos de objeto.



Agrupamento e agregação

Agrupamento (rolando para cima)

Os dados exibidos em um widget são agrupados (às vezes chamados de rolados) a partir dos pontos de dados subjacentes coletados durante a aquisição. Por exemplo, se você tiver um widget de gráfico de linha mostrando Storage IOPS ao longo do tempo, talvez queira ver uma linha separada para cada um dos seus data centers, para uma comparação rápida. Você pode optar por agrupar esses dados de várias maneiras:

- **Média:** Exibe cada linha como a *média* dos dados subjacentes.
- **Maximum:** Exibe cada linha como *maximum* dos dados subjacentes.
- **Minimum:** Exibe cada linha como *minimum* dos dados subjacentes.
- **Soma:** Exibe cada linha como *soma* dos dados subjacentes.
- **Count:** Exibe uma *count* de objetos que relataram dados dentro do período de tempo especificado. Você pode escolher a janela de tempo *inteiro* conforme determinado pelo intervalo de tempo do painel.

Passos

Para definir o método de agrupamento, faça o seguinte.

1. Na consulta do seu widget, escolha um tipo de ativo e uma métrica (por exemplo, *Storage*) e métrica (como *Performance IOPS Total*).
2. Para **Group**, escolha um método de implementação (como *Average*) e selecione os atributos ou métricas pelos quais os dados serão gerados (por exemplo, *Data Center*).

O widget é atualizado automaticamente e mostra os dados para cada um dos seus data centers.

Você também pode optar por agrupar *all* dos dados subjacentes no gráfico ou tabela. Nesse caso, você obterá uma única linha para cada consulta no widget, que mostrará a média, min, Max, soma ou contagem da métrica ou métricas escolhidas para todos os ativos subjacentes.

Clicar na legenda de qualquer widget cujos dados estão agrupados por "todos" abre uma página de consulta mostrando os resultados da primeira consulta usada no widget.

Se você tiver definido um filtro para a consulta, os dados serão agrupados com base nos dados filtrados.

Observe que quando você optar por agrupar um widget por qualquer campo (por exemplo, *Model*), você ainda precisará filtrar por esse campo para exibir adequadamente os dados desse campo no gráfico ou tabela.

Agregando dados

Você pode alinhar ainda mais seus gráficos de séries temporais (linha, área, etc.) agregando pontos de dados em intervalos de minuto, hora ou dia antes que esses dados sejam posteriormente agrupados por atributo (se escolhido). Você pode optar por agregar pontos de dados de acordo com sua *média*, *máxima*, *mínima*, *soma* ou *contagem*.

Um pequeno intervalo combinado com um longo intervalo de tempo pode resultar em um aviso de "intervalo de agregação resultou em muitos pontos de dados." Você pode ver isso se tiver um intervalo pequeno e aumentar o período de tempo do painel para 7 dias. Neste caso, o Insight aumentará temporariamente o intervalo de agregação até selecionar um período de tempo menor.

Você também pode agregar dados no widget de gráfico de barras e no widget de valor único.

A maioria dos contadores de ativos se agrega a *medium* por padrão. Alguns contadores se agregam a *Max*, *min* ou *sum* por padrão. Por exemplo, erros de porta se agregam a *sum* por padrão, onde as IOPS de armazenamento se agregam a *medium*.

Mostrando resultados superiores/inferiores

Em um widget de gráfico, você pode mostrar os resultados **Top** ou **Bottom** para dados acumulados e escolher o número de resultados mostrados na lista suspensa fornecida. Em um widget de tabela, você pode classificar por qualquer coluna.

Widget Gráfico superior/inferior

Em um widget de gráfico, quando você escolhe agrupar dados por um atributo específico, você tem a opção de exibir os resultados N superior ou N inferior. Observe que você não pode escolher os resultados superiores ou inferiores quando optar por rollup por atributos *all*.

Você pode escolher os resultados a serem exibidos escolhendo **Top** ou **Bottom** no campo **Show** da consulta e selecionando um valor na lista fornecida.

Widget de tabela mostra entradas

Em um widget de tabela, você pode selecionar o número de resultados mostrados nos resultados da tabela. Não é dada a opção de escolher resultados superiores ou inferiores porque a tabela permite classificar ascendente ou descendente por qualquer coluna sob demanda.

Você pode escolher o número de resultados a serem exibidos na tabela no painel selecionando um valor no campo **Mostrar entradas** da consulta.

Agrupando no Widget Tabela

Os dados em um widget de tabela podem ser agrupados por qualquer atributo disponível, permitindo que você veja uma visão geral de seus dados e detalhe-os para mais detalhes. As métricas na tabela são agrupadas para facilitar a visualização em cada linha colapsada.

Os widgets da tabela permitem agrupar os dados com base nos atributos definidos. Por exemplo, você pode querer que sua tabela mostre o total de IOPS de armazenamento agrupado pelos data centers em que esses armazenamentos estão ativos. Ou você pode querer exibir uma tabela de máquinas virtuais agrupadas de acordo com o hipervisor que as hospeda. Na lista, você pode expandir cada grupo para exibir os ativos nesse grupo.

O agrupamento só está disponível no tipo de widget Tabela.

Exemplo de agrupamento (com rollup explicado)

Os widgets da tabela permitem agrupar dados para facilitar a exibição.

Neste exemplo, criaremos um widget de tabela mostrando todas as VMs agrupadas por Data Center.

Passos

1. Crie ou abra um dashboard e adicione um widget **Tabela**.
2. Selecione *Virtual Machine* como o tipo de ativo para este widget.
3. Clique no Seletor de coluna e escolha *Nome do hipervisor* e *IOPS - Total*.

Essas colunas são agora exibidas na tabela.

4. Vamos ignorar qualquer VM sem IOPS e incluir apenas VMs com IOPS total superior a 1. Clique no botão **Filtrar por** e selecione *IOPS - Total*. Clique em *any*, e no campo **de**, digite **1**. Deixe o campo **to** vazio. Clique no campo de filtro para aplicar o filtro.

A tabela agora mostra todas as VMs com IOPS total maior ou igual a 1. Observe que não há agrupamento na tabela. Todas as VMs são mostradas.

5. Clique no botão **Agrupar por []**.

Você pode agrupar por qualquer atributo ou anotação mostrada. Escolha *all* para exibir todas as VMs em um único grupo.

Qualquer cabeçalho de coluna para uma métrica de desempenho exibe um menu "três pontos" contendo uma opção **Roll up**. O método de rolagem padrão é *Average*. Isso significa que o número mostrado para o grupo é a média de todo o total de IOPS relatado para cada VM dentro do grupo. Você pode optar por rolar essa coluna por *média*, *soma*, *mínimo* ou *máximo*. Qualquer coluna exibida que contenha métricas de desempenho pode ser agrupada individualmente.



6. Clique em *All* e selecione *Hypervisor name*.

A lista de VM agora é agrupada por Hypervisor. É possível expandir cada hipervisor para visualizar as VMs hospedadas por ele.

7. Clique em **Salvar** para salvar a tabela no painel. Você pode redimensionar ou mover o widget conforme desejado.

8. Clique em **Salvar** para salvar o painel.

Implementação de dados de desempenho

Se você incluir uma coluna para dados de desempenho (por exemplo, *IOPS - Total*) em um widget de tabela, quando você optar por agrupar os dados, poderá escolher um método de rolagem para essa coluna. O método de rolagem padrão é exibir a média (*avg*) dos dados subjacentes na linha do grupo. Você também pode optar por exibir a soma, o mínimo ou o máximo dos dados.

Seletor de gama de tempo do tablier

Você pode selecionar o intervalo de tempo para os dados do painel. Apenas os dados relevantes para o intervalo de tempo selecionado serão apresentados nos widgets no painel de instrumentos. Pode selecionar entre os seguintes intervalos de tempo:

- Durar 15 minutos
- Durar 30 minutos
- Durar 60 minutos
- Últimas 2 horas
- Últimas 3 horas (este é o padrão)
- Últimas 6 horas
- Últimas 12 horas
- Últimas 24 horas
- Últimos 2 dias

- Últimos 3 dias
- Últimos 7 dias
- Últimos 30 dias
- Intervalo de tempo personalizado

O intervalo de tempo personalizado permite-lhe seleccionar até 31 dias consecutivos. Também pode definir a hora de início e a hora de fim do dia para este intervalo. A hora de Início padrão é 12:00 AM no primeiro dia seleccionado e a hora de término padrão é 11:59 PM no último dia seleccionado. Clicar em **Apply** aplicará o intervalo de tempo personalizado ao painel.

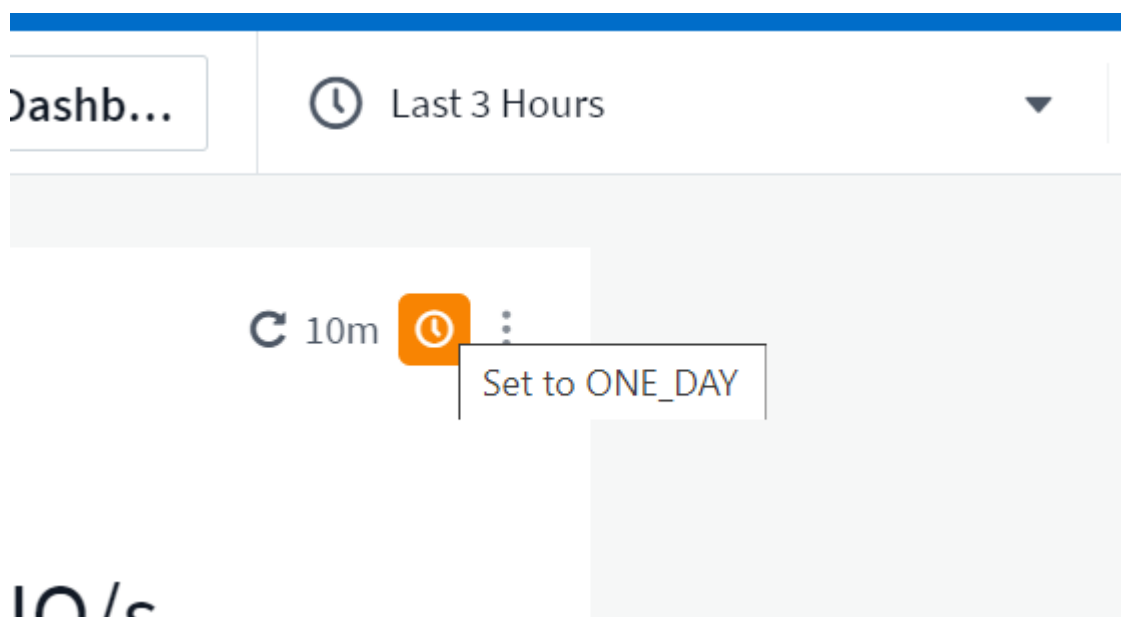
Substituindo o tempo do Painel em widgets individuais

Você pode substituir a configuração de intervalo de tempo do painel principal em widgets individuais. Esses widgets exibirão dados com base no período de tempo definido, não no período de tempo do painel.

Para substituir o tempo do painel e forçar um widget a usar seu próprio período de tempo, no modo de edição do widget, escolha o intervalo de tempo deisired e salve o widget no painel.

O widget exibirá seus dados de acordo com o cronograma definido para ele, independentemente do período de tempo seleccionado no próprio painel.

O período de tempo definido para um widget não afetará nenhum outro widget no painel.



Eixo primário e secundário

Diferentes métricas usam diferentes unidades de medidas para os dados que relatam em um gráfico. Por exemplo, quando se olha para IOPS, a unidade de medida é o número de operações de e/S por segundo de tempo (e/S), enquanto a latência é puramente uma medida de tempo (milissegundos, microssegundos, segundos, etc.). Ao mapear ambas as métricas em um gráfico de linha única usando um único conjunto de valores a para o eixo Y, os números de latência (normalmente um punhado de milissegundos) são mapeados na mesma escala com o IOPS (normalmente numerando nos milhares), e a linha de latência se perde nessa escala.

Mas é possível traçar ambos os conjuntos de dados em um único gráfico significativo, definindo uma unidade

de medida no eixo Y primário (lado esquerdo) e a outra unidade de medida no eixo Y secundário (lado direito). Cada métrica é mapeada em sua própria escala.

Passos

Este exemplo ilustra o conceito de eixos primários e secundários em um widget de gráfico.

1. Crie ou abra um painel. Adicione um gráfico de linha, gráfico de spline, gráfico de área ou widget de gráfico de área empilhada ao painel.
2. Selecione um tipo de ativo (por exemplo *Storage*) e escolha *IOPS - Total* para sua primeira métrica. Defina os filtros que você quiser e escolha um método de roll-up, se desejado.

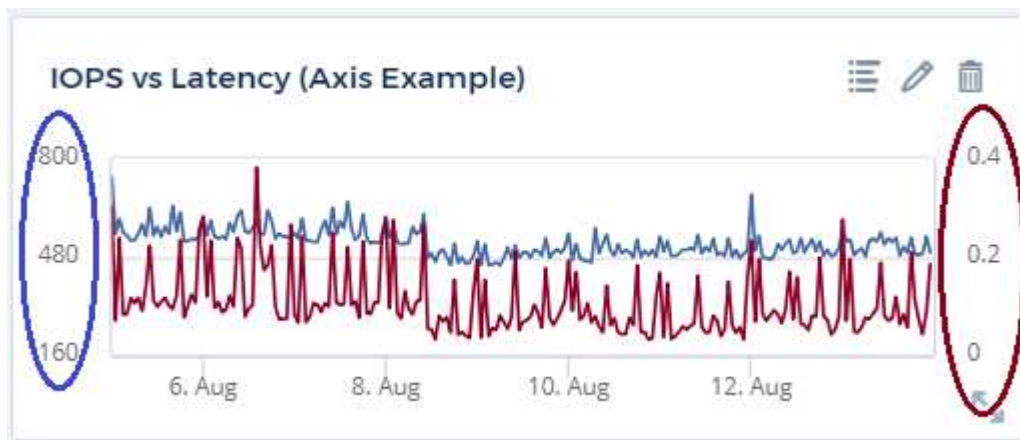
A linha IOPS é exibida no gráfico, com sua escala mostrada à esquerda.

3. Clique em **[-Query]** para adicionar uma segunda linha ao gráfico. Para esta linha, escolha *latência - total* para a métrica.

Observe que a linha é exibida na parte inferior do gráfico. Isso ocorre porque está sendo desenhado *na mesma escala* da linha IOPS.

4. Na consulta de latência, selecione **eixo Y: Secundário**.

A linha de latência agora é desenhada em sua própria escala, que é exibida no lado direito do gráfico.



Expressões em widgets

Em um painel, qualquer widget de séries temporais (linha, spline, área, área empilhada) gráfico de barras, gráfico de colunas, gráfico de pizza ou widget de tabela permite criar expressões a partir de métricas que você escolher e mostrar o resultado dessas expressões em um único gráfico (ou coluna no caso do [widget da tabela](#)). Os exemplos a seguir usam expressões para resolver problemas específicos. No primeiro exemplo, queremos mostrar IOPS de leitura como uma porcentagem do total de IOPS para todos os ativos de storage no locatário. O segundo exemplo dá visibilidade ao IOPS "do sistema" ou "sobrecarga" que ocorre no locatário - aqueles IOPS que não são diretamente da leitura ou da gravação de dados.

Você pode usar variáveis em expressões (por exemplo, `_ Var1 * 100_`)

Exemplo de expressões: Ler porcentagem de IOPS

Neste exemplo, queremos mostrar IOPS de leitura como uma porcentagem do total de IOPS. Você pode pensar nisso como a seguinte fórmula:

```
Read Percentage = (Read IOPS / Total IOPS) x 100
```

Esses dados podem ser exibidos em um gráfico de linhas no painel. Para fazer isso, siga estas etapas:

Passos

1. Crie um novo painel ou abra um painel existente no modo de edição.
2. Adicione um widget ao painel. Escolha **Gráfico de área**.

O widget abre no modo de edição. Por padrão, uma consulta é exibida mostrando *IOPS - Total* para ativos *Storage*. Se desejar, selecione um tipo de ativo diferente.

3. Clique no link **Converter para expressão** à direita.

A consulta atual é convertida em modo de expressão. Observe que você não pode alterar o tipo de ativo enquanto estiver no modo expressão. Enquanto você estiver no modo expressão, o link muda para **Revert to Query**. Clique aqui se desejar voltar ao modo consulta a qualquer momento. Esteja ciente de que alternar entre modos irá redefinir os campos para seus padrões.

Por enquanto, permaneça no modo de expressão.

4. A métrica **IOPS - total** está agora no campo variável alfabética "**a**". No campo variável "**b**", clique em **Select** e escolha **IOPS - Read**.

Você pode adicionar até um total de cinco variáveis alfabéticas para a sua expressão clicando no botão mais seguindo os campos variáveis. Para nosso exemplo de porcentagem de leitura, precisamos apenas de IOPS total ("**a**") e IOPS de leitura ("**b**").

5. No campo **expression**, você usa as letras correspondentes a cada variável para construir sua expressão. Sabemos que a porcentagem de leitura (ler IOPS/IOPS total) x 100, então escreveríamos esta expressão como:

```
(b / a) * 100
```

- . O campo **Label** identifica a expressão. Altere o rótulo para "porcentagem de leitura", ou algo igualmente significativo para você.
- . Altere o campo **Units** para "%" ou "Percent".

O gráfico exibe a porcentagem de leitura de IOPS ao longo do tempo para os dispositivos de armazenamento escolhidos. Se desejar, você pode definir um filtro ou escolher um método de *rollup* diferente. Esteja ciente de que, se você selecionar soma como o método *rollup*, todos os valores percentuais serão adicionados juntos, o que pode potencialmente ir mais alto que 100%.

6. Clique em **Salvar** para salvar o gráfico em seu painel.

Expressões exemplo: I/O "System"

Exemplo 2: Entre as métricas coletadas de fontes de dados estão leitura, gravação e IOPS total. No entanto, o número total de IOPS relatado por uma fonte de dados às vezes inclui IOPS "do sistema", que são as operações de e/S que não são parte direta da leitura ou gravação de dados. Esta e/S do sistema também pode ser considerada como e/S "overhead", necessária para uma operação adequada do sistema, mas não diretamente relacionada com as operações de dados.

Para mostrar essas I/os do sistema, você pode subtrair IOPS de leitura e gravação do total de IOPS relatado da aquisição. A fórmula pode ser assim:

$$\text{System IOPS} = \text{Total IOPS} - (\text{Read IOPS} + \text{Write IOPS})$$

Esses dados podem ser exibidos em um gráfico de linha no painel. Para fazer isso, siga estas etapas:

Passos

1. Crie um novo painel ou abra um painel existente no modo de edição.
2. Adicione um widget ao painel. Escolha **Gráfico de linha**.

O widget abre no modo de edição. Por padrão, uma consulta é exibida mostrando *IOPS - Total* para ativos *Storage*. Se desejar, selecione um tipo de ativo diferente.

3. No campo **Roll Up**, escolha *sum* por *all*.

O gráfico exibe uma linha mostrando a soma do total de IOPS.

4. Clique no ícone *duplicar esta consulta* para criar uma cópia da consulta.

Uma cópia da consulta é adicionada abaixo do original.

5. Na segunda consulta, clique no botão **Converter para expressão**.

A consulta atual é convertida em modo de expressão. Clique em **Revert to Query** se desejar voltar para o modo Query a qualquer momento. Esteja ciente de que alternar entre modos irá redefinir os campos para seus padrões.

Por enquanto, permaneça no modo de expressão.

6. A métrica *IOPS - total* está agora no campo variável alfabética "a". Clique em *IOPS - Total* e mude-o para *IOPS - Read*.
7. No campo variável "b", clique em **Select** e escolha *IOPS - Write*.
8. No campo **expression**, você usa as letras correspondentes a cada variável para construir sua expressão. Nós escreveríamos nossa expressão simplesmente como:

a + b

Na seção Exibir, escolha **Gráfico de área** para essa expressão.

9. O campo **Label** identifica a expressão. Altere o rótulo para "System IOPS" ou algo igualmente significativo para você.

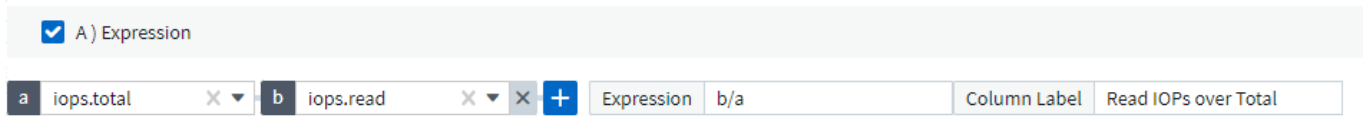
O gráfico exibe o total de IOPS como um gráfico de linha, com um gráfico de área mostrando a combinação de IOPS de leitura e gravação abaixo disso. A lacuna entre os dois mostra as IOPS que não estão diretamente relacionadas às operações de leitura ou gravação de dados. Estas são as suas IOPS do "sistema".

10. Clique em **Salvar** para salvar o gráfico em seu painel.

Para usar uma variável em uma expressão, basta digitar o nome da variável, por exemplo, `_ var1 * 100_`. Somente variáveis numéricas podem ser usadas em expressões.

Expressões em um widget de tabela

Widgets de tabela manipulam expressões um pouco diferente. Você pode ter até cinco expressões em um único widget de tabela, cada uma das quais é adicionada como uma nova coluna à tabela. Cada expressão pode incluir até cinco valores nos quais realizar seu cálculo. Você pode facilmente nomear a coluna algo significativo.



Variáveis

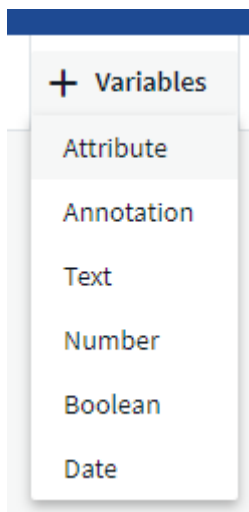
Variáveis permitem alterar os dados exibidos em alguns ou todos os widgets em um painel de uma vez. Ao definir um ou mais widgets para usar uma variável comum, as alterações feitas em um só lugar fazem com que os dados exibidos em cada widget sejam atualizados automaticamente.

As variáveis do dashboard vêm em vários tipos, podem ser usadas em diferentes campos e devem seguir regras para nomear. Estes conceitos são explicados aqui.

Tipos de variáveis

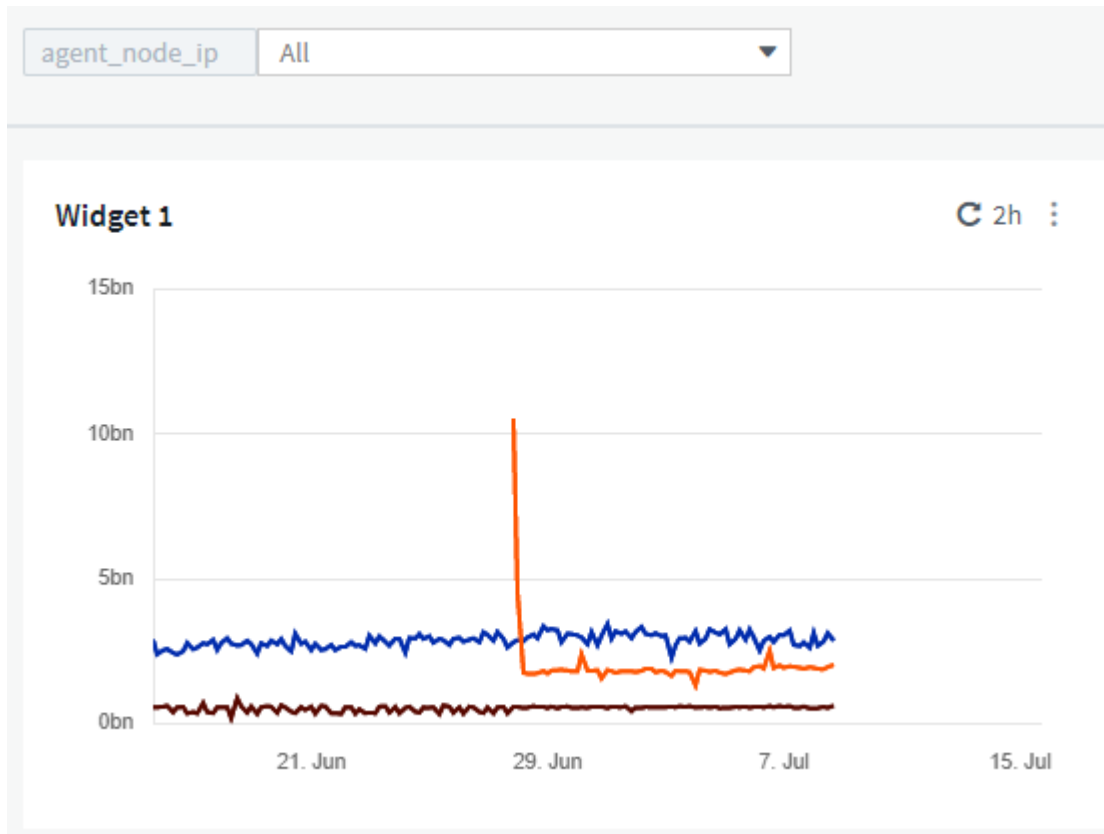
Uma variável pode ser um dos seguintes tipos:

- **Atributo:** Use atributos ou métricas de um objeto para filtrar
- **Anotação:** Use uma pré-definida "Anotação" para filtrar dados do widget.
- **Texto:** Uma cadeia alfanumérica.
- **Numérico:** Um valor numérico. Use por si só, ou como um valor "de" ou "para", dependendo do campo do widget.
- **Boolean:** Use para campos com valores de True/False, Yes/no, etc. para a variável booleana, as opções são Sim, não, nenhum, qualquer.
- **Data:** Um valor de data. Use como um valor "de" ou "para", dependendo da configuração do seu widget.

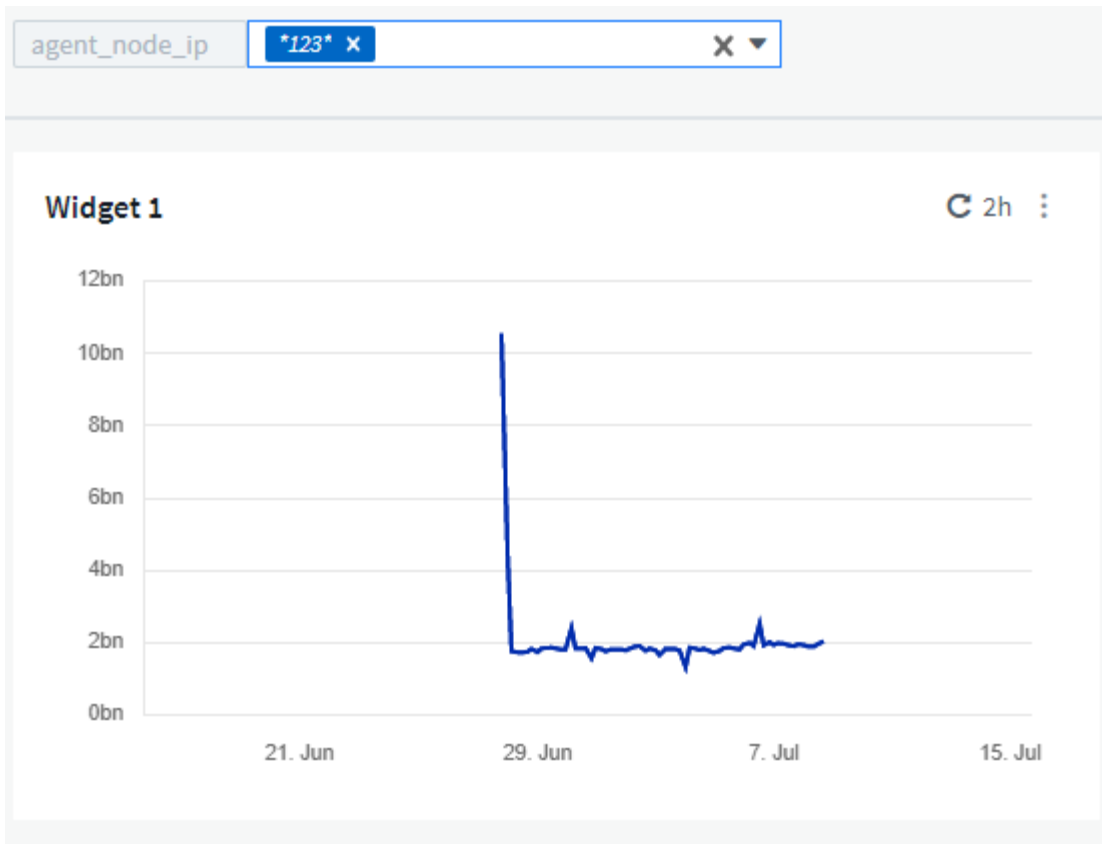


Variáveis de atributo

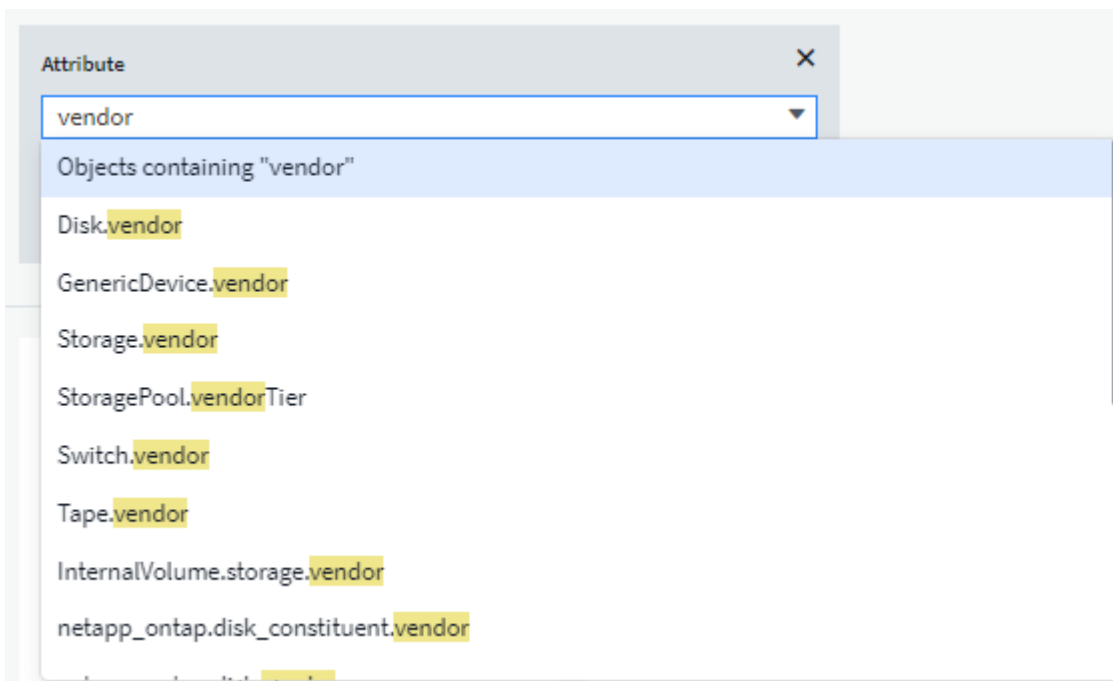
Selecionar uma variável tipo Atributo permite filtrar dados de widget contendo o valor ou valores de atributo especificado. O exemplo abaixo mostra um widget de linha exibindo tendências de memória livre para nós de Agente. Criamos uma variável para IPs de nó de agente, atualmente definida para mostrar todos os IPs:



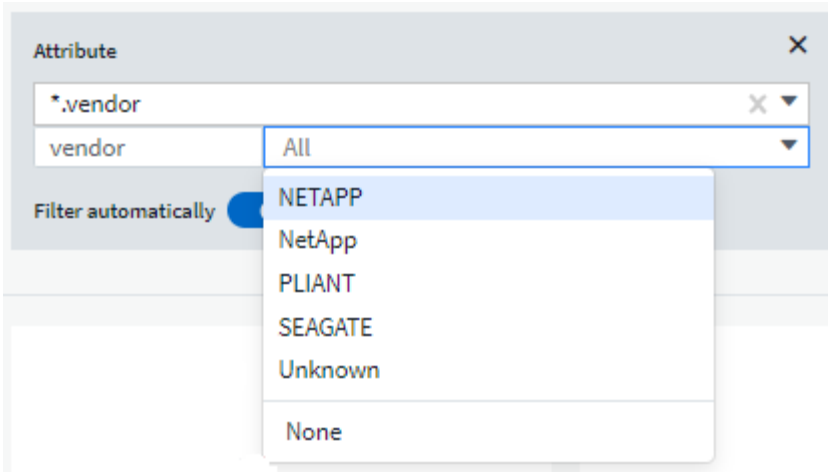
Mas se você quiser ver temporariamente apenas nós em sub-redes individuais em seu locatário, você pode definir ou alterar a variável para um IP ou IPs específicos do nó de agente. Aqui estamos vendo apenas os nós na sub-rede "123":



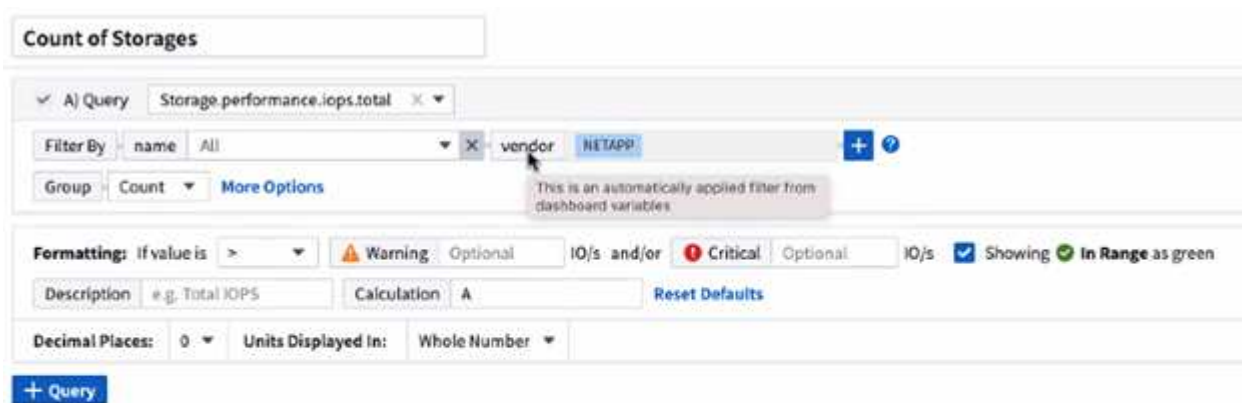
Você também pode definir uma variável para filtrar em objetos *all* com um atributo específico, independentemente do tipo de objeto, por exemplo, objetos com um atributo de "vendedor", especificando **.vendedor* no campo variável. Você não precisa digitar "*"; o Data Infrastructure Insights fornecerá isso se você selecionar a opção curinga.



Quando você lista suspensa a lista de opções para o valor da variável, os resultados são filtrados, portanto, mostre apenas os fornecedores disponíveis com base nos objetos do seu painel.



Se você editar um widget em seu painel onde o filtro de atributo é relevante (ou seja, os objetos do widget contêm qualquer atributo **.vendor*), ele mostrará que o filtro de atributo é aplicado automaticamente.

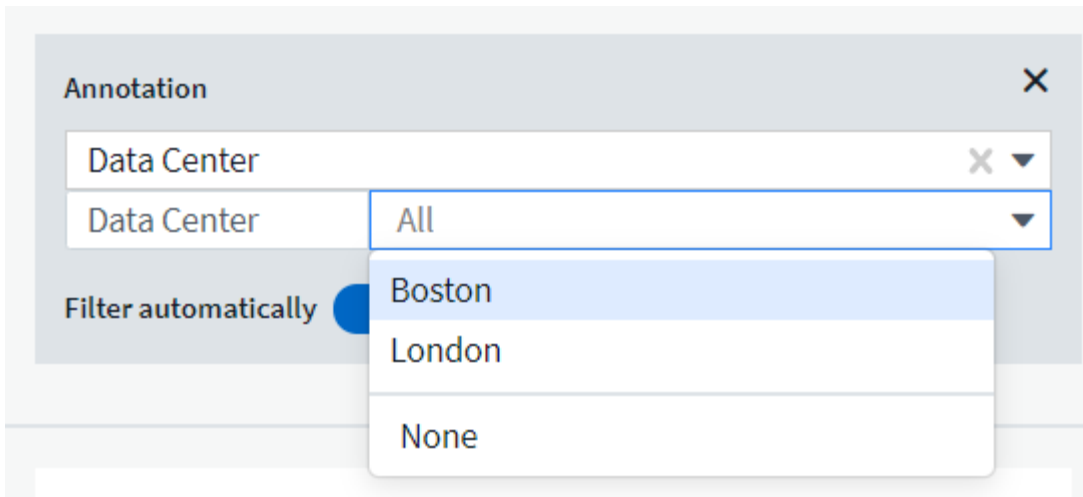


14

Aplicar variáveis é tão fácil quanto alterar os dados de atributos de sua escolha.

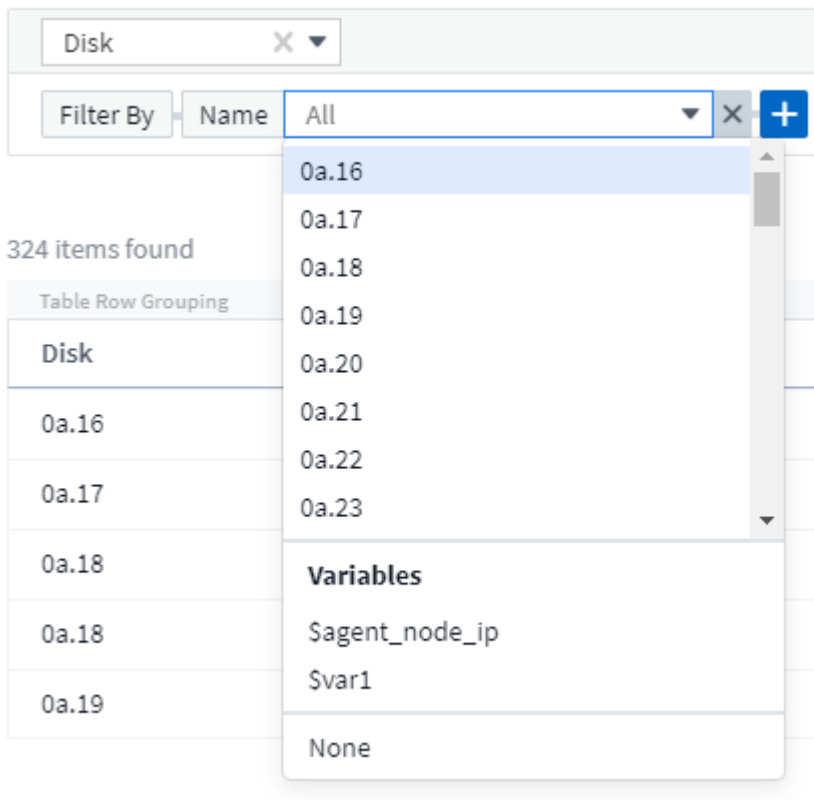
Variáveis de anotação

Escolher uma variável Annotation permite filtrar objetos associados a essa anotação, por exemplo, aqueles pertencentes ao mesmo Data Center.



Texto, número, Data ou variável booleana

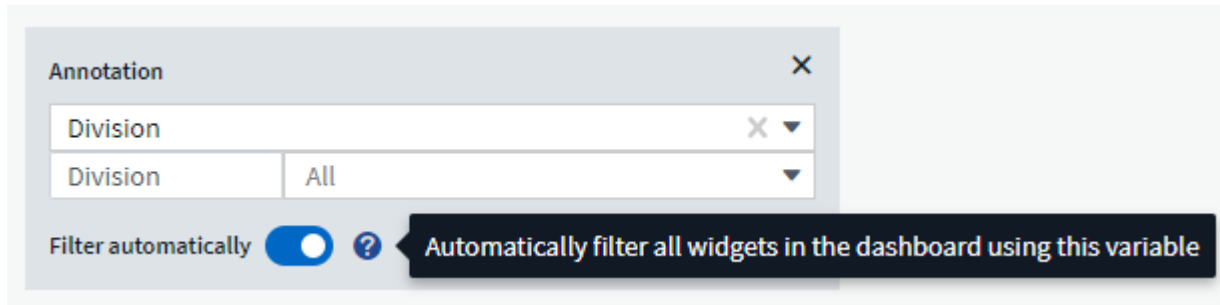
Você pode criar variáveis genéricas que não estão associadas a um atributo específico selecionando um tipo de variável de *Text*, *number*, *boolean* ou *Date*. Uma vez criada a variável, você pode selecioná-la em um campo de filtro de widget. Ao definir um filtro em um widget, além de valores específicos que você pode selecionar para o filtro, todas as variáveis que foram criadas para o painel são exibidas na lista - estas são agrupadas na seção "variáveis" na lista suspensa e têm nomes começando com " Escolher uma variável neste filtro permitirá que você pesquise valores que você insira no campo variável no próprio painel. Todos os widgets que usam essa variável em um filtro serão atualizados dinamicamente.



Escopo do filtro variável

Quando você adiciona uma variável Annotation ou Attribute ao seu painel, a variável pode ser aplicada a *all* widgets no painel, o que significa que todos os widgets no painel exibirão resultados filtrados de acordo com o

valor definido na variável.



Observe que somente as variáveis Atributo e Anotação podem ser filtradas automaticamente assim. As variáveis non-Annotation ou -Attribute não podem ser filtradas automaticamente. Widgets individuais devem ser configurados para usar variáveis desses tipos.

Para desativar a filtragem automática para que a variável se aplique apenas aos widgets onde você a definiu especificamente, clique no controle deslizante "Filtrar automaticamente" para desativá-la.

Para definir uma variável em um widget individual, abra o widget no modo de edição e selecione a anotação ou atributo específico no campo *Filtrar por*. Com uma variável Annotation, você pode selecionar um ou mais valores específicos, ou selecionar o nome da variável (indicado pela entrada "") para permitir digitar a variável no nível do painel. O mesmo se aplica às variáveis Atributo. Apenas os widgets para os quais você definiu a variável mostrará os resultados filtrados.

A filtragem em variáveis é *contextual*; quando você seleciona um valor de filtro ou valores para uma variável, as outras variáveis em sua página mostrarão apenas valores relevantes para esse filtro. Por exemplo, ao definir um filtro de variável para um armazenamento específico *Model*, quaisquer variáveis definidas como filtro para armazenamento *Name* apenas mostrarão valores relevantes para esse modelo.

Para usar uma variável em uma expressão, basta digitar o nome da variável como parte da expressão, por exemplo, `_ var1 * 100_`. Somente variáveis numéricas podem ser usadas em expressões. Não é possível usar as variáveis Anotação numérica ou Atributo em expressões.

A filtragem em variáveis é *contextual*; quando você seleciona um valor de filtro ou valores para uma variável, as outras variáveis em sua página mostrarão apenas valores relevantes para esse filtro. Por exemplo, ao definir um filtro de variável para um armazenamento específico *Model*, quaisquer variáveis definidas como filtro para armazenamento *Name* apenas mostrarão valores relevantes para esse modelo.

Nomenclatura variável

Nomes das variáveis:

- Deve incluir apenas as letras a-z, os dígitos 0-9, ponto (.), sublinhado (_) e espaço ().
- Não pode ter mais de 20 caracteres.
- São sensíveis a maiúsculas e minúsculas: O `CityName` e o `cityname` são variáveis diferentes.
- Não pode ser o mesmo que um nome de variável existente.
- Não pode estar vazio.

Widgets do indicador de formatação

Os widgets Solid e Bullet Gauge permitem definir limites para os níveis *Warning* e/ou *Critical*, fornecendo uma representação clara dos dados que você especificar.

Widget 12 Override Dashboard Time 🕒 ✕

✓ A) Query Storage.performance.iops.total 📄 🗑️

Filter By +


Group Avg Time aggregate by Avg Less Options

Formatting: If value is > ⚠️ Warning 500 IO/s and/or 🔴 Critical 1000 IO/s Showing 🟢 In Range as green

Description IOPS - Total Calculation A Min Value Optional Max Value 1200

Display: Bullet Gauge Decimal Places: 2 Color: ☒ Units Displayed In: Auto Format

+ Query



904.21 IO/s
IOPS - Total

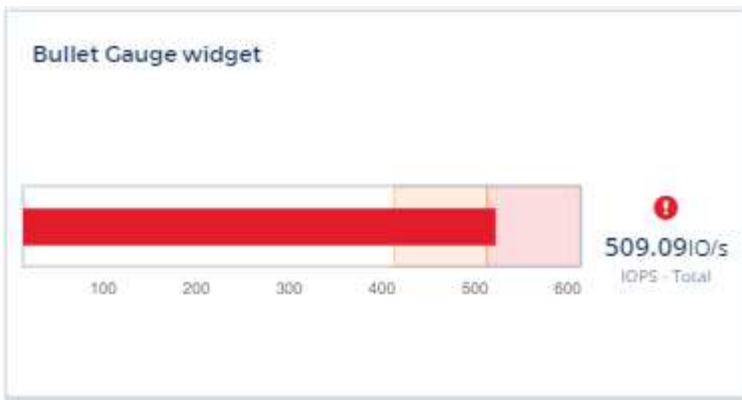
Cancel Save

Para definir a formatação desses widgets, siga estas etapas:

1. Escolha se deseja destacar valores maiores que (>) ou menores que (<) seus limites. Neste exemplo, destacaremos valores superiores a (>) os níveis de limiar.
2. Escolha um valor para o limite "Aviso". Quando o widget apresenta valores superiores a este nível, apresenta o indicador a laranja.
3. Escolha um valor para o limite "crítico". Valores superiores a este nível farão com que o indicador seja apresentado a vermelho.

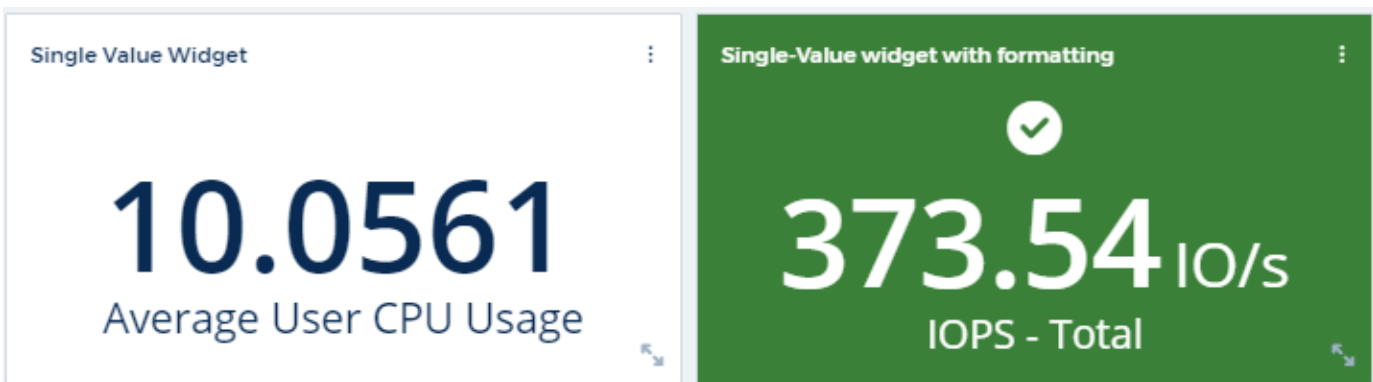
Opcionalmente, você pode escolher um valor mínimo e máximo para o medidor. Os valores abaixo do mínimo não apresentam o indicador. Os valores acima do máximo irão apresentar um indicador completo. Se você não escolher valores mínimos ou máximos, o widget seleciona os valores mínimos e máximos ideais com base no valor do widget.





Formatação Widget de valor único

No widget de valor único, além de definir limites de aviso (laranja) e crítico (vermelho), você pode optar por ter valores "em intervalo" (aqueles abaixo do nível de aviso) exibidos com fundo verde ou branco.



Clicar no link em um widget de valor único ou em um widget de indicador exibirá uma página de consulta correspondente à primeira consulta no widget.

Formatar Widgets de tabela

Como widgets de valor único e de indicador, você pode definir a formatação condicional em widgets de tabela, permitindo destacar dados com cores e/ou ícones especiais.

A formatação condicional permite que você defina e realce limiares de nível de aviso e nível crítico em widgets de tabela, trazendo visibilidade instantânea para outliers e pontos de dados excepcionais.

14 items found in 1 group

Table Row Grouping	Expanded Detail	Metrics & Attributes	
All	Storage Pool	capacityRatio.used (%)	capacity.provisioned (GiB)
All (14)	--	95.15	
--	rtp-sa-cl06-02:aggr_data1_rtp_sa_cl06_02	0.79	
--	rtp-sa-cl06-01:aggr_data1_rtp_sa_cl06_01	2.45	
--	rtp-sa-cl06-02:aggr0_rtp_sa_cl06_02_root	95.15	
--	rtp-sa-cl06-01:aggr0_rtp_sa_cl06_01_root	95.15	

Formatting: Show Expanded Details Conditional Formatting: Background Color + Icon Show In Range as green

Conditional Formatting Settings:

- If value is: > (Greater than)
- Warning: 70 %
- Critical: 90 %

A formatação condicional é definida separadamente para cada coluna de uma tabela. Por exemplo, você pode escolher um conjunto de limites para uma coluna de capacidade e outro conjunto para uma coluna de taxa de transferência.

Se você alterar a exibição de unidade de uma coluna, a formatação condicional permanecerá e refletirá a alteração de valores. As imagens abaixo mostram a mesma formatação condicional, embora a unidade de visualização seja diferente.

The top screenshot shows a table with the column 'capacity.used (GiB)' sorted in descending order. The values are 40,754.06, 10,313.56, 9,544.84, 8,438.99, and 6,671.72. The first two rows are highlighted in red, and the next two in yellow. A context menu is open for the column 'throughput.total (MiB/s)', showing the 'Conditional Formatting' section with a 'Reset' button. The 'If value is' dropdown is set to '> (Greater than)'. The 'Warning' rule is set to 8000 GiB, and the 'Critical' rule is set to 10000 GiB.

The bottom screenshot shows the same table but with the column 'capacity.used (TiB)'. The values are 39.80, 10.07, 9.32, 8.24, and 6.52. The first two rows are highlighted in red, and the next two in yellow. The context menu for 'throughput.total (MiB/s)' is open, showing the 'Unit Display' section with 'Base Unit' set to 'gibibyte (GiB)' and 'Displayed In' set to 'tebibyte (TiB)'. The 'Conditional Formatting' section is also visible, with the 'If value is' dropdown set to '> (Greater than)'. The 'Warning' rule is set to 8000 GiB, and the 'Critical' rule is set to 10000 GiB.

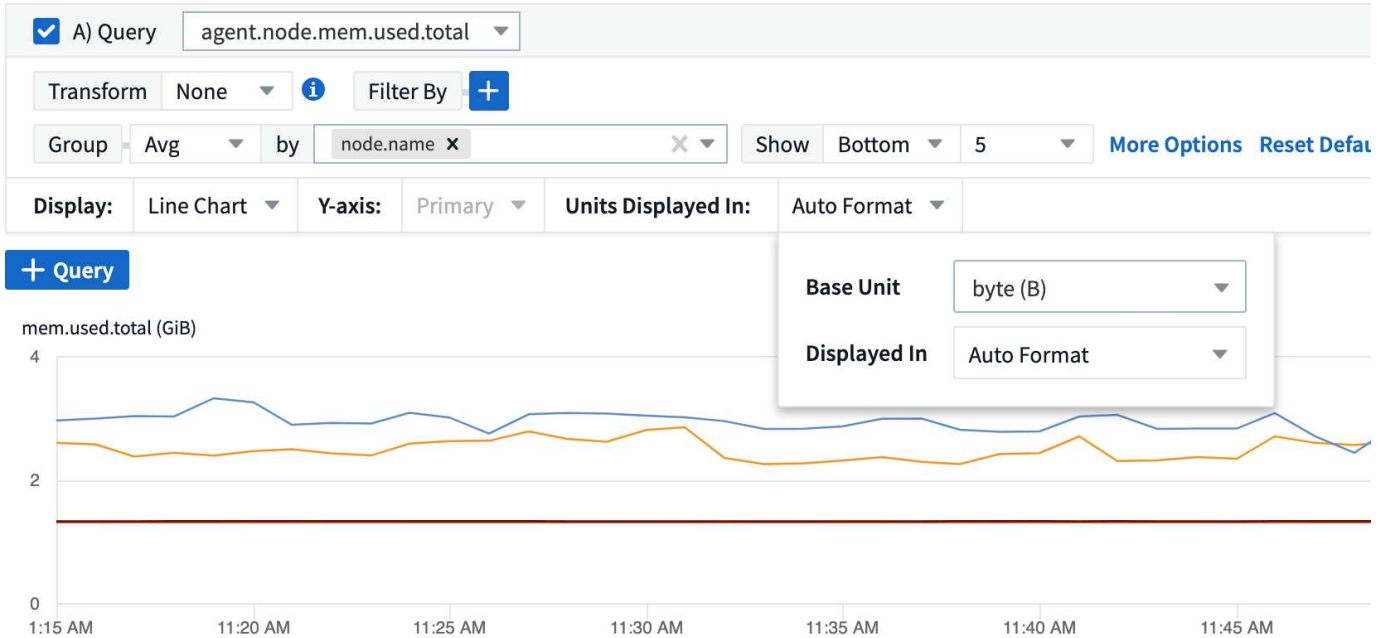
Você pode escolher se deseja exibir a formatação da condição como cor, ícones ou ambos.

Escolhendo a unidade para exibir dados

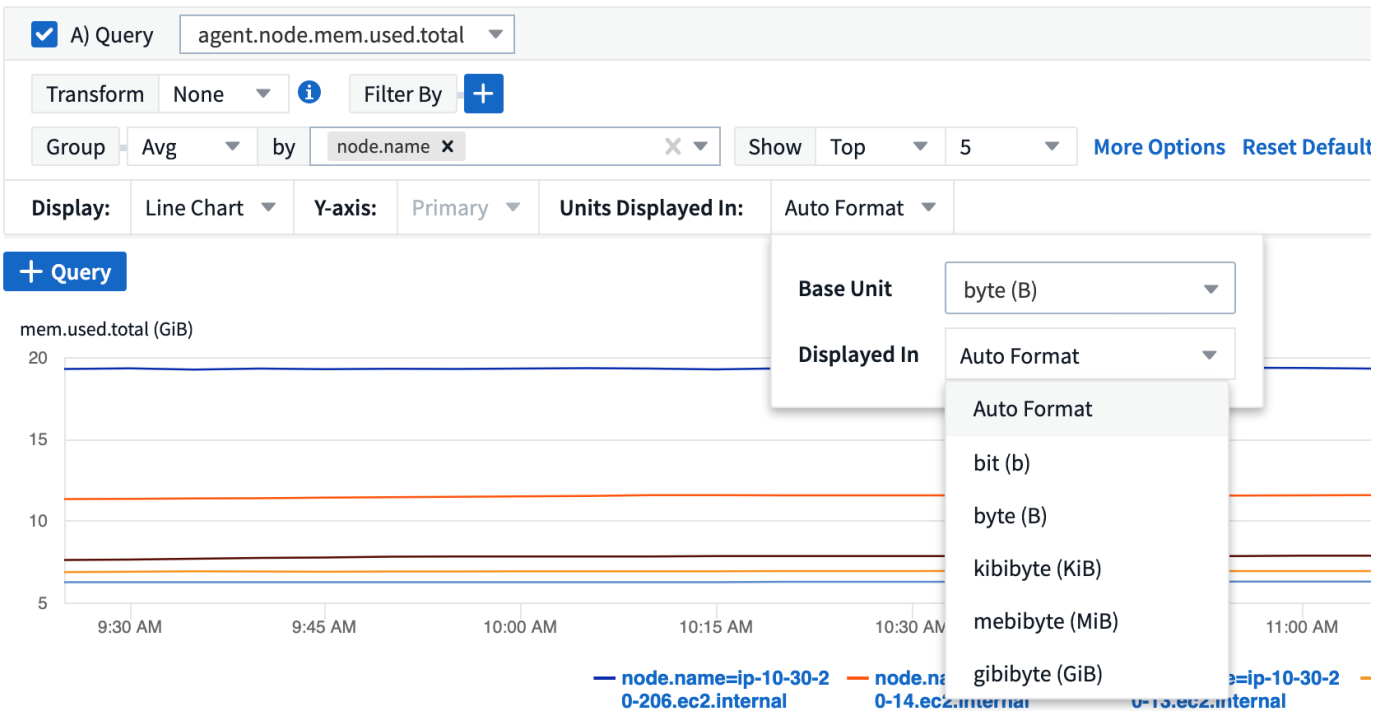
A maioria dos widgets em um painel permite que você especifique as unidades nas quais exibir valores, por exemplo *megabytes*, *milhares*, *porcentagem*, *milissegundos (ms)*, etc. em muitos casos, o Data Infrastructure Insights sabe o melhor formato para os dados que estão sendo adquiridos. Nos casos em que o melhor

formato não é conhecido, você pode definir o formato desejado.

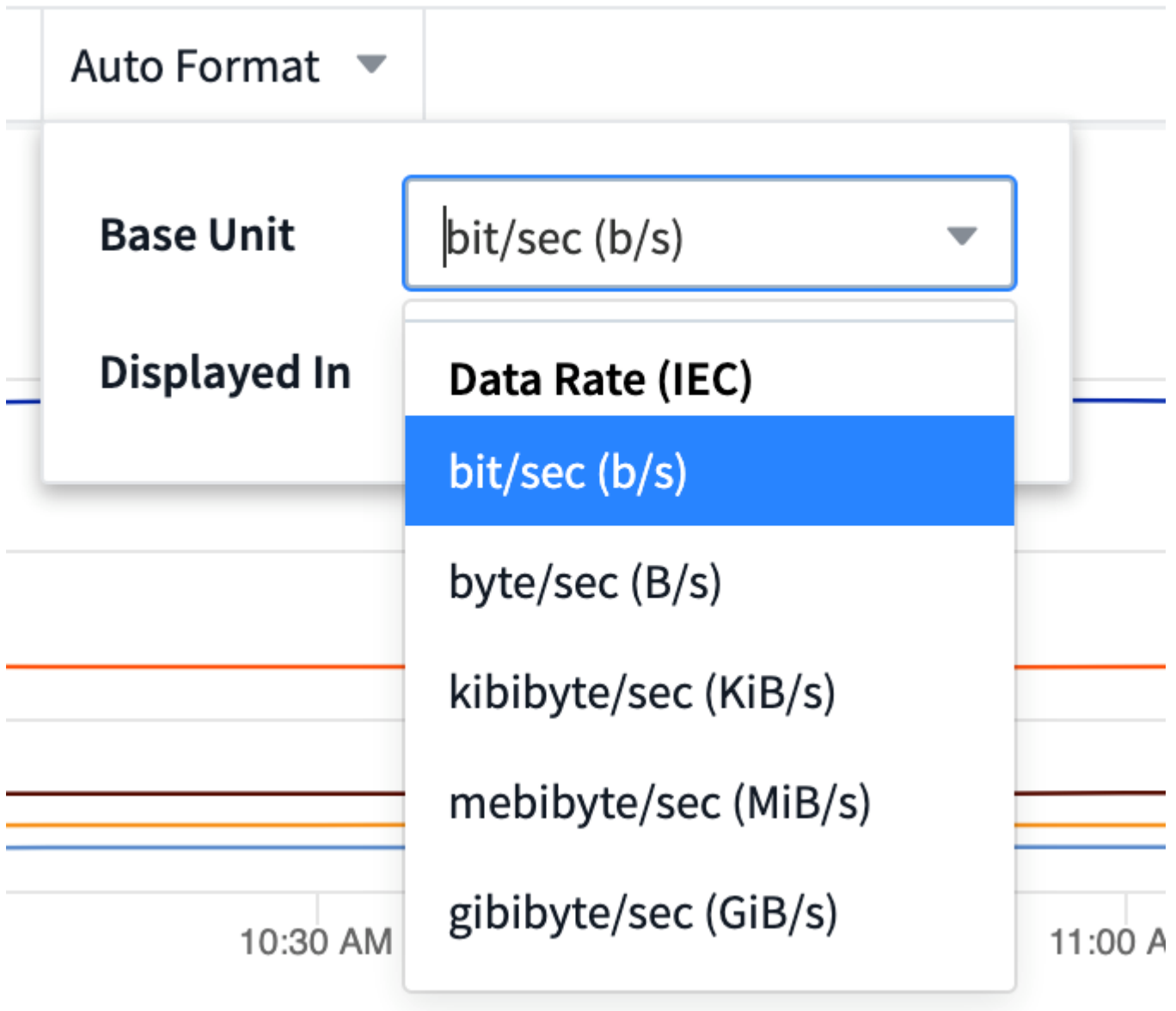
No exemplo de gráfico de linhas abaixo, os dados selecionados para o widget são conhecidos por estarem em *bytes* (a unidade de dados IEC base: Consulte a tabela abaixo), de modo que a Unidade base é selecionada automaticamente como 'byte (B)'. No entanto, os valores de dados são grandes o suficiente para serem apresentados como gibibytes (GiB), então o Data Infrastructure Insights por padrão formata automaticamente os valores como GiB. O eixo Y no gráfico mostra "GiB" como unidade de visualização e todos os valores são apresentados em termos dessa unidade.



Se pretender apresentar o gráfico numa unidade diferente, pode escolher outro formato para apresentar os valores. Como a unidade base neste exemplo é *byte*, você pode escolher entre os formatos suportados "baseados em bytes": Bit (b), byte (B), kibibyte (KiB), mebibyte (MiB), gibibibyte (GiB). O rótulo e os valores do eixo Y mudam de acordo com o formato que você escolher.



Nos casos em que a unidade base não é conhecida, pode atribuir uma unidade entre a "[unidades disponíveis](#)", ou escrever a sua própria. Depois de atribuir uma unidade base, pode seleccionar para apresentar os dados num dos formatos suportados adequados.



Para limpar as configurações e começar de novo, clique em **Redefinir padrões**.

Uma palavra sobre o formato automático

A maioria das métricas são reportadas por coletores de dados na menor unidade, por exemplo, como um número inteiro, como 1.234.567.890 bytes. Por padrão, o Data Infrastructure Insights formata automaticamente o valor para a exibição mais legível. Por exemplo, um valor de dados de 1.234.567.890 bytes seria formatado automaticamente para 1,23 *Gibibytes*. Você pode optar por exibi-lo em outro formato, como *Mebibytes*. O valor será exibido em conformidade.



O Data Infrastructure Insights usa padrões de nomenclatura de números em inglês americano. O "billion" americano equivale a "mil milhões".

Widgets com várias consultas

Se você tiver um widget de série temporal (ou seja, linha, spline, área, área empilhada) que tenha duas consultas onde ambas são plotadas o eixo Y primário, a unidade base não é mostrada na parte superior do eixo Y. No entanto, se seu widget tiver uma consulta no eixo Y primário e uma consulta no eixo Y secundário, as unidades base para cada um serão mostradas.



Se o widget tiver três ou mais consultas, as unidades base não serão mostradas no eixo Y.

Unidades disponíveis

A tabela a seguir mostra todas as unidades disponíveis por categoria.

Categoria	Unidades
Moeda	dólar
Dados (IEC)	byte de bit kibibibibibyte mebibibbyte de byte de byte de byte de byte de byte de byte de byte
DataRate (IEC)	bit/sec byte/sec kibibibyte/sec mebibyte/sec gibibibibibibibibibyte/sec
Dados (métrico)	gigabyte terabyte de petabyte
DataRate (métrica)	megabyte/seg. gigabyte/seg. terabyte/seg. petabyte/seg. exabyte/seg
IEC	kibi mebi gibi tebi pebi exbi
Decimal	número inteiro milhares de milhões de bilião de bilião de biliões
Porcentagem	porcentagem
Tempo	nanossegundos microssegundos milissegundo segundo segundo segundo minuto hora
Temperatura	celsius fahrenheit
Frequência	hertz kilohertz megahertz gigahertz megahertz
CPU	nanonúcleos micronúcleos millicors quilocores megacores gigacores teracores petacores exacores
Taxa de transferência	Operações de e/S/seg. Operações/seg. Solicitações/seg. Leituras/seg. Gravações/seg. Operações/min. Leituras/min. Gravações/min

Modo de TV e Atualização automática

Os dados nos widgets nos painéis e nas páginas de destino do ativo são atualizados automaticamente de acordo com um intervalo de atualização determinado pelo intervalo de tempo do painel selecionado. O intervalo de atualização baseia-se no facto de o widget ser série temporal (linha, spline, área, gráfico de área empilhada) ou não série temporal (todos os outros gráficos).

Intervalo de tempo do tablier	Intervalo de atualização de séries temporais	Intervalo de atualização não-série temporal
Durar 15 minutos	10 segundos	1 minuto
Durar 30 minutos	15 segundos	1 minuto
Durar 60 minutos	15 segundos	1 minuto
Últimas 2 horas	30 segundos	5 minutos
Últimas 3 horas	30 segundos	5 minutos
Últimas 6 horas	1 minuto	5 minutos
Últimas 12 horas	5 minutos	10 minutos
Últimas 24 horas	5 minutos	10 minutos
Últimos 2 dias	10 minutos	10 minutos
Últimos 3 dias	15 minutos	15 minutos
Últimos 7 dias	1 hora	1 hora
Últimos 30 dias	2 horas	2 horas

Cada widget exibe seu intervalo de atualização automática no canto superior direito do widget.

A atualização automática não está disponível para o intervalo de tempo personalizado do painel de instrumentos.

Quando combinado com o **modo de TV**, a atualização automática permite a exibição de dados quase em tempo real em um painel ou página de ativos. O modo de TV oferece uma exibição organizada; o menu de navegação está oculto, proporcionando mais espaço real para a exibição de dados, assim como o botão Editar. O modo de TV ignora os tempos limite típicos do Data Infrastructure Insights, deixando o visor em direto até terminar sessão manual ou automaticamente por protocolos de segurança de autorização.



Como o NetApp BlueXP tem seu próprio tempo limite de login de usuário de 7 dias, o Insights de infraestrutura de dados também deve fazer logout nesse evento. Você pode simplesmente fazer login novamente e seu painel continuará sendo exibido.

- Para ativar o modo de TV, clique no botão modo de TV.
- Para desativar o modo de TV, clique no botão **Exit** (Sair) no canto superior esquerdo do ecrã.

Você pode suspender temporariamente a atualização automática clicando no botão Pausa no canto superior direito. Durante a pausa, o campo de intervalo de tempo do tablier apresenta o intervalo de tempo ativo dos dados em pausa. Os seus dados ainda estão a ser adquiridos e atualizados enquanto a atualização automática está em pausa. Clique no botão continuar para continuar a atualização automática dos dados.



Grupos do painel de instrumentos

O agrupamento permite visualizar e gerenciar painéis relacionados. Por exemplo, você pode ter um grupo de dashboard dedicado ao storage no localatário. Os grupos de painéis são gerenciados na página **painéis > Mostrar todos os painéis**.

Dashboard Groups (3) + ◀

Search groups..

- All Dashboards (60)
- My Dashboards (11)
- Storage Group (7) ⋮

Dashboards (7)

- Name ↑
- Dashboard - Storage Cost
- Dashboard - Storage IO Detail
- Dashboard - Storage Overview
- Gauges Storage Performance
- Storage Admin - Which nodes are in high demand?
- Storage Admin - Which pools are in high demand?
- Storage IOPs

Dois grupos são mostrados por padrão:

- **Todos os painéis** lista todos os painéis que foram criados, independentemente do proprietário.
- **Meus painéis** lista somente os painéis criados pelo usuário atual.

O número de painéis contidos em cada grupo é mostrado ao lado do nome do grupo.

Para criar um novo grupo, clique no botão criar novo grupo de painel*. Digite um nome para o grupo e clique em **criar grupo**. Um grupo vazio é criado com esse nome.

Para adicionar painéis ao grupo, clique no grupo *todos os painéis* para mostrar todos os painéis no localatário, clique em *Meus painéis* se você quiser ver apenas os painéis que possui e siga um dos seguintes procedimentos:

- Para adicionar um único painel, clique no menu à direita do painel e selecione *Adicionar ao grupo*.
- Para adicionar vários painéis a um grupo, selecione-os clicando na caixa de seleção ao lado de cada painel, depois clique no botão **ações em massa** e selecione *Adicionar ao grupo*.

Remova os painéis do grupo atual da mesma maneira selecionando *Remover do grupo*. Não é possível remover painéis do grupo *todos os painéis* ou *Meus painéis*.






A remoção de um painel de um grupo não exclui o painel do Data Infrastructure Insights. Para remover completamente um painel, selecione o painel e clique em *Delete*. Isso remove-o de qualquer grupo a que pertencia e não está mais disponível para nenhum usuário.

Fixe seus painéis favoritos

Você pode gerenciar ainda mais seus painéis fixando os favoritos no topo da lista de painéis. Para fixar um painel, basta clicar no botão de atalho exibido quando você passar o Mouse sobre um painel em qualquer lista.

O pino/desbloqueio do tablier é uma preferência de utilizador individual e independente do grupo (ou grupos) ao qual o tablier pertence.

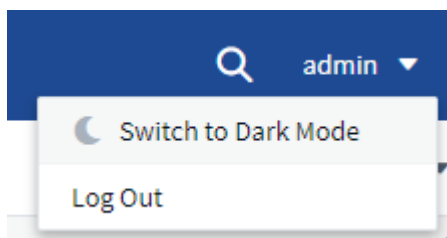
Dashboards (7)

<input type="checkbox"/>	Name ↑
	Dashboard - Storage Overview
	Storage Admin - Which nodes are in high demand?
	Storage IOPs
	Dashboard - Storage Cost
	Dashboard - Storage IO Detail
	Gauges Storage Performance
	Storage Admin - Which pools are in high demand?

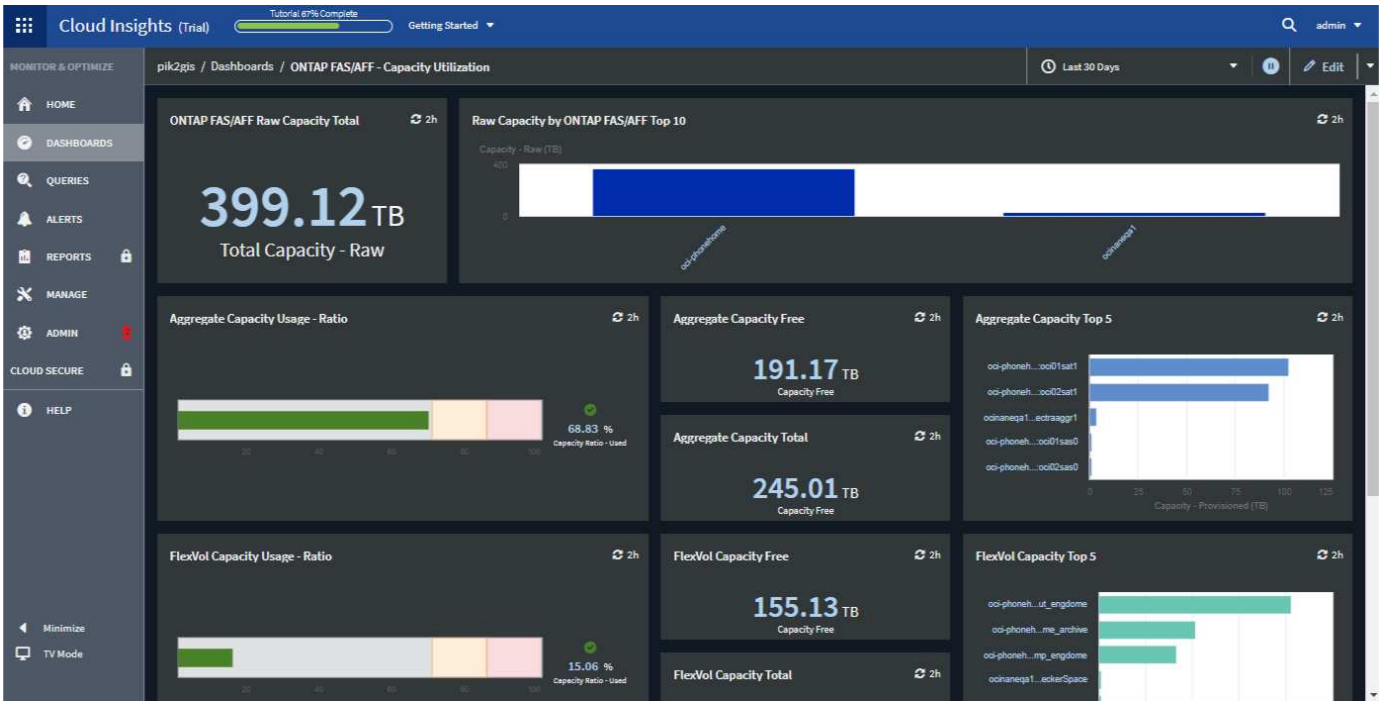
Tema escuro

Você pode optar por exibir Insights de infraestrutura de dados usando um tema claro (o padrão), que exibe a maioria das telas usando um fundo claro com texto escuro, ou um tema escuro que exibe a maioria das telas usando um fundo escuro com texto claro.

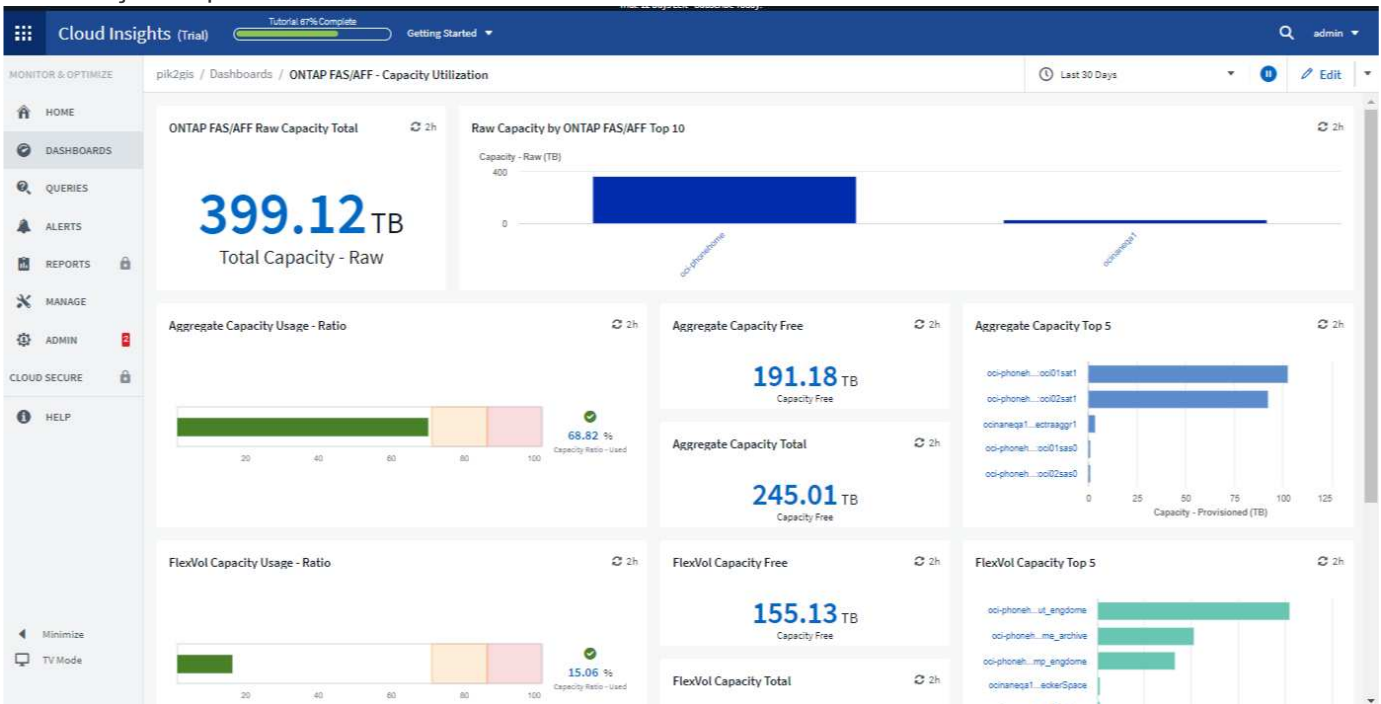
Para alternar entre temas claros e escuros, clique no botão de nome de usuário no canto superior direito da tela e escolha o tema desejado.



Vista do painel do tema escuro:



Visualização do painel de tema claro:



Algumas áreas de tela, como certos gráficos de widgets, ainda mostram fundos claros, mesmo quando vistos em tema escuro.

Interpolação do Gráfico de linhas

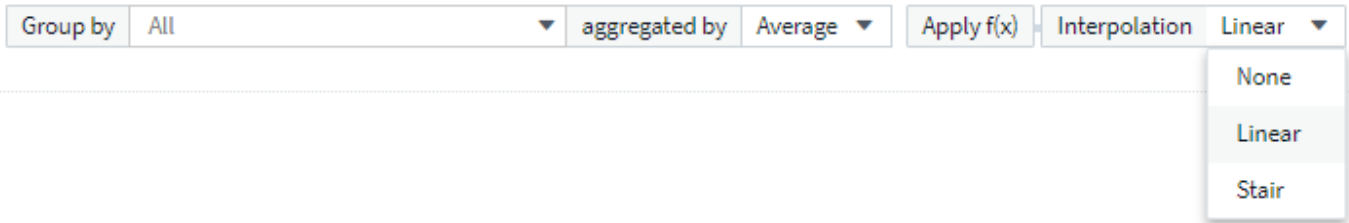
Diferentes coletores de dados frequentemente pesquisam seus dados em intervalos diferentes. Por exemplo, o coletor de dados A pode pesquisar a cada 15 minutos, enquanto o coletor de dados B faz pesquisas a cada cinco minutos. Quando um widget de gráfico de linha (também gráficos de spline, área e área empilhada) está agregando esses dados de vários coletores de dados em uma única linha (por exemplo, quando o widget está agrupando por "todos"), e atualizando a linha a cada cinco minutos, os dados do coletor B podem ser

mostrados com precisão enquanto os dados do Coletor A podem ter lacunas, afetando o agregado até que o Coletor Um polls novamente.

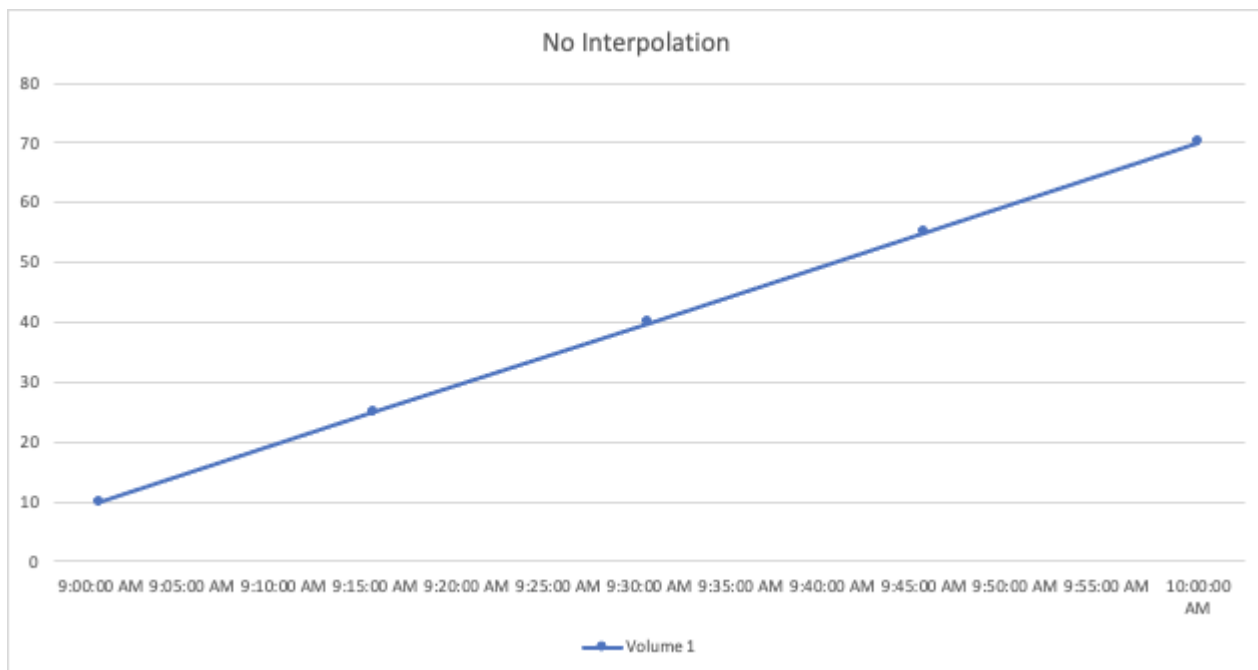
Para aliviar isso, o Data Infrastructure Insights interpola os dados ao agregar, usando os pontos de dados adjacentes para ter uma "melhor suposição" nos dados até que os coletores de dados pesquisem novamente. Você sempre pode visualizar os dados de objeto de cada coletor de dados individualmente ajustando o agrupamento do widget.

Métodos de interpolação

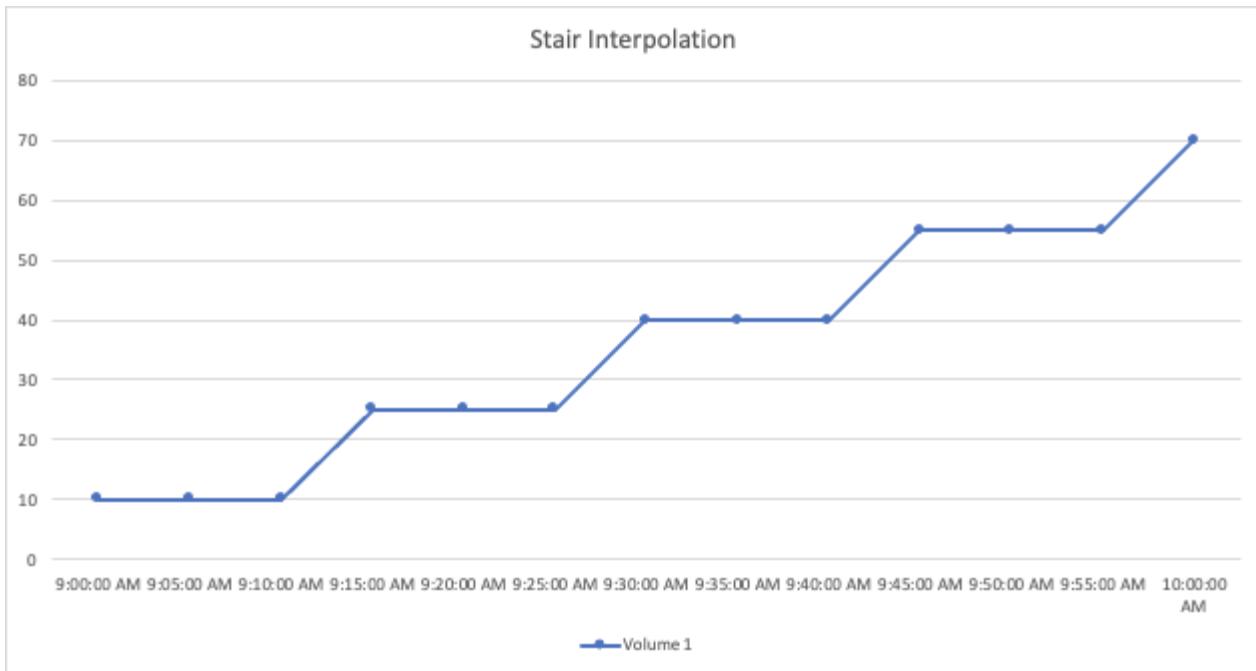
Ao criar ou modificar um gráfico de linhas (ou gráfico de spline, área ou área empilhada), você pode definir o método de interpolação para um de três tipos. Na seção "Agrupar por", escolha a interpolação desejada.



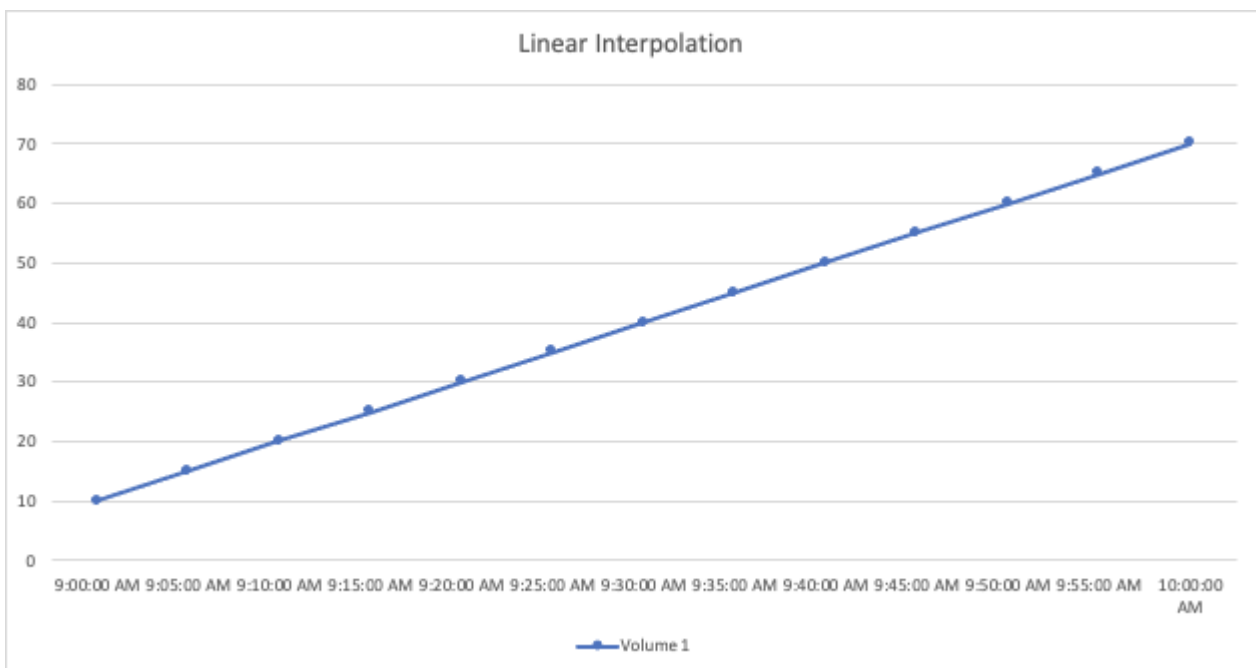
- **Nenhum:** Não faça nada, ou seja, não gere pontos entre eles.



- **Stair:** Um ponto é gerado a partir do valor do ponto anterior. Em uma linha reta, isso seria exibido como um layout típico de "escada".



- **Linear:** Um ponto é gerado como o valor entre a conexão dos dois pontos. Gera uma linha que se parece com a linha conetando os dois pontos, mas com pontos de dados adicionais (interpolados).



Painéis de amostra

Exemplo de dashboard: Desempenho da máquina virtual

Atualmente, existem muitos desafios que as operações DE TI enfrentam. Os administradores precisam fazer mais com menos, e é preciso ter visibilidade total dos data centers dinâmicos. Neste exemplo, mostraremos como criar um painel com widgets que fornecem informações operacionais sobre o desempenho da máquina virtual (VM) em seu locatário. Ao seguir este exemplo e criar widgets para atender às suas próprias

necessidades específicas, você pode fazer coisas como visualizar o desempenho do armazenamento de back-end em comparação com o desempenho da máquina virtual frontend ou visualizar a latência da VM versus a demanda de e/S.

Sobre esta tarefa

Aqui vamos criar um painel de desempenho de máquina virtual contendo o seguinte:

- Uma tabela que lista nomes de VMs e dados de performance
- Um gráfico comparando a latência da VM com a latência do storage
- Um gráfico mostrando leitura, gravação e IOPS total para VMs
- Um gráfico mostrando a taxa máxima de transferência para suas VMs

Este é apenas um exemplo básico. Você pode personalizar seu painel para destacar e comparar os dados de desempenho que escolher, a fim de se direcionar para suas próprias práticas recomendadas operacionais.

Passos

1. Faça login no Insight como um usuário com permissões administrativas.
2. No menu **Dashboards**, selecione **[-New dashboard]**.

Abre-se a página **novo painel**.

3. Na parte superior da página, insira um nome exclusivo para o painel, por exemplo, "desempenho da VM por aplicativo".
4. Clique em **Salvar** para salvar o painel com o novo nome.
5. Vamos começar a adicionar nossos widgets. Se necessário, clique no ícone **Editar** para ativar o modo Editar.
6. Clique no ícone **Adicionar widget** e selecione **Tabela** para adicionar um novo widget de tabela ao painel.

A caixa de diálogo Editar widget é aberta. Os dados padrão exibidos são para todos os armazenamentos em seu locatário.


Hypervisor Name ↑	Virtual Machine	Capacity - Total (GB)	IOPS - Total (IO/s)	Latency - Total (ms)
10.197.143.53 (9)	--	1,690.58	1.80	12.04
10.197.143.54 (7)	--	1,707.60	4.62	12.69
10.197.143.57 (11)	--	1,509.94	1.14	1.15
10.197.143.58 (10)	--	1,818.34	5.83	2.57
AzureComputeDefaultAvailabilitySet (363)	-- N/A	N/A	N/A	N/A
anandh9162020113920-rg-avset.anandh91620201	--	N/A	N/A	N/A
anandh916202013287-rg-avset.anandh91620201	--	N/A	N/A	N/A
anandh91720201288-rg-avset.anandh91720201	--	N/A	N/A	N/A
anjaliIngrun48-rg-avset.anjalivIngrun48-rg.398	--	N/A	N/A	N/A
anjaliIngrun50-rg-avset.anjalivIngrun50-rg.398	--	N/A	N/A	N/A
batutiscanaryHA97a-rg-avset.batutiscanaryha97	--	N/A	N/A	N/A
batutiscanaryHA97b-rg-avset.batutiscanaryha97	--	N/A	N/A	N/A

- Podemos personalizar este widget. No campo Nome na parte superior, exclua "Widget 1" e digite "Tabela de desempenho da Máquina Virtual".
- Clique no menu suspenso tipo de ativo e altere *Storage* para *Virtual Machine*.


Os dados da tabela são alterados para mostrar todas as máquinas virtuais no localatário.

- Vamos adicionar algumas colunas à tabela. Clique no ícone de engrenagem à direita e selecione *Hypervisor name*, *IOPS - total* e *latência - total*. Você também pode tentar digitar o nome na pesquisa para exibir rapidamente o campo desejado.

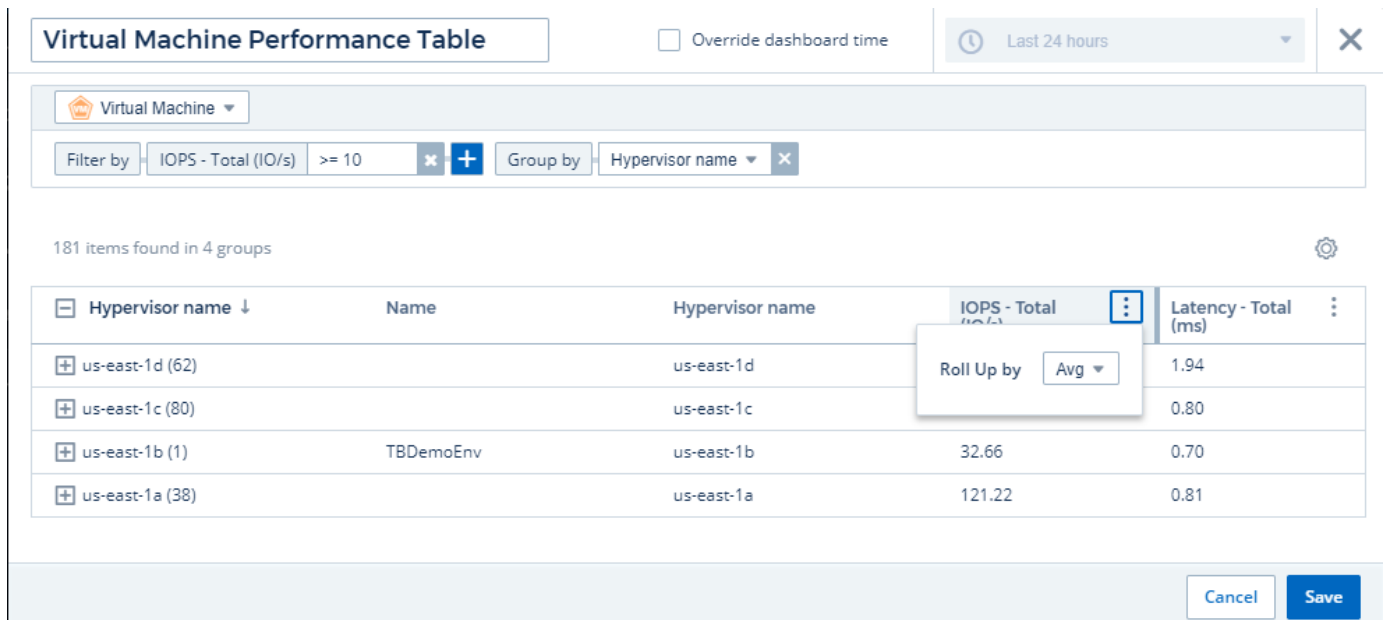
Estas colunas são agora apresentadas na tabela. Você pode classificar a tabela por qualquer uma dessas colunas. Observe que as colunas são exibidas na ordem em que foram adicionadas ao widget.

- Para este exercício, excluiríamos VMs que não estão ativamente em uso, então vamos filtrar qualquer coisa com menos de 10 IOPS totais. Clique no botão  ao lado de **Filtrar por** e selecione *IOPS - Total*. Clique em **any** e digite "10" no campo **de**. Deixe o campo **to** vazio. Clique em sair do campo de filtro ou pressione Enter para definir o filtro.

A tabela agora mostra apenas VMs com 10 ou mais IOPS total.

- Podemos recolher ainda mais a tabela agrupando os resultados. Clique no botão  ao lado de **Group by** e selecione um campo para agrupar, como *Application* ou *Hypervisor name*. O agrupamento é aplicado automaticamente.

As linhas da tabela são agora agrupadas de acordo com sua configuração. Você pode expandir e recolher os grupos conforme necessário. As linhas agrupadas mostram dados agrupados para cada uma das colunas. Algumas colunas permitem que você escolha o método de rolagem para essa coluna.



The screenshot shows the 'Virtual Machine Performance Table' widget interface. At the top, there's a title 'Virtual Machine Performance Table' and a search bar. Below that, there are filters: 'Filter by' set to 'IOPS - Total (IO/s) >= 10' and 'Group by' set to 'Hypervisor name'. The table displays 181 items grouped by Hypervisor name. The columns shown are Name, Hypervisor name, IOPS - Total (IO/s), and Latency - Total (ms). A dropdown menu is open over the 'IOPS - Total' column, showing 'Roll Up by' with 'Avg' selected. At the bottom right, there are 'Cancel' and 'Save' buttons.

Hypervisor name ↓	Name	Hypervisor name	IOPS - Total (IO/s)	Latency - Total (ms)
us-east-1d (62)		us-east-1d		1.94
us-east-1c (80)		us-east-1c		0.80
us-east-1b (1)	TBDemoEnv	us-east-1b	32.66	0.70
us-east-1a (38)		us-east-1a	121.22	0.81

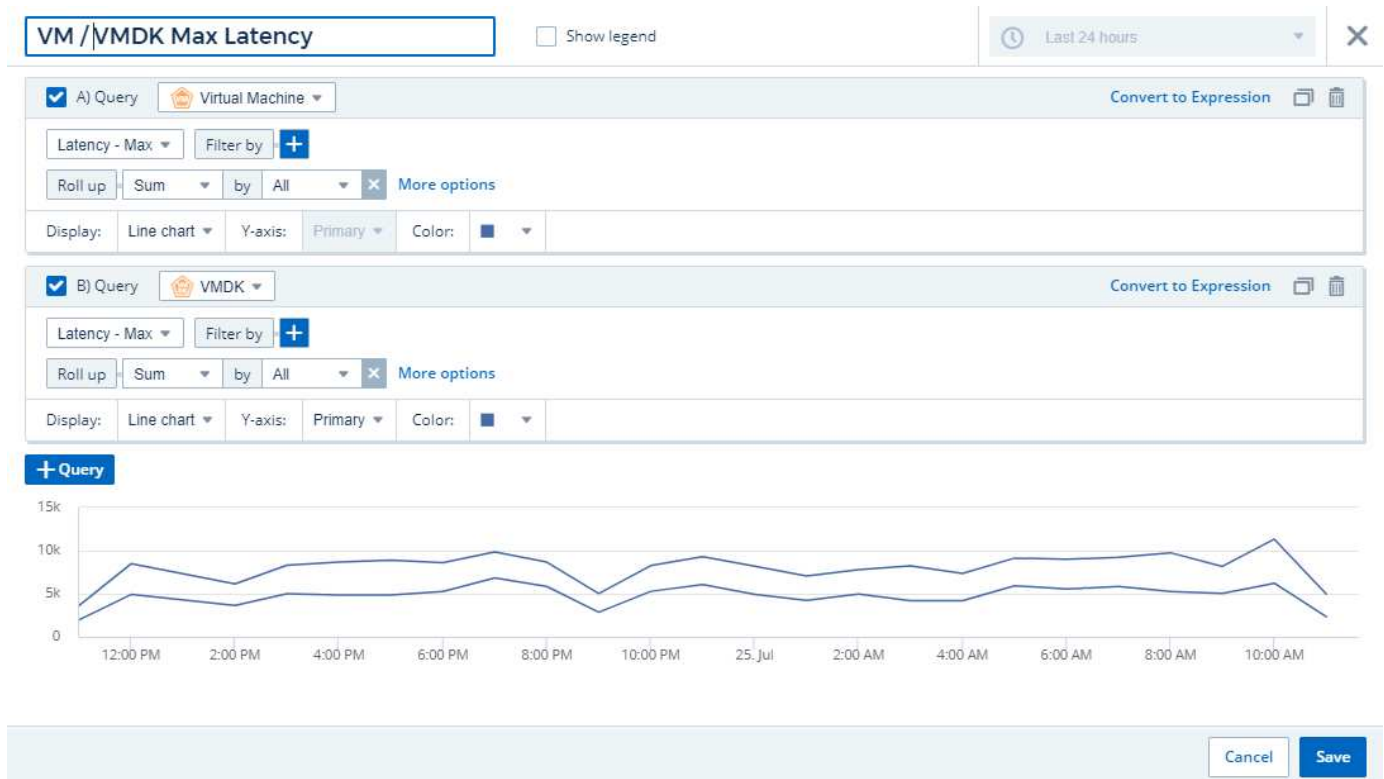
- Quando tiver personalizado o widget da tabela para sua satisfação, clique no botão **[Save]**.

O widget da tabela é salvo no painel.

Você pode redimensionar o widget no painel arrastando o canto inferior direito. Torne o widget mais amplo para mostrar todas as colunas claramente. Clique em **Salvar** para salvar o painel atual.

Em seguida, vamos adicionar alguns gráficos para mostrar nosso desempenho de VM. Vamos criar um gráfico de linha comparando a latência da VM com a latência do VMDK.

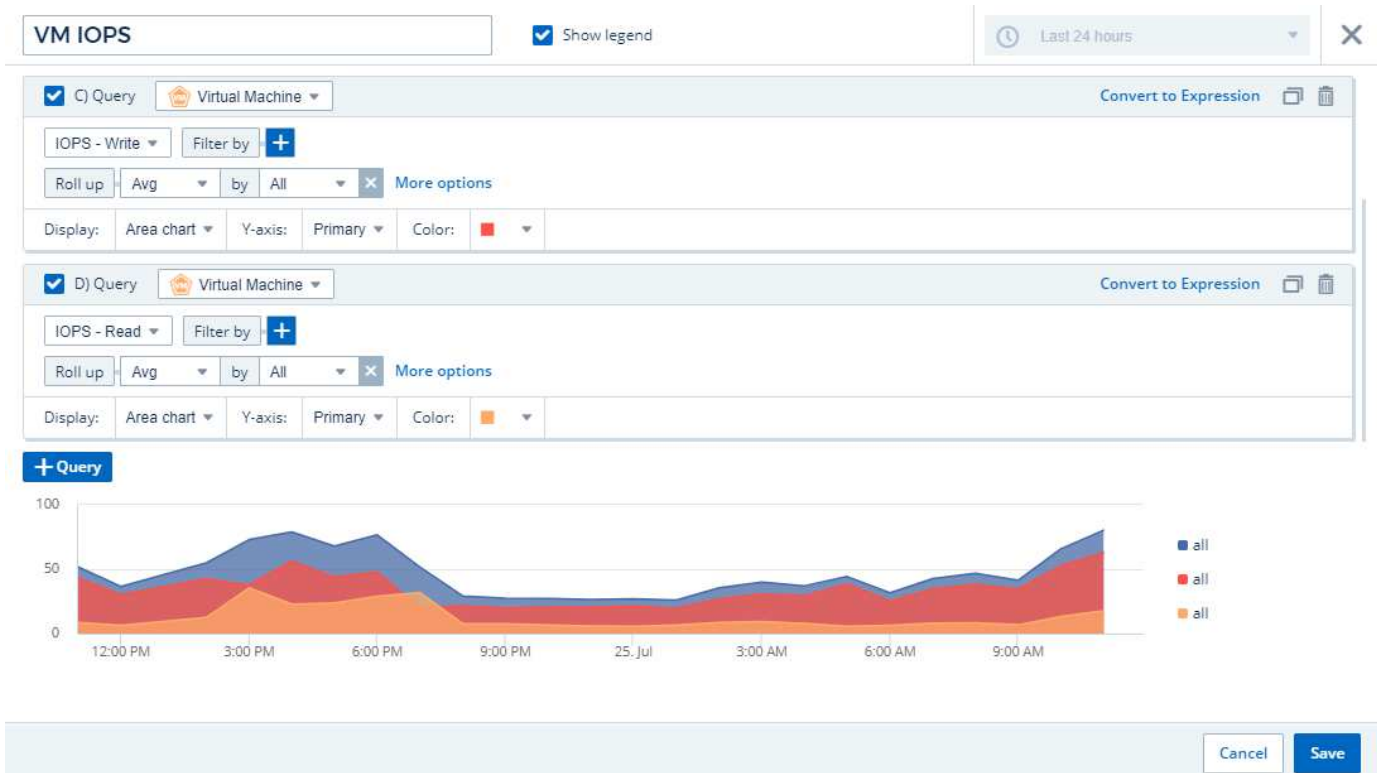
1. Se necessário, clique no ícone **Editar** no painel para ativar o modo Editar.
2. Clique no ícone **[Add widget]** e selecione *Line Chart* para adicionar um novo widget de gráfico de linha ao painel.
3. A caixa de diálogo **Edit Widget** é aberta. Nomeie este widget "VM / VMDK Max latência"
4. Selecione **Virtual Machine** e escolha *latency - Max*. Defina os filtros que desejar ou deixe **Filtrar por** vazio. Para **Roll up**, escolha *sum* por *all*. Exiba esses dados como um *Gráfico de linha* e deixe *eixo Y* como *primário*.
5. Clique no botão **[-Query]** para adicionar uma segunda linha de dados. Para esta linha, selecione *VMDK e latência - Max*. Defina os filtros que desejar ou deixe **Filtrar por** vazio. Para **Roll up**, escolha *sum* por *all*. Exiba esses dados como um *Gráfico de linha* e deixe *eixo Y* como *primário*.
6. Clique em **[Save]** para adicionar este widget ao painel.



Em seguida, vamos adicionar um gráfico mostrando VM Read, Write e Total IOPS em um único gráfico.

1. Clique no ícone **[Add widget]** e selecione *Area Chart* para adicionar um novo widget de gráfico de área ao painel.
2. A caixa de diálogo Editar widget é aberta. Nomeie este widget "VM IOPS"
3. Selecione **Virtual Machine** e escolha *IOPS - Total*. Defina os filtros que desejar ou deixe **Filtrar por** vazio. Para **Roll up**, escolha *sum* por *all*. Exiba esses dados como um *Gráfico de Área* e deixe o *eixo Y* como *primário*.
4. Clique no botão **[-Query]** para adicionar uma segunda linha de dados. Para esta linha, selecione **Virtual Machine** e escolha *IOPS - Read*.
5. Clique no botão **[-Query]** para adicionar uma terceira linha de dados. Para esta linha, selecione **Virtual Machine** e escolha *IOPS - Write*.

6. Clique em **Mostrar legenda** para exibir uma legenda desse widget no painel.



1. Clique em **[Save]** para adicionar este widget ao painel.

Em seguida, vamos adicionar um gráfico mostrando a taxa de transferência de VM para cada aplicativo associado à VM. Vamos usar o recurso Roll Up para isso.

1. Clique no ícone **[Add widget]** e selecione *Line Chart* para adicionar um novo widget de gráfico de linha ao painel.
2. A caixa de diálogo Editar widget é aberta. Nomeie este widget "taxa de transferência de VM por aplicativo"
3. Selecione Máquina Virtual e escolha throughput - Total. Defina os filtros que desejar ou deixe o filtro vazio. Para rolar, escolha "Max" e selecione por "Application" ou "Name". Mostre as 10 principais aplicações. Exiba esses dados como um Gráfico de linha e deixe o eixo Y como primário.
4. Clique em **[Save]** para adicionar este widget ao painel.

Você pode mover widgets no painel segurando o botão do Mouse em qualquer lugar na parte superior do widget e arrastando-o para um novo local.

Você pode redimensionar widgets arrastando o canto inferior direito.

Certifique-se de **[Save]** o painel depois de fazer as alterações.

Seu painel final de desempenho da VM será parecido com isso:



Melhores práticas para painéis e Widgets

Dicas e truques para ajudá-lo a aproveitar ao máximo os recursos poderosos de painéis e widgets.

Encontrar a métrica certa

O Data Infrastructure Insights adquire contadores e métricas usando nomes que às vezes diferem do coletor de dados para o coletor de dados.

Ao procurar a métrica ou o contador certo para o widget do seu painel, tenha em mente que a métrica que você deseja pode estar sob um nome diferente daquele que você está pensando. Embora as listas suspensas no Data Infrastructure Insights geralmente sejam alfabéticas, às vezes um termo pode não aparecer na lista onde você acha que deveria. Por exemplo, termos como "capacidade bruta" e "capacidade usada" não aparecem juntos na maioria das listas.

Prática recomendada: Use o recurso de pesquisa em campos como Filtrar por ou locais como o seletor de colunas para encontrar o que você está procurando. Por exemplo, a busca por "CAP" mostrará todas as métricas com "capacidade" em seus nomes, não importa onde elas ocorram na lista. Em seguida, você pode selecionar facilmente as métricas que deseja nessa lista mais curta.

Aqui estão algumas frases alternativas que você pode tentar ao procurar métricas:

Quando você quiser encontrar:	Tente também procurar:
CPU	Processador
Capacidade	Capacidade bruta utilizada capacidade provisionada capacidade de pools de storage capacidade inferior a outro tipo de ativo> capacidade escrita
Velocidade do disco	Menor velocidade do disco com menor desempenho do tipo de disco
Host	Hosts de hipervisor

Hipervisor	O host é hipervisor
Microcódigo	Firmware
Nome	Alias Nome do hypervisor Nome do armazenamento Nome do arquivo Nome simples Nome do recurso Nome do recurso Alias da estrutura
Ler / escrever	IOPS parcial de R/W de gravação pendente - latência de gravação da capacidade escrita - utilização da cache de leitura - leitura
Máquina virtual	VM é virtual

Esta não é uma lista abrangente. Estes são exemplos de termos de pesquisa possíveis apenas.

Encontrar os ativos certos

Os ativos que você pode referenciar em filtros de widget e pesquisas variam de tipo de ativo para tipo de ativo.

Em painéis e páginas de ativos, o tipo de ativo em torno do qual você está construindo seu widget determina os outros contadores de tipos de ativos para os quais você pode filtrar ou adicionar uma coluna. Tenha em mente o seguinte ao criar seu widget:

Este tipo de ativo / contador:	Podem ser filtrados para os seguintes ativos:
Máquina virtual	VMDK
Datastore(s)	Volume interno VMDK Virtual Machine volume
Hipervisor	A máquina virtual é o host do hypervisor
Host(s)	Máquina virtual de host de cluster de volume interno
Malha	Porta

Esta não é uma lista abrangente.

Prática recomendada: Se você estiver filtrando para um tipo de ativo específico que não aparece na lista, tente construir sua consulta em torno de um tipo de ativo alternativo.

Exemplo de plotagem de dispersão: Conhecendo seu eixo

Alterar a ordem dos contadores em um widget de plotagem de dispersão altera os eixos nos quais os dados são exibidos.

Sobre esta tarefa

Este exemplo criará um gráfico de dispersão que permitirá que você veja VMs de baixo desempenho que têm alta latência em comparação com IOPS baixo.

Passos

1. Crie ou abra um painel no modo de edição e adicione um widget **Scatter Plot Chart**.
2. Selecione um tipo de ativo, por exemplo, *Máquina Virtual*.
3. Selecione o primeiro contador que pretende traçar. Para este exemplo, selecione *latência - total*.

Latência - Total é mapeado ao longo do eixo X do gráfico.

4. Selecione o segundo contador que pretende traçar. Para este exemplo, selecione *IOPS - Total*.

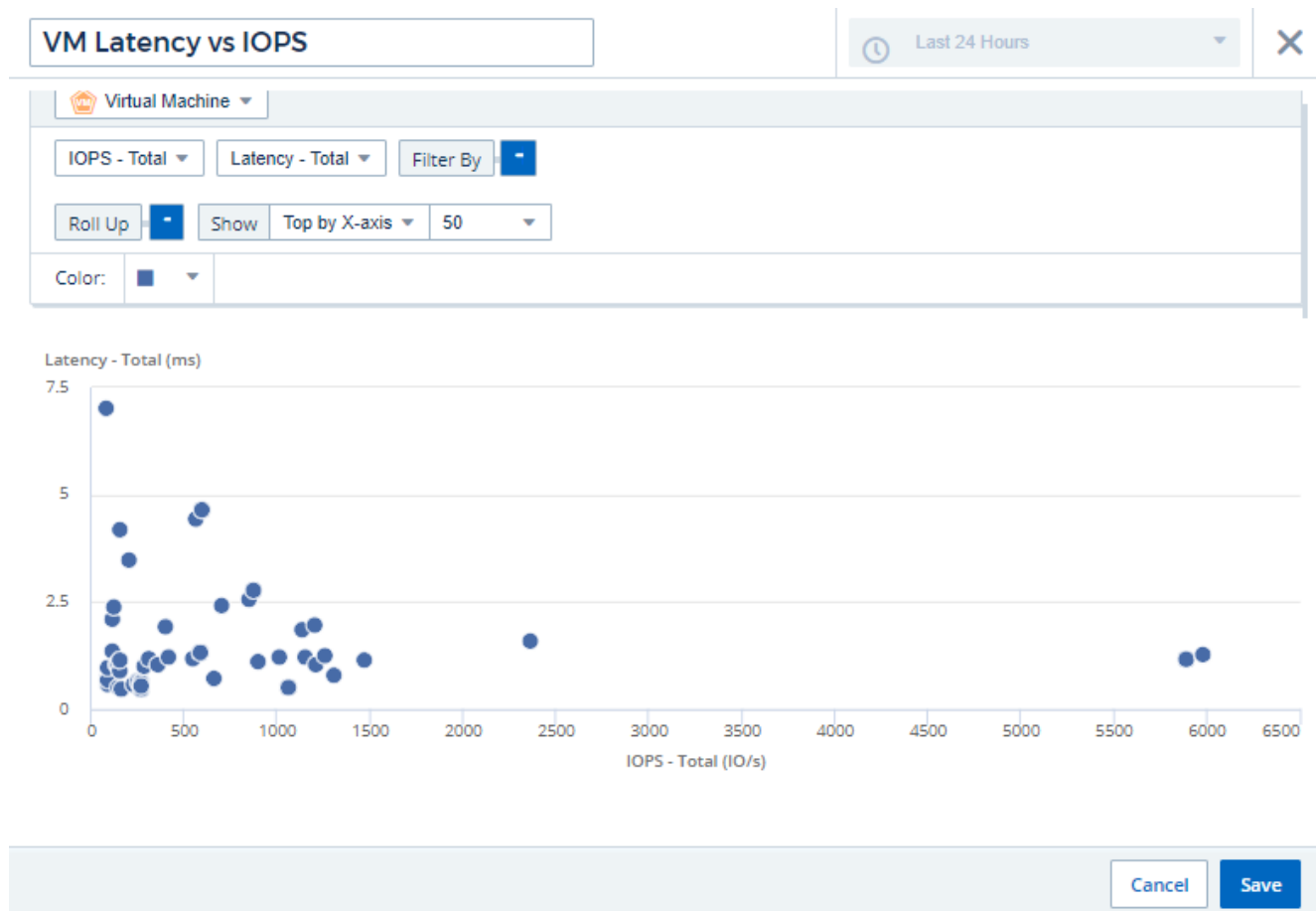
IOPS - Total é mapeado ao longo do eixo Y no gráfico. VMs com maior latência são exibidas no lado direito do gráfico. Apenas as 100 principais VMs de maior latência são exibidas, porque a configuração **Top by X-axis** é atual.



5. Agora inverta a ordem dos contadores definindo o primeiro contador para *IOPS - total* e o segundo para *latência - total*.

Latência- Total agora é mapeado ao longo do eixo Y no gráfico, e *IOPS - total* ao longo do eixo X. As VMs com IOPS mais alto agora são exibidas no lado direito do gráfico.

Observe que, como não alteramos a configuração **Top by X-Axis**, o widget agora exibe as 100 principais VMs de IOPS mais altas, já que é o que está atualmente traçado ao longo do eixo X.



Você pode optar pelo gráfico para exibir o N superior por eixo X, N superior por eixo Y, N inferior por eixo X ou N inferior por eixo Y. Em nosso exemplo final, o gráfico está exibindo as 100 principais VMs que têm o maior total de IOPS. Se mudarmos para **topo por eixo Y**, o gráfico exibirá novamente as 100 principais VMs que têm a maior latência total.

Observe que em um gráfico de plotagem de dispersão, você pode clicar em um ponto para detalhar a página de ativos desse recurso.

Trabalhando com consultas

Ativos usados em consultas

As consultas permitem que você monitore e solucione problemas de sua rede pesquisando os ativos e as métricas do locatário em um nível granular com base em critérios selecionados pelo usuário (por exemplo, anotações).

Observe que as regras de anotação, que atribuem automaticamente anotações a ativos, *require* uma consulta.

Você pode consultar os ativos de inventário físico ou virtual (e suas métricas associadas) no seu locatário ou as métricas fornecidas com integração, como Kubernetes ou dados avançados do ONTAP.

Ativos de inventário

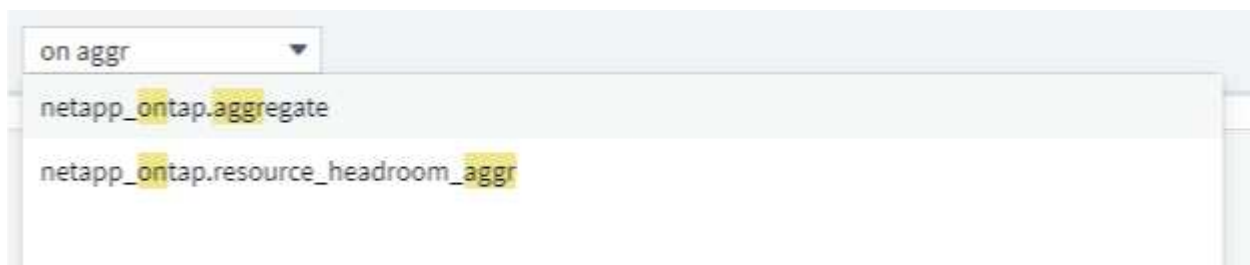
Os seguintes tipos de ativos podem ser usados em consultas, widgets de painel e Landing pages de ativos personalizados. Os campos e contadores disponíveis para filtros, expressões e exibição variam entre os tipos

de ativos. Nem todos os ativos podem ser usados em todos os tipos de widget.

- Aplicação
- Armazenamento de dados
- Disco
- Malha
- Dispositivo genérico
- Host
- Volume interno
- Sessão iSCSI
- Portal de rede iSCSI
- Caminho
- Porta
- Qtree
- Cota
- Partilhar
- Armazenamento
- Nó de storage
- Pool de storage
- Máquina de Storage Virtual (SVM)
- Interruptor
- Fita
- VMDK
- Máquina virtual
- Volume
- Zona
- Membro da zona

Métricas de integração

Além de consultar ativos de inventário e suas métricas de desempenho associadas, você também pode consultar métricas de **dados de integração**, como as geradas pelo Kubernetes ou Docker, ou fornecidas com métricas avançadas do ONTAP.



Criando consultas

As consultas permitem que você pesquise os ativos em seu locatário em um nível granular, permitindo filtrar os dados que você deseja e classificar os resultados de acordo com o seu gosto.

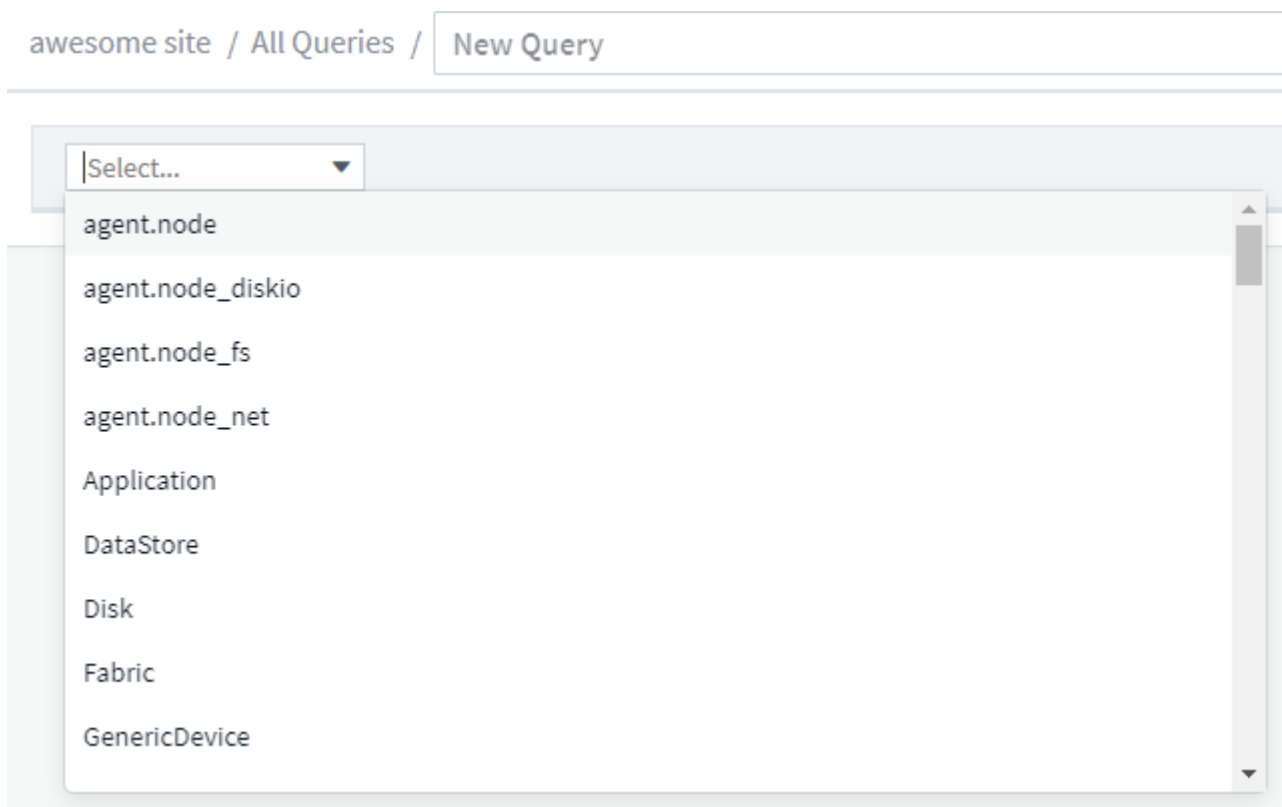
Por exemplo, você pode criar uma consulta para *volumes*, adicionar um filtro para localizar *storages* específicos associados aos volumes selecionados, adicionar outro filtro para encontrar uma *anotação* específica, como "Tier 1" nos armazenamentos selecionados e, finalmente, adicionar outro filtro para localizar todos os armazenamentos com *IOPS - leitura (IO/s)* maior que 25. Quando os resultados são exibidos, você pode classificar as colunas de informações associadas à consulta em ordem crescente ou decrescente.

Observação: Quando um novo coletor de dados é adicionado que adquire ativos, ou qualquer anotação ou atribuição de aplicativo é feita, você pode consultar esses novos ativos, anotações ou aplicativos somente depois que as consultas forem indexadas. A indexação ocorre em um intervalo programado regularmente ou durante determinados eventos, como regras de anotação em execução.

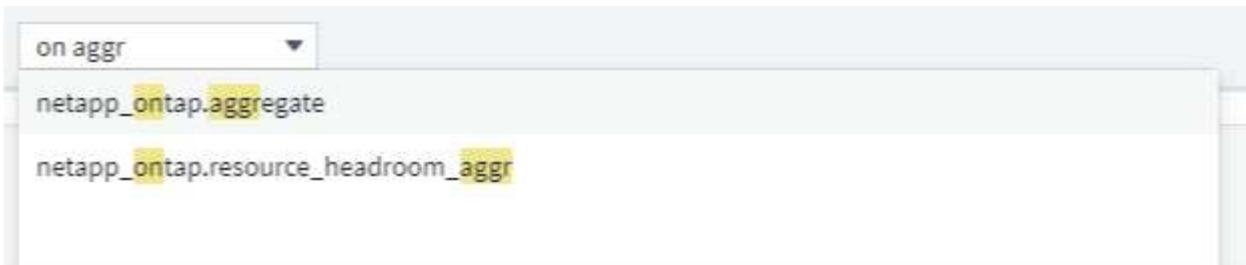
Criar uma consulta é muito simples:

1. Navegue até **consultas > * Nova consulta**.
2. Na lista 'Selecionar...', selecione o tipo de objeto que deseja consultar. Pode percorrer a lista ou começar a escrever para encontrar mais rapidamente o que está a procurar.

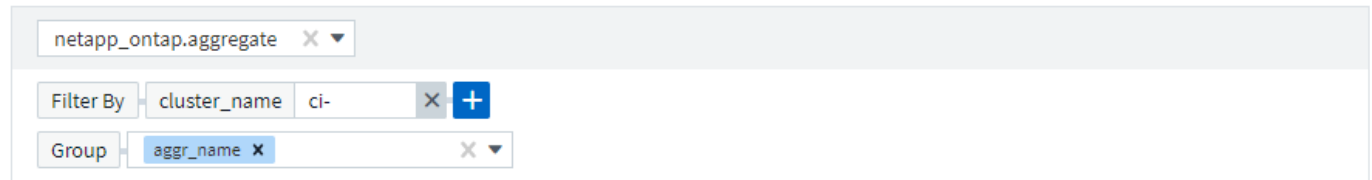
Lista de deslocamento:



Tipo de pesquisa:



Você pode adicionar filtros para restringir ainda mais sua consulta clicando no botão * no campo **Filtrar por**. Agrupar linhas por objeto ou atributo. Ao trabalhar com dados de integração (Kubernetes, métricas avançadas do ONTAP, etc.), você pode agrupar por vários atributos, se desejado.



5 items found

Table Row Grouping	Metrics & Attributes	
aggr_name	cp_read_blocks	cluster_name ↓
oci02sat0	0.59	oci-phonehome
oci02sat1	0.15	oci-phonehome
oci02sat2	212.64	oci-phonehome
oci01sat0	0.39	oci-phonehome
oci01sat1	48.89	oci-phonehome

A lista de resultados da consulta mostra um número de colunas padrão, dependendo do tipo de objeto pesquisado. Para adicionar, remover ou alterar as colunas, clique no ícone de engrenagem à direita da tabela. As colunas disponíveis variam com base no tipo ativo/métrico.




Escolhendo agregação, unidades, formatação condicional

Agregação e unidades

Para colunas "valor", você pode refinar ainda mais os resultados da consulta escolhendo como os valores exibidos são agregados, bem como selecionar as unidades em que esses valores são exibidos. Essas opções são encontradas selecionando o menu "três pontos" no canto superior de uma coluna.

143 items found

Table Row Grouping	Metrics & Attributes
agent.node_diskio ↑	io_time (ms) 
nvme0n1	20,604,960.00
nvme0n1	29,184,970.00
nvme0n1	4,642,684.00
nvme0n1	31,918,988.00
nvme0n1	29,258,256.00
nvme0n1	18,022,164.00
nvme0n1	28,483,300.00
nvme0n1	69,835,016.00
nvme0n1	15,952,780.00
nvme0n1	44,169,696.00
nvme0n1	12,138,928.00
nvme0n1	5,234,528.00
nvme0n1	34,260,552.00

▼ Aggregation

Group By

Time Aggregate By


▼ Unit Display


Base Unit

Displayed In

▼ Conditional Formatting Reset

If value is

 Warning ms

 Critical ms

> Rename Column

Unidades

Pode selecionar as unidades em que pretende visualizar os valores. Por exemplo, se a coluna selecionada mostrar capacidade bruta e os valores forem mostrados no GiB, mas você preferir exibi-los como TiB, basta selecionar TiB na lista suspensa Exibição da unidade.

Agregação

Pelo mesmo token, se os valores mostrados forem agregados a partir dos dados subjacentes como "média", mas você preferir mostrar a soma de todos os valores, selecione "soma" na lista suspensa *Group by* (se você quiser que quaisquer valores agrupados mostrem as somas) ou na lista suspensa *time Aggregate by* (se quiser que os valores de linha mostrem somas de dados subjacentes).

Você pode optar por agregar pontos de dados agrupados por *média*, *Máx*, *Mín* ou *soma*.

Você pode agregar dados de linha individuais por *média*, *último ponto de dados adquirido*, *máximo*, *mínimo* ou *soma*.

Formatação condicional

A formatação condicional permite destacar os limites de nível de aviso e nível crítico na lista de resultados da

consulta, trazendo visibilidade instantânea para outliers e pontos de dados excepcionais.

143 items found

Table Row Grouping	Metrics & Attributes
agent.node_diskio ↑	io_time (sec)
nvme0n1	20,604.96
nvme0n1	29,184.97
nvme0n1	4,642.68
nvme0n1	31,918.99
nvme0n1	29,258.26
nvme0n1	18,022.16
nvme0n1	28,483.30
nvme0n1	69,835.02
nvme0n1	15,952.78

⋮

- > Aggregation
- > Unit Display
- ∨ Conditional Formatting Reset
 - If value is: > (Greater than)
 - Warning: 10000 sec
 - Critical: 20000 sec
- > Rename Column

A formatação condicional é definida separadamente para cada coluna. Por exemplo, você pode escolher um conjunto de limites para uma coluna de capacidade e outro conjunto para uma coluna de taxa de transferência.

Mudar o nome da coluna

Renomear uma coluna altera o nome exibido na lista resultados da consulta. O novo nome da coluna também é mostrado no arquivo resultante se você exportar a lista de consulta para .CSV.

Guardar

Depois de configurar sua consulta para mostrar os resultados desejados, você pode clicar no botão **Salvar** para salvar a consulta para uso futuro. Dê-lhe um nome significativo e único.

Mais sobre filtragem

Curingas e expressões

Quando você está filtrando valores de texto ou lista em consultas ou widgets de painel, à medida que você começa a digitar, você recebe a opção de criar um filtro * curinga* com base no texto atual. Selecionar esta opção irá retornar todos os resultados que correspondem à expressão curinga. Você também pode criar **expressões** usando NOT OU OU, ou pode selecionar a opção "nenhum" para filtrar valores nulos no campo.

kubernetes.pod x ▾

Filter By pod_name ingest x + ?

Group pod_name x

- Create wildcard containing "ingest"
- ci-service-datalake-ingestion-85b5bdfd6d-2qbwr
- service-foundation-ingest-767dfd5bfc-vxd5p
- None

71 items found

Table Row Grouping

Os filtros baseados em caracteres universais ou expressões (por exemplo, NÃO, OU, "nenhum", etc.) são exibidos em azul escuro no campo de filtro. Os itens que você selecionar diretamente da lista são exibidos em azul claro.

kubernetes.pod x ▾

Filter By pod_name *ingest* x ci-service-audit-5f775dd975-brfdc x x ▾ x + ?

Group pod_name x ▾

3 items found

3 items found

Table Row Grouping

pod_name
ci-service-audit-5f775dd975-brfdc
ci-service-datalake-ingestion-85b5bdfd6d-2qbwr
service-foundation-ingest-767dfd5bfc-vxd5p

Observe que a filtragem de caracteres curinga e expressão funciona com texto ou listas, mas não com valores numéricos, datas ou booleanos.

Refinando filtros

Você pode usar o seguinte para refinar seu filtro:

Filtro	O que faz	Exemplo	Resultado
--------	-----------	---------	-----------

* (Asterisco)	permite-lhe procurar tudo	vol*rhel	retorna todos os recursos que começam com "vol" e terminam com "rhel"
? (ponto de interrogação)	permite-lhe procurar um número específico de caracteres	BOS-PRD??-S12	Retorna BOS-PRD 12_-S12, BOS-PRD23_-S12 , e assim por diante
OU	permite especificar várias entidades	FAS2240 OU CX600 OU FAS3270	Retorna qualquer um de FAS2440, CX600 ou FAS3270
NÃO	permite excluir texto dos resultados da pesquisa	NÃO EMC*	Retorna tudo o que não começa com "EMC"
<i>Nenhum</i>	Procura valores NULL em todos os campos	<i>Nenhum</i>	retorna resultados onde o campo de destino está vazio
Não *	Procura valores NULL em campos <i>text-only</i>	Não *	retorna resultados onde o campo de destino está vazio

Se você incluir uma string de filtro em aspas duplas, o Insight trata tudo entre a primeira e a última citação como uma correspondência exata. Quaisquer caracteres especiais ou operadores dentro das aspas serão tratados como literais. Por exemplo, a filtragem para "*" retornará resultados que são um asterisco literal; o asterisco não será tratado como um curinga neste caso. Os operadores OU E NÃO também serão tratados como strings literais quando incluídos em aspas duplas.

O que faço agora que tenho resultados de consultas?

A consulta fornece um local simples para adicionar anotações ou atribuir aplicativos a ativos. Note que só pode atribuir aplicações ou anotações aos seus ativos de inventário (disco, armazenamento, etc.). As métricas de integração não podem assumir atribuições de anotações ou aplicativos.

Para atribuir uma anotação ou aplicação aos ativos resultantes da sua consulta, selecione simply o(s) ativo(s) utilizando a coluna da caixa de verificação à esquerda da tabela de resultados e, em seguida, clique no botão **ações em massa** à direita. Escolha a ação desejada para aplicar aos ativos selecionados.

The screenshot shows a search interface with a filter for 'Volume' and a table of query results. The table has columns for Name, Storage Pools, Capacity - Raw (GB), and Mapped Ports. A bulk actions menu is open over the table, showing options: Add Annotation, Remove Annotation, Add Application, and Remove Application. The table contains 5 rows, with 2 selected (checked).

Name ↑	Storage Pools	Capacity - Raw (GB)	Mapped Ports
<input type="checkbox"/> DmoESX_optimus:mc_Dm...	optimus-02:aggr1_optimu...	N/A	
<input checked="" type="checkbox"/> DmoSAN_optimus:hoffma...	optimus-02:aggr1_optimu...	N/A	
<input checked="" type="checkbox"/> DmoSAN_optimus:mc_D...	optimus-02:aggr1_optimu...	N/A	US:windows_zu08
<input type="checkbox"/> oci-3070-01:/vol/vfiler_lun...	oci-3070-01:aggr5	N/A	OS:windows
<input type="checkbox"/> spectravs1:sjimmyscsi:/v...	ocinaneqa1-01:spectraaggr1	N/A	OS:linux

As regras de anotação requerem consulta

Se você estiver configurando "Regras de anotação", cada regra deve ter uma consulta subjacente para trabalhar. Mas, como você viu acima, as consultas podem ser feitas tão amplas ou estreitas quanto você precisa.

Visualizar consultas

Você pode visualizar suas consultas para monitorar seus ativos e alterar a forma como suas consultas exibem os dados relacionados aos seus ativos.

Passos

1. Faça login no seu locatário do Data Infrastructure Insights.
2. Clique em **consultas** e selecione **Mostrar todas as consultas**. Você pode alterar a forma como as consultas são exibidas fazendo qualquer um dos seguintes procedimentos:
3. Você pode inserir texto na caixa de filtro para pesquisar para exibir consultas específicas.
4. Você pode alterar a ordem de classificação das colunas na tabela de consultas para ascendente (seta para cima) ou descendente (seta para baixo) clicando na seta no cabeçalho da coluna.
5. Para redimensionar uma coluna, passe o Mouse sobre o cabeçalho da coluna até que uma barra azul apareça. Coloque o Mouse sobre a barra e arraste-a para a direita ou para a esquerda.
6. Para mover uma coluna, clique no cabeçalho da coluna e arraste-a para a direita ou para a esquerda.


Ao percorrer os resultados da consulta, esteja ciente de que os resultados podem mudar à medida que o Data Infrastructure Insights faz o polling automático de seus coletores de dados. Isso pode resultar em alguns itens em falta ou alguns itens que aparecem fora de ordem, dependendo de como eles são classificados.

Exportar resultados da consulta para um arquivo .CSV

Você pode exportar os resultados de qualquer consulta para um arquivo .CSV, que permitirá analisar os dados ou importá-los para outro aplicativo.

Passos

1. Faça login no Data Infrastructure Insights.
2. Clique em **consultas** e selecione **Mostrar todas as consultas**.

A página consultas é exibida.
3. Clique em uma consulta.
4. Clique  para exportar os resultados da consulta para um arquivo .CSV.



Exportar para .CSV também está disponível no menu "três pontos" nos widgets da tabela do painel, bem como na maioria das tabelas da página de destino.

Os dados exportados refletirão os nomes atuais de filtragem, colunas e colunas exibidos.

Observação: Quando uma vírgula aparece em um nome de ativo, a exportação encerra o nome em aspas, preservando o nome do ativo e o formato .csv adequado.

Ao abrir um arquivo .CSV exportado com o Excel, se você tiver um nome de objeto ou outro campo que esteja

no formato NN:NN (dois dígitos seguidos por dois pontos seguidos por mais dois dígitos), o Excel às vezes interpretará esse nome como um formato de hora, em vez de formato de texto. Isso pode resultar na exibição de valores incorretos no Excel nessas colunas. Por exemplo, um objeto chamado "81:45" seria exibido no Excel como "81:45:00".

Para contornar isso, importe o .CSV para o Excel usando as seguintes etapas:

1. Abra uma nova folha no Excel.
2. Na guia "dados", escolha "de texto".
3. Localize o arquivo .CSV desejado e clique em "Importar".
4. No assistente Importar, escolha "delimitado" e clique em Avançar.
5. Escolha "vírgula" para o delimitador e clique em Avançar.
6. Selecione as colunas desejadas e escolha "texto" para o formato de dados da coluna.
7. Clique em concluir.

Seus objetos devem ser exibidos no Excel no formato adequado.

Modificar ou excluir uma consulta

Você pode alterar os critérios associados a uma consulta quando quiser alterar os critérios de pesquisa dos ativos que você está consultando.

Modificando uma consulta

Passos

1. Clique em **explorar** e selecione **todas as consultas métricas**.

A página consultas é exibida.

2. Clique no nome da consulta
3. Para adicionar um critério à consulta, clique no ícone colunas e selecione uma métrica ou atributo na lista.

Quando tiver efetuado todas as alterações necessárias, proceda de uma das seguintes formas:

- Clique no botão **Salvar** para salvar a consulta com o nome que foi usado inicialmente.
- Clique na lista suspensa ao lado do botão **Salvar** e selecione **Salvar como** para salvar a consulta com outro nome. Isso não substitui a consulta original.
- Clique na lista suspensa ao lado do botão **Salvar** e selecione **Renomear** para alterar o nome da consulta que você usou inicialmente. Isso substitui a consulta original.
- Clique na lista suspensa ao lado do botão **Salvar** e selecione **descartar alterações** para reverter a consulta para as últimas alterações salvas.

Excluindo uma consulta

Para excluir uma consulta, clique em **consultas** e selecione **Mostrar todas as consultas** e siga um destes procedimentos:

1. Clique no menu "três pontos" à direita da consulta e clique em **Excluir**.

2. Clique no nome da consulta e selecione **Excluir** no menu suspenso **Salvar**.

Copiando valores de tabela

Você pode copiar valores em tabelas para a área de transferência para uso em caixas de pesquisa ou outros aplicativos.

Sobre esta tarefa

Existem dois métodos que você pode usar para copiar valores de tabelas ou resultados de consulta para a área de transferência.

Passos

1. Método 1: Realce o texto desejado com o Mouse, copie-o e cole-o em campos de pesquisa ou outros aplicativos.
2. Método 2: Para campos de valor único, passe o Mouse sobre o campo e clique no ícone da área de transferência que aparece. O valor é copiado para a área de transferência para uso em campos de pesquisa ou outros aplicativos.

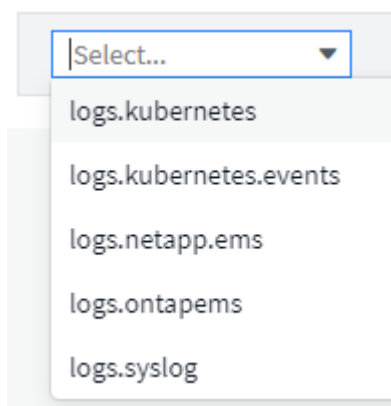
Observe que somente valores que são links para ativos podem ser copiados usando esse método. Apenas os campos que incluem valores únicos (ou seja, não listas) têm o ícone de cópia.

Explorador de registros

O Data Infrastructure Insights Log Explorer é uma ferramenta poderosa para consultar logs do sistema. Além de ajudar com investigações, você também pode salvar uma consulta de log em um Monitor para fornecer alertas quando esses gatilhos de log específicos são ativados.

Para começar a explorar os logs, clique em **consultas de log > Nova consulta de log**.

Selecione um registro disponível na lista.



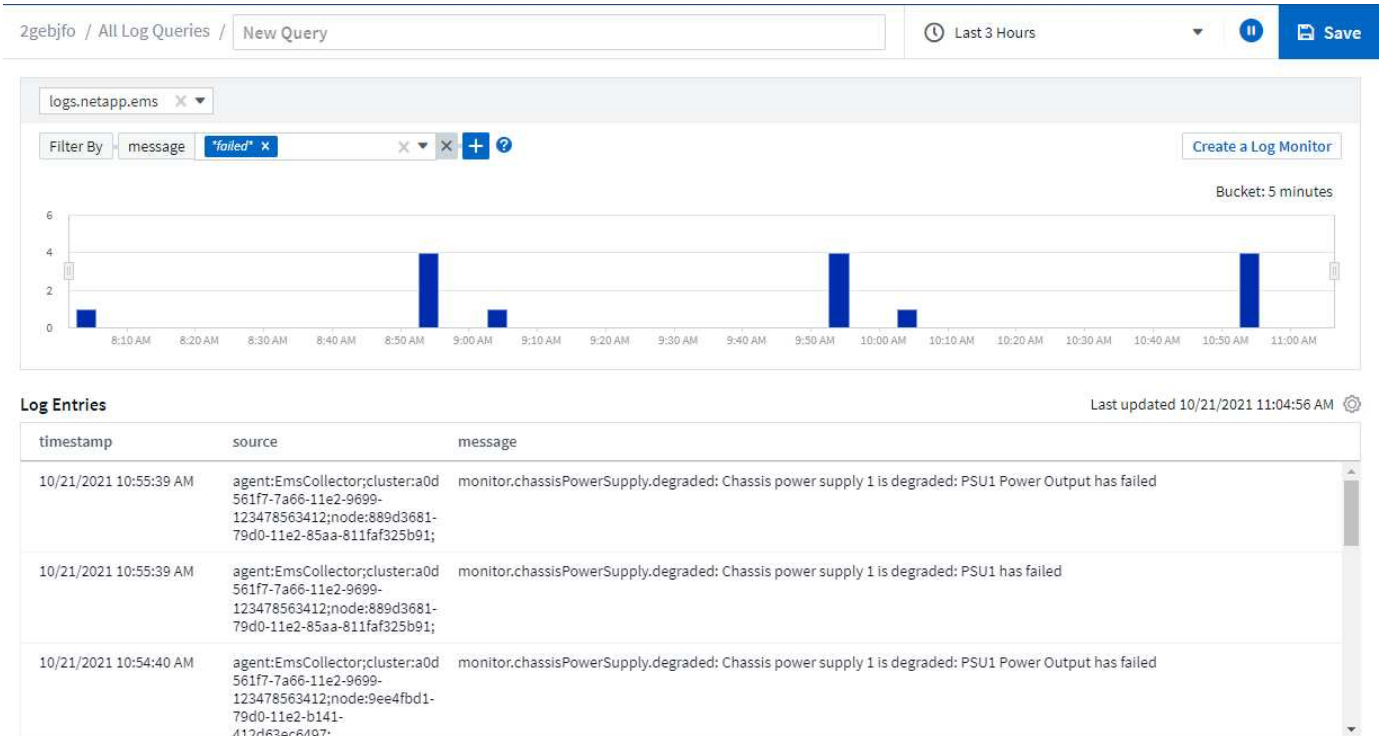
Os tipos de logs disponíveis para consulta podem variar de acordo com o seu ambiente. Tipos de log adicionais podem ser adicionados ao longo do tempo.

Você pode definir filtros para refinar ainda mais os resultados da consulta. Por exemplo, para localizar todas as mensagens de log mostrando uma falha, defina um filtro para *messages* contendo a palavra "failed".



Você pode começar a digitar o texto desejado no campo de filtro; o Data Infrastructure Insights solicitará que você crie uma pesquisa curinga contendo a cadeia de caracteres à medida que você digita.

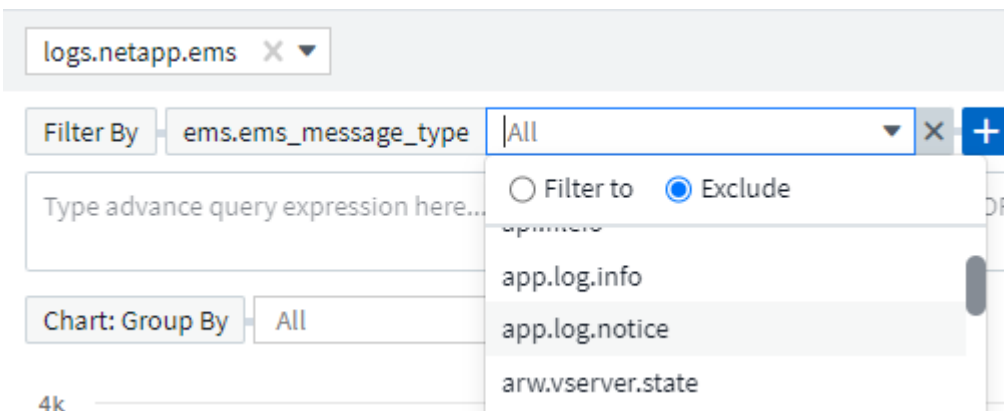
Os resultados são exibidos em um gráfico mostrando o número de instâncias de log em cada período de tempo mostrado. Abaixo do gráfico estão as entradas de log. O gráfico e as entradas são atualizados automaticamente com base no intervalo de tempo selecionado.



Filtragem

Incluir / excluir

Ao filtrar os logs, você pode optar por **incluir** (ou seja, "Filtrar para") ou **excluir** as strings que você digita. Strings excluídas são exibidas no filtro concluído como "Not <string>".



Os filtros baseados em caracteres universais ou expressões (por exemplo, NÃO, OU, "nenhum", etc.) são exibidos em azul escuro no campo de filtro. Os itens que você selecionar diretamente da lista são exibidos em azul claro.



Em qualquer ponto, você pode clicar em *Create a Log Monitor* para criar um novo monitor com base no filtro atual.

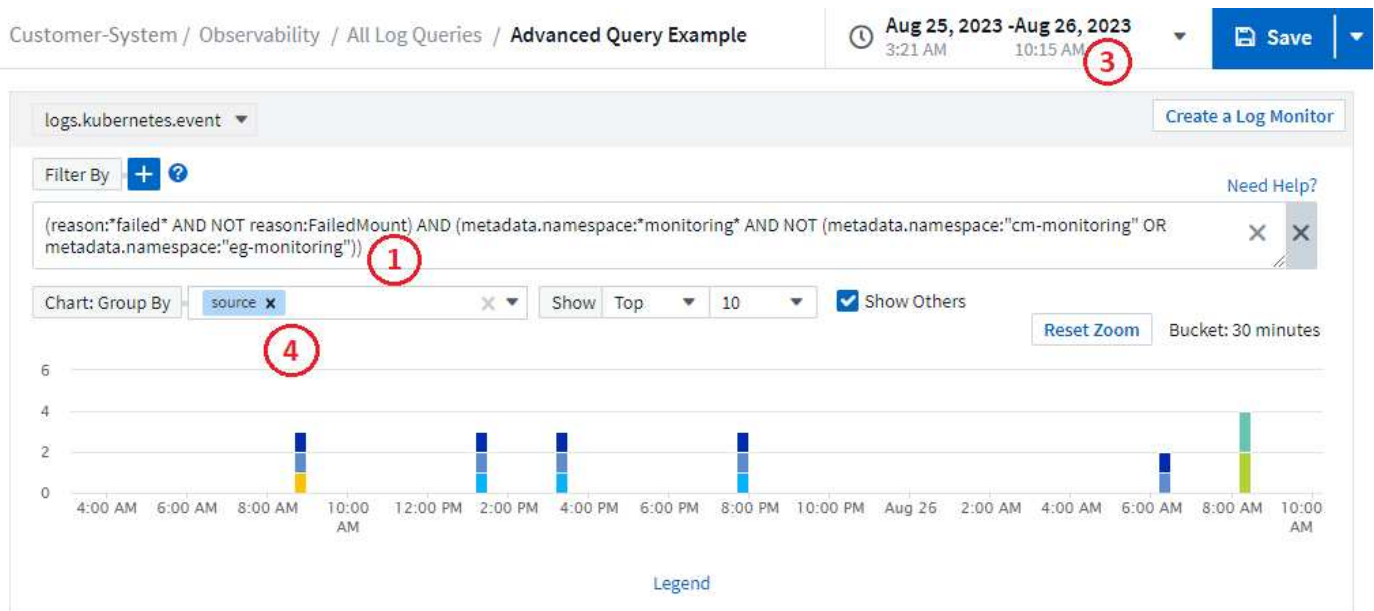
Filtragem avançada

Quando você está filtrando valores de texto ou lista em consultas ou widgets de painel, à medida que você começa a digitar, você recebe a opção de criar um filtro * curinga* com base no texto atual. Selecionar esta opção irá retornar todos os resultados que correspondem à expressão curinga. Você também pode criar expressões usando NOT, E, ou OU, ou, ou você pode selecionar a opção "nenhum" para filtrar os valores nulos.



Certifique-se de salvar sua consulta com antecedência e muitas vezes enquanto você cria sua filtragem. A consulta avançada é uma entrada de string "livre-forma", e a análise de erros pode ocorrer à medida que você constrói.

Dê uma olhada nesta imagem de tela mostrando resultados filtrados para uma consulta avançada do log *logs.kubernetes.event*. Há muita coisa acontecendo nesta página, o que é explicado abaixo da imagem:



Log Entries 2 Last updated 08/30/2023 9:54:13 AM

timestamp	source	message	metadata.namespace ↑	reason
08/26/2023 8:40:28 AM	kubernetes_cluster:eg-stream;namespace:33994-monitoring;pod_name:event-exporter-5db67db995-bxmkf;	Error: context deadline exceeded	k3s-cm-monitoring	Failed
08/26/2023 8:40:28 AM	kubernetes_cluster:eg-stream;namespace:ph-monitoring;pod_name:event-exporter-c4446976c-jxrdc;	Error: context deadline exceeded	k3s-cm-monitoring	Failed
08/26/2023 8:40:29 AM	kubernetes_cluster:eg-	Error: failed to reserve	k3s-cm-monitoring	Failed

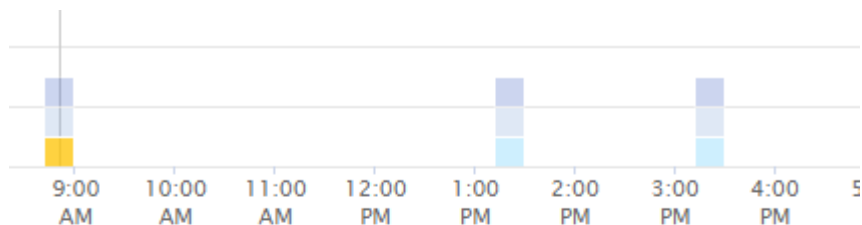
1. Esta cadeia de caracteres de consulta avançada filtra para o seguinte:

- Filtro para entradas de log com um *reason* que inclui a palavra "failed", mas não qualquer coisa com a razão específica de "FailedMount".
- Inclua qualquer uma dessas entradas que também incluía um *metadata.namespace* incluindo a palavra "monitoramento", mas exclua os espaços de nomes específicos de "monitoramento cm" ou

"monitoramento por exemplo".

Note que no caso acima, uma vez que ambos "cm-monitoring" e "eg-monitoring" contêm um traço ("-"), as strings devem ser incluídas em aspas duplas ou um erro de análise será exibido. Strings que não incluem traços, espaços, etc. não precisam ser incluídas em aspas. Em caso de dúvida, tente colocar a string em aspas.

- Os resultados do filtro atual, incluindo quaisquer valores "Filtrar por" E o filtro consulta Avançada, são exibidos na lista de resultados. A lista pode ser ordenada por qualquer coluna exibida. Para apresentar colunas adicionais, selecione o ícone de "engrenagem".
- O gráfico foi ampliado para mostrar apenas os resultados do log que ocorreram dentro de um período de tempo específico. O intervalo de tempo aqui apresentado reflete o nível de zoom atual. Selecione o botão *Reset Zoom* para definir o nível de zoom de volta para o intervalo de tempo atual do Data Infrastructure Insights.
- Os resultados do gráfico foram agrupados pelo campo *source*. O gráfico mostra os resultados em cada coluna agrupada em cores. Passar o Mouse sobre uma coluna no gráfico exibirá alguns detalhes sobre as entradas específicas.



Friday 08/25/2023 08:51:00 AM		
	kubernetes_cluster:vanilla25;namespace:docker-monitoring;pod_name:event-exporter-7d468bbf5b-8bzqt;	1 33.33%
	kubernetes_cluster:vanilla25;namespace:eg-monitoring;pod_name:event-exporter-7c4cb666d6-xd9mb;	1 33.33%
	kubernetes_cluster:vanilla25;namespace:oc-k3s-monitoring;pod_name:event-exporter-99d5fcfd8-lbg99;	1 33.33%
Total		3

Refinando filtros

Você pode usar o seguinte para refinar seu filtro:

Filtro	O que faz
* (Asterisco)	permite-lhe procurar tudo
? (ponto de interrogação)	permite-lhe procurar um número específico de caracteres
OU	permite especificar várias entidades
NÃO	permite excluir texto dos resultados da pesquisa

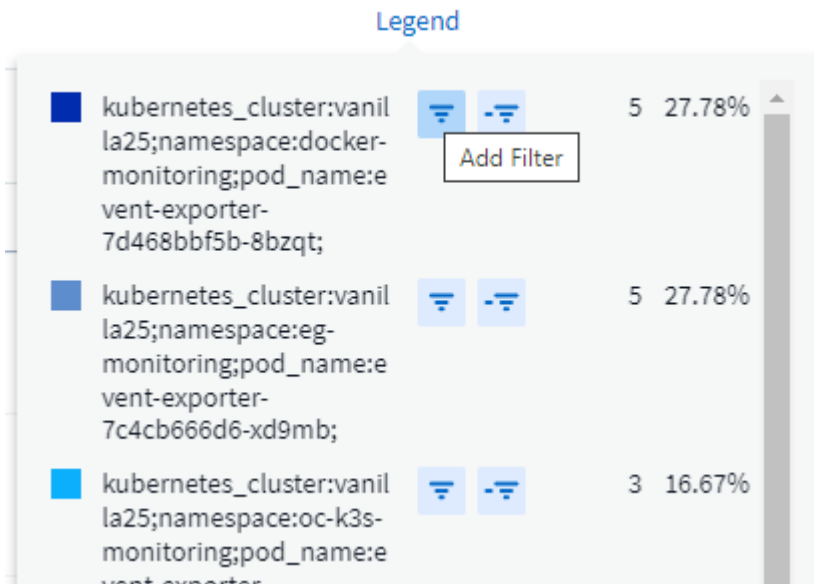
Nenhum	Procura valores NULL em todos os campos
Não *	Procura valores NULL em campos <i>text-only</i>

Se você incluir uma string de filtro em aspas duplas, o Insight trata tudo entre a primeira e a última citação como uma correspondência exata. Quaisquer caracteres especiais ou operadores dentro das aspas serão tratados como literais. Por exemplo, a filtragem para "*" retornará resultados que são um asterisco literal; o asterisco não será tratado como um curinga neste caso. Os operadores OU E NÃO também serão tratados como strings literais quando incluídos em aspas duplas.

Você pode combinar um filtro simples com um filtro de consulta avançado; o filtro resultante é um "E" dos dois.

A Legenda do Gráfico

O *Legend* abaixo do gráfico também tem algumas surpresas. Para cada resultado (com base no filtro atual) mostrado na Legenda, você tem uma opção para exibir apenas resultados para essa linha (Adicionar filtro) ou para exibir quaisquer resultados NÃO para essa linha (Adicionar filtro de exclusão). O gráfico e a lista de entradas de Registro são atualizados para mostrar resultados com base na sua seleção. Para remover essa filtragem, abra a Legenda novamente e selecione [X] para limpar o filtro baseado em Legenda.



Detalhes do log

Clicar em qualquer lugar de uma entrada de log na lista abrirá um painel de detalhes para essa entrada. Aqui você pode explorar mais informações sobre o evento.

Clique em "Adicionar filtro" para adicionar o campo selecionado ao filtro atual. A lista de entrada de registro será atualizada com base no novo filtro.

Observe que alguns campos não podem ser adicionados como filtros; nesses casos, o ícone *Adicionar filtro* não está disponível.

Log Details



timestamp

09/20/2021 9:03:36 PM

message

2021-09-20T15:33:36Z E! [processors.execcd] stderr: "Total time to process mountstats file: /hostfs/proc/1/mountstats, was: 0s"

id: 227814532095936770

node_name: ci-auto-dsacq-insights-1.cloudinsights-dev.netapp.com

Add Filter



source: telegraf-ds-dfcc5

type: logs.kubernetes

kubernetes

kubernetes.annotations.openshift.io_scc: telegraf-hostaccess

kubernetes.container_hash: ci-registry.nane.openenglab.netapp.com:8077/telegraf@sha256:00b45a7cc0761c

Solução de problemas

Aqui você encontrará sugestões para solucionar problemas com consultas de Log.

Problema:	Tente isto:
Não vejo mensagens "depurar" na minha consulta de log	Mensagens de log de depuração não são coletadas. Para capturar mensagens que você deseja, altere a gravidade da mensagem relevante para o nível <i>informacional</i> , <i>erro</i> , <i>alerta</i> , <i>emergência</i> , ou <i>aviso</i> .

Insights

Insights

Insights permitem que você analise coisas como o uso de recursos e como isso afeta outros recursos ou análises completas.

Vários Insights estão disponíveis. Navegue até **Dashboards > Insights** para começar a mergulhar. Você pode exibir Insights ativos (Insights que estão ocorrendo atualmente) na guia principal ou Insights inativos na guia *Inactive Insights*. Insights inativos são aqueles que estavam ativos anteriormente, mas não estão mais ocorrendo.

Tipos de insight

Recursos compartilhados sob estresse

Workloads de alto impacto podem reduzir o desempenho de outros workloads em um recurso compartilhado. Isso coloca o recurso compartilhado sob estresse. O Data Infrastructure Insights fornece ferramentas para ajudar você a investigar a saturação e o impactos dos recursos no localatário. ["Saiba mais"](#)

Namespaces do Kubernetes estão ficando sem espaço

Os namespaces do Kubernetes que estão fora do espaço Insight oferecem uma visão das cargas de trabalho nos namespaces do Kubernetes que correm o risco de ficar sem espaço, com uma estimativa do número de dias restantes antes que cada espaço fique cheio. ["Saiba mais"](#)

Recupere o storage frio da ONTAP

O Insight *Reclaim ONTAP Cold Storage* fornece dados sobre capacidade inativa, potencial economia de custo/energia e itens de ação recomendados para volumes em sistemas ONTAP. ["Saiba mais"](#)



Este é um recurso *Preview* e pode mudar com o tempo à medida que as melhorias são feitas. ["Saiba mais"](#) Sobre os recursos do Data Infrastructure Insights Preview.

Insights: Recursos compartilhados sob estresse

Workloads de alto impacto podem reduzir o desempenho de outros workloads em um recurso compartilhado. Isso coloca o recurso compartilhado sob estresse. O Data Infrastructure Insights fornece ferramentas para ajudar você a investigar a saturação e o impactos dos recursos no localatário.

Terminologia

Ao falar sobre carga de trabalho ou impactos de recursos, as seguintes definições são úteis.

Um **workloads exigentes** é uma carga de trabalho que atualmente é identificada como impactando outros recursos no pool de armazenamento compartilhado. Esses workloads geram IOPS mais altos (por exemplo), reduzindo o IOPS nos workloads afetados. As cargas de trabalho exigentes são às vezes chamadas de cargas de trabalho extremamente consumidoras_.

Uma carga de trabalho **impactada** é uma carga de trabalho que é afetada por uma carga de trabalho de alto consumo no pool de armazenamento compartilhado. Esses workloads apresentam IOPS reduzidos e/ou latência mais alta, causados por workloads exigentes.

Observe que se o Data Infrastructure Insights não descobrir o workload de computação líder, o volume ou o volume interno em si será reconhecido como o workload. Isso se aplica a workloads exigentes e afetados.

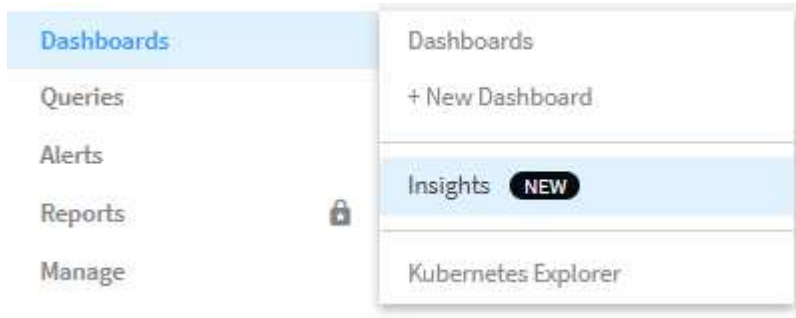
A saturação de recursos compartilhados é a taxa de impactos do IOPS para *linha de base*.

Baseline é definido como o ponto de dados máximo relatado para cada carga de trabalho na hora imediatamente anterior à saturação detetada.

Uma **contenção** ou **saturação** ocorre quando o IOPS está afetando outros recursos ou cargas de trabalho no pool de armazenamento compartilhado.

Workloads exigentes

Para começar a analisar cargas de trabalho exigentes e impactadas em seus recursos compartilhados, clique em **painéis > Insights** e selecione **recursos compartilhados sob estresse** Insight.



O Data Infrastructure Insights exibe uma lista de todas as cargas de trabalho em que uma saturação foi detetada. Observe que o Data Infrastructure Insights mostrará cargas de trabalho em que pelo menos um recurso *exigente* * ou * *recurso afetado* foi detetado.

Clique em uma carga de trabalho para exibir a página de detalhes para ela. O gráfico superior mostra a atividade no recurso compartilhado (por exemplo, um pool de armazenamento) no qual a contenção/saturação está ocorrendo.



Abaixo estão dois gráficos que mostram as cargas de trabalho *exigentes* e as cargas de trabalho que são *afetadas* por essas cargas de trabalho exigentes.





Abaixo de cada tabela, há uma lista de workloads e/ou recursos que afetam ou são afetados pela contenção. Clicar em um recurso (por exemplo, uma VM) abre uma página de detalhes para esse recurso. Clicar em uma carga de trabalho abre uma página de consulta mostrando os pods envolvidos. Observe que se o link abrir uma consulta vazia, pode ser porque o pod afetado não faz mais parte da contenção ativa. Você pode modificar o intervalo de tempo da consulta para exibir a lista de pods em um intervalo de tempo maior ou mais focado.

O que faço para resolver a saturação?

Há uma série de etapas que você pode tomar para reduzir ou eliminar a chance de saturação em seu inquilino. Estes são mostrados expandindo o link **Mostrar recomendações** na página. Aqui estão algumas coisas que você pode tentar.

- Mova os consumidores de IOPS alto

Mova as cargas de trabalho "exigentes" para pools de storage menos saturados. Recomenda-se avaliar o nível e a capacidade desses pools antes de mover as cargas de trabalho, a fim de evitar custos desnecessários ou contenções adicionais.

- Implementar uma política de qualidade de serviço (QoS)

A implementação de uma política de QoS por workload para garantir recursos livres suficientes disponíveis aliviará a saturação no pool de storage. Esta é uma solução a longo prazo.

- Adicione recursos adicionais

Se o recurso compartilhado (por exemplo, pool de armazenamento) atingir o ponto de saturação de IOPS, adicionar mais ou mais discos mais rápidos ao pool garantirá recursos livres suficientes disponíveis para aliviar a saturação.

Finalmente, você pode clicar no **Copy Insight Link** para copiar o url da página para a área de transferência, para compartilhar com os colegas mais facilmente.

Insights: Namespaces do Kubernetes sem espaço

Ficar sem espaço em seu inquilino nunca é uma boa situação. O Data Infrastructure Insights ajuda a prever o tempo que você fez antes dos volumes persistentes do Kubernetes ficarem cheios.

Os namespaces *Kubernetes em execução fora do espaço* Insight oferecem uma visão das cargas de trabalho nos namespaces do Kubernetes que correm o risco de ficar sem espaço, com uma estimativa do número de dias restantes antes que cada volume persistente fique cheio.

Pode visualizar este Insight navegando até **painéis > Insights**.

Kubernetes Namespaces Running Out of Space (3)

Description	Estimated Days to Full	Workloads at Risk	Detected ↓
1 workload at risk on es	35	1	2 days ago
1 workload at risk on manager	24	1	2 days ago
2 workloads at risk on cloudinsights	1	2	2 days ago

Clique em uma carga de trabalho para abrir uma página de detalhes do Insight. Nesta página, você verá um gráfico mostrando as tendências de capacidade de carga de trabalho, bem como uma tabela mostrando o seguinte:

- Nome da carga de trabalho
- Volume persistente afetado
- Tempo previsto para cheio em dias
- Capacidade de volume persistente
- Recurso de armazenamento de backend afetado, com capacidade atual usada fora da capacidade total. Clicar neste link irá opoen a página de destino detalhada para o volume de back-end.

Workloads at risk (2)

<input type="checkbox"/> Workloads	Persistent Volume (pvClaim)	Time to Full (Days) ↓	Persistent Volume Capacity (GiB)	Backend Storage Resource (Capacity Used)
<input checked="" type="checkbox"/> multi (1)	pv1 (pvc1)	1	4.00	internal-volume-601 60.00% (3.00/5.00 GiB)
<input checked="" type="checkbox"/> taskmanager (1)	pv1 (pvc1)	1	4.00	internal-volume-601 60.00% (3.00/5.00 GiB)

O que posso fazer se estou ficando sem espaço?

Na página Insight, clique em ** Mostrar recomendações** para ver possíveis soluções. A opção mais fácil quando ficar sem espaço é sempre adicionar mais capacidade, e o Data Infrastructure Insights mostra a capacidade ideal a ser adicionada para aumentar o tempo de espera para uma previsão de 60 dias. Outras recomendações também são mostradas.

Show Recommendations

- 1 Get time to full back up to 60 days by adding more capacity to backend resources
Add to the following resources to bring time-to-full up to ideal capacity.

Backend Resource ↓	Current Capacity (time to full)	Recommended Capacity to Add	Ideal Capacity (time to full)
internal-volume-601	2.00 GiB 1 Days	+ 518.79 GiB	= 520.79 GiB 60 Days

- 2 Use NetApp Astra Trident with your K8s to automatically grow capacity
Astra Trident can keep your capacity lean without risk of running out of space.

[Learn more about !\[\]\(0f848bbd71cef6b345273b16f905912a_img.jpg\) Astra Trident](#)

[Copy Insight Link](#)

É aqui também que você pode copiar um link conveniente para este Insight, para marcar a página ou para compartilhar facilmente com sua equipe.

Insights: Recupere o storage frio da ONTAP

O Insight *Reclaim ONTAP Cold Storage* fornece dados sobre capacidade inativa, potencial economia de custo/energia e itens de ação recomendados para volumes em sistemas ONTAP.

Para exibir esses insights, navegue até **painéis > Insights** e confira o Insight *recuperar o storage frio do ONTAP*. Observe que esse Insight listará somente armazenamentos afetados se o Data Infrastructure Insights detectar armazenamento frio, caso contrário você verá uma mensagem "All Clear".

Tenha em mente que os dados inativos com menos de 30 dias de idade não são exibidos.

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

A descrição do Insight fornece uma indicação rápida da quantidade de dados detetados como "frios" e em que armazenamento esses dados residem. A tabela também fornece uma contagem de workloads com dados inativos.

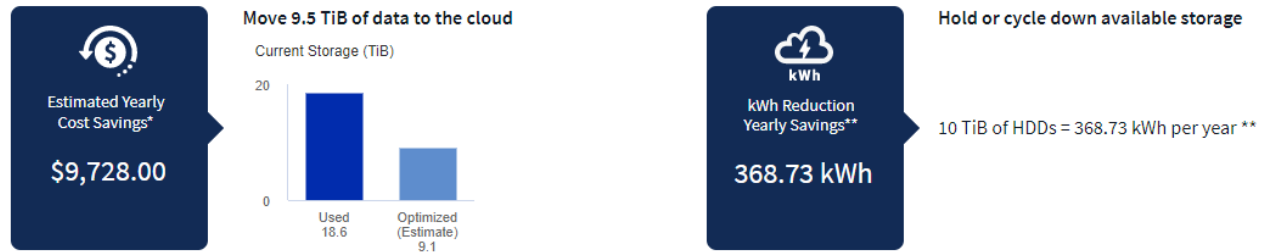
A seleção de um Insight da lista abre uma página que mostra mais detalhes, incluindo recomendações para mover dados para a nuvem ou reduzir o ciclo de discos não usados, bem como economia estimada de custo e energia que você poderia obter com a implementação dessas recomendações. A página ainda fornece um link útil para "[Calculadora de TCO da NetApp](#)" que você possa experimentar os números.



150 Workloads on storage `rtp-sa-cl01` contains a total of 9.5 TiB of cold data.

You could lower costs 9.3% a year and reduce your carbon footprint by moving cold storage to the cloud.

Detected: 2 months ago, 9:21 AM
(ACTIVE)
May 19, 2023 10:05AM



*Visit the [NetApp TCO Calculator](#) for your actual cost savings.
Go to [Annotation Page](#) to edit the cloud tier cost in the tier annotation.

** Based on average disk power consumption

Recomendações

Na página Insight, expanda **recomendações** para explorar as seguintes opções:

- Mova workloads não utilizados (Zumbis) para uma camada de storage (HDD) de custo mais baixo

Usando o sinalizador de Zumbis, storage frio e número de dias, encontre a maior quantidade de dados mais fria e mova a carga de trabalho para uma camada de storage de custo mais baixo (como um pool de storage que usa storage em disco rígido). Uma carga de trabalho é considerada um "Zumbi" quando o is não recebeu nenhuma solicitação significativa de IO por 30 dias ou mais.

- Excluir workloads não utilizados

Verifique quais workloads não estão em uso e considere arquivá-los ou removê-los do sistema de storage.

- Considere a solução Fabric Pool da NetApp

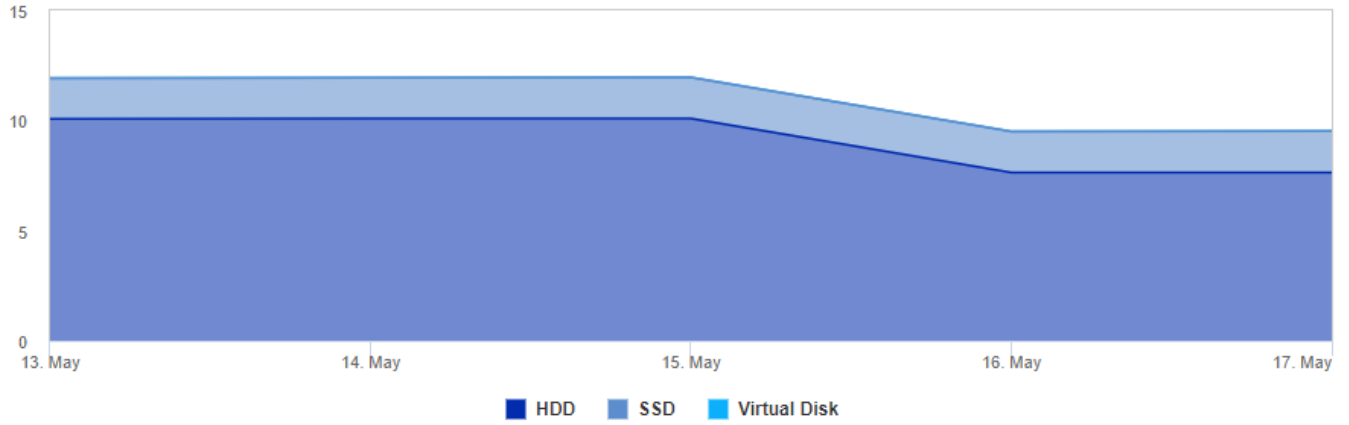
O NetApp "[Solução Fabric Pool](#)" coloca automaticamente dados inativos em camadas de storage de nuvem de baixo custo, aumentando assim a eficiência de sua categoria de performance e fornecendo proteção remota de dados.

Visualize e explore

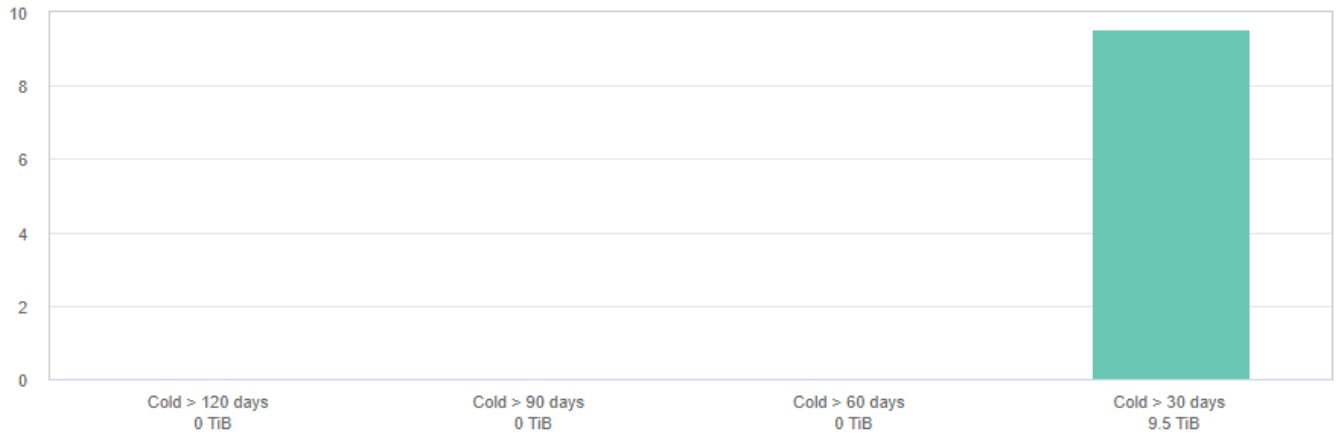
Os gráficos e a tabela fornecem informações de tendências adicionais, além de permitir que você explore as cargas de trabalho individuais.

Cluster Cold Storage Trend [Show Details](#)

Cold Data (TiB)



Cold Storage by Days Cold (TiB)



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

Monitores e alertas

Alertas com monitores

Você cria monitores para definir limites que acionam alertas para notificá-lo sobre problemas relacionados aos recursos da rede. Por exemplo, você pode criar um monitor para alertar para *node write latency* para qualquer um dos vários protocolos.



Monitores e alertas estão disponíveis em todas as edições do Data Infrastructure Insights, no entanto, o Basic Edition está sujeito ao seguinte: * Você só pode ter até cinco monitores personalizados ativos de cada vez. Qualquer monitor além de cinco será criado ou movido para o estado *Pausado*. * Os monitores de métricas VMDK, Virtual Machine, Host e datastore não são suportados. Se você tiver monitores criados para essas métricas, eles serão pausados e não poderão ser retomados ao fazer o downgrade para Basic Edition.

Os monitores permitem definir limites para métricas geradas por objetos de "infraestrutura", como armazenamento, VM, EC2 e portas, bem como para dados de "integração", como os coletados para Kubernetes, métricas avançadas do ONTAP e plugins do Telegraf. Esses monitores *métricos* alertam você quando os limites de nível de aviso ou nível crítico são cruzados.

Você também pode criar monitores para acionar alertas de nível de aviso, crítico ou informativo quando os eventos *log* especificados são detetados.

O Data Infrastructure Insights também fornece várias opções "[Monitores definidos pelo sistema](#)", com base no seu ambiente.

Melhores práticas de segurança

Os alertas do Data Infrastructure Insights são projetados para destacar pontos de dados e tendências em seu locatário, e o Data Infrastructure Insights permite que você insira qualquer endereço de e-mail válido como destinatário de alerta. Se você estiver trabalhando em um ambiente seguro, esteja especialmente ciente de quem está recebendo a notificação ou de outra forma tem acesso ao alerta.

Monitor métrico ou de registro?

1. No menu Data Infrastructure Insights, clique em **Alertas > Gerenciar monitores**

É apresentada a página da lista de monitores, mostrando os monitores atualmente configurados.

2. Para modificar um monitor existente, clique no nome do monitor na lista.
3. Para adicionar um monitor, clique em * Monitor*.



Ao adicionar um novo monitor, você será solicitado a criar um Monitor de métricas ou um Monitor de Registros.

- *Metric* monitora alertas sobre gatilhos relacionados à infraestrutura ou ao desempenho
- *Log* monitora o alerta na atividade relacionada ao log

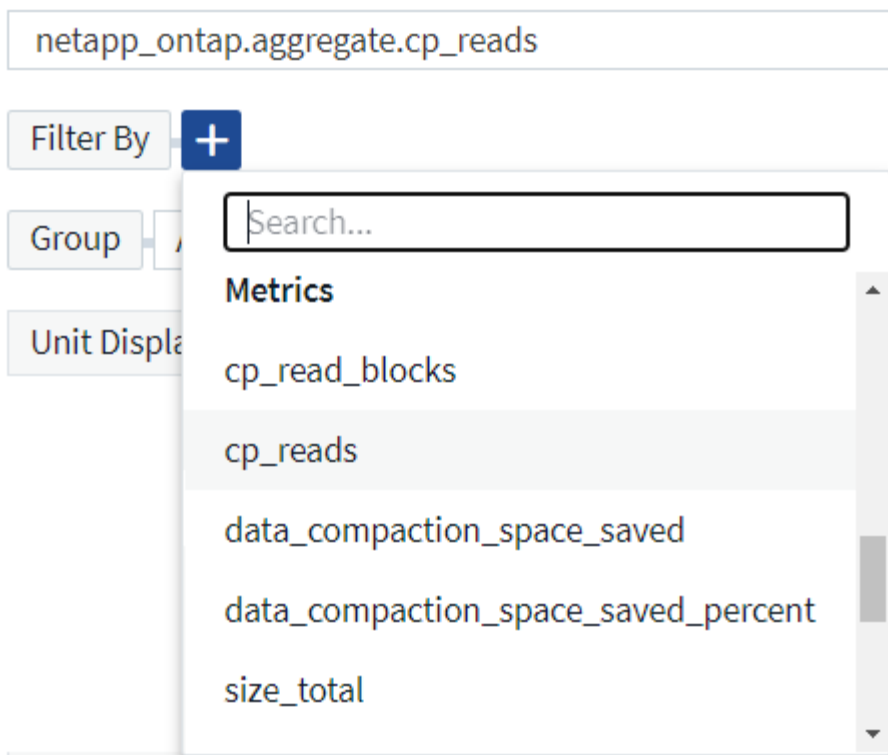
Depois de escolher o tipo de monitor, a caixa de diálogo Configuração do monitor é exibida. A configuração varia dependendo do tipo de monitor que você está criando.

Monitor métrico

1. Na lista suspensa, procure e escolha um tipo de objeto e uma métrica para monitorar.

Você pode definir filtros para restringir quais atributos ou métricas do objeto monitorar.

1 Select a metric to monitor



Ao trabalhar com dados de integração (Kubernetes, dados avançados do ONTAP, etc.), a filtragem de métricas remove os pontos de dados individuais/não correspondidos da série de dados plotados, ao contrário dos dados de infraestrutura (armazenamento, VM, portas, etc.), onde os filtros funcionam no valor agregado da série de dados e potencialmente removem todo o objeto do gráfico.



Para criar um monitor de várias condições (por exemplo, IOPS > X e latência > Y), defina a primeira condição como um limite e a segunda condição como um filtro.

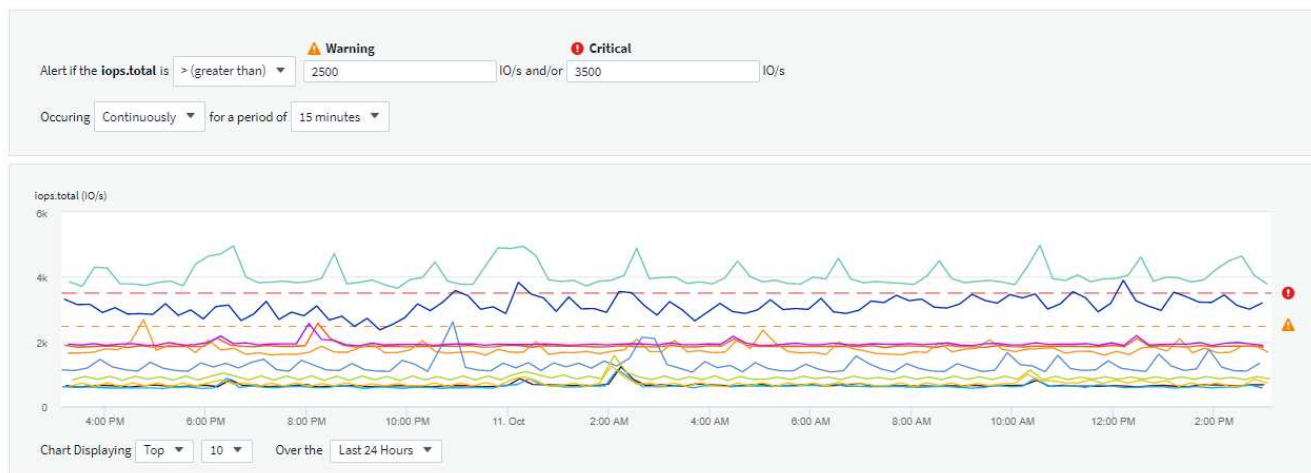
Defina as condições do Monitor.

1. Depois de escolher o objeto e a métrica a monitorar, defina os limites nível de Advertência e/ou nível crítico.
2. Para o nível *Warning*, digite 200 para nosso exemplo. A linha tracejada que indica este nível de aviso é apresentada no gráfico de exemplo.
3. Para o nível *Critical*, digite 400. A linha tracejada indicando este nível crítico é exibida no gráfico de exemplo.

O gráfico exibe dados históricos. As linhas de Aviso e nível crítico no gráfico são uma representação visual do Monitor, para que você possa ver facilmente quando o Monitor pode acionar um alerta em cada caso.

4. Para o intervalo de ocorrência, escolha *continuamente* por um período de *15 minutos*.

Você pode optar por acionar um alerta no momento em que um limite é violado ou esperar até que o limite esteja em violação contínua por um período de tempo. Em nosso exemplo, não queremos ser alertados sempre que o total de IOPS atingir picos acima do nível de Aviso ou crítico, mas apenas quando um objeto monitorado excede continuamente um desses níveis por pelo menos 15 minutos.



Defina o comportamento da resolução de alerta

Você pode escolher como um alerta de monitor métrico é resolvido. São apresentadas duas opções:

- Resolva quando a métrica retornar ao intervalo aceitável.
- Resolva quando a métrica estiver dentro do intervalo aceitável por um período de tempo especificado, de 1 minuto a 7 dias.

Monitor de registro

Ao criar um **monitor de log**, primeiro escolha qual log monitorar na lista de Registros disponíveis. Em seguida, você pode filtrar com base nos atributos disponíveis como acima. Você também pode escolher um ou mais atributos "Agrupar por".



O filtro do Monitor de Registros não pode estar vazio.

1 Select the log to monitor

Log Source logs.netapp.ems

Filter By

- ems.ems_message_type Nblade.vscanConnBackPressure
- ems.cluster_vendor NetApp
- ems.cluster_model FAS* AFF* ASA* FDvM*

Group By

- ems.cluster_uuid
- ems.cluster_vendor
- ems.cluster_model
- ems.cluster_name
- ems.svm_uuid
- ems.svm_name

Defina o comportamento do alerta

Você pode criar o monitor para alertar com um nível de gravidade de *crítico*, *Aviso* ou *informativa*, quando as condições definidas acima ocorrem uma vez (ou seja, imediatamente), ou esperar para alertar até que as condições ocorram 2 vezes ou mais.

Defina o comportamento da resolução de alerta

Você pode escolher como um alerta de monitor de log é resolvido. São apresentadas três opções:

- **Resolve instantaneamente:** O alerta é imediatamente resolvido sem necessidade de qualquer outra ação

- **Resolver com base no tempo:** O alerta é resolvido após o tempo especificado ter passado
- **Resolver com base na entrada de log:** O alerta é resolvido quando uma atividade de log subsequente ocorreu. Por exemplo, quando um objeto é registrado como "disponível".

- Resolve instantly
- Resolve based on time
- Resolve based on log entry

Log Source logs.netapp.ems ▾

Filter By ems.ems_message_type "object.store.available" × × ▾ × +

Monitor de detecção de anomalias

1. Na lista suspensa, procure e escolha um tipo de objeto e uma métrica para monitorar.

Você pode definir filtros para restringir quais atributos ou métricas do objeto monitorar.

1 Select a metric anomaly to monitor

Object Storage × ▾ Metric iops.total × ▾

Filter by Attribute + ?

Filter by Metric + ?

Group by Storage ▾

Unit Displayed In Whole Number ▾

Defina as condições do Monitor.

1. Depois de escolher o objeto e a métrica para monitorar, defina as condições em que uma anomalia é detectada.
 - Escolha se deseja detectar uma anomalia quando a métrica escolhida **picos acima** dos limites previstos, **caí abaixo** desses limites, ou **picos acima ou abaixo** dos limites.
 - Defina a **sensibilidade** da detecção. **Low** (menos anomalias são detectadas), **Medium** ou **High** (mais anomalias são detectadas).
 - Defina os alertas como **Aviso** ou **crítico**.
 - Se desejar, você pode optar por reduzir o ruído, ignorando anomalias quando a métrica escolhida estiver abaixo de um limite definido.

2 Define the monitor's conditions

Trigger alert when **performance.iops.total** Spikes above ▼ the predicted bounds.

Set sensitivity: Low (detect fewer anomalies) ▼

Alert severity: Critical ▼

To reduce noise, ignore anomalies when **performance.iops.total** is below Optional IO/s

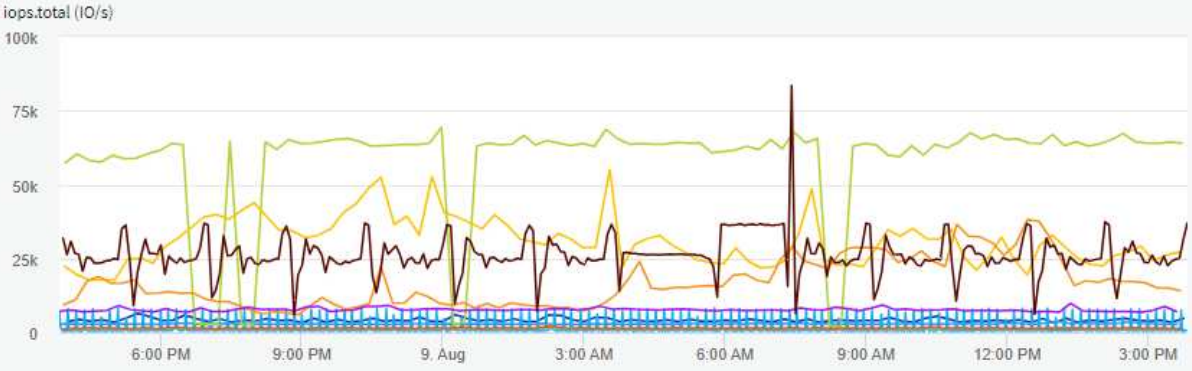
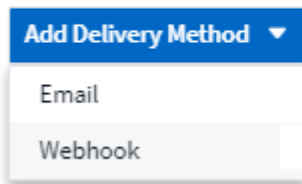


Chart Displaying Top ▼ 10 ▼ Over the Last 24 Hours ▼

Selecione o tipo de notificação e destinatários

Na seção *Configurar notificação(s) da equipe*, você pode escolher se deseja alertar sua equipe por e-mail ou Webhook.

3 Set up team notification(s) (alert your team via email, or Webhook)



Alerta via e-mail:

Especifique os destinatários de e-mail para notificações de alerta. Se desejar, você pode escolher diferentes destinatários para alertas ou alertas críticos.

3 Set up team notification(s)

The screenshot shows two identical sections for setting up email notifications. Each section starts with an 'Email' icon and the text 'Email'. The first section has a 'Notify team on' dropdown menu with 'Critical, Resolved' selected, and a list below it with 'Critical' and 'Resolved' checked, and 'Warning' unchecked. The 'Add Recipients (Required)' field contains two email addresses: 'user_1@email.com' and 'user_2@email.com'. The second section has a 'Notify team on' dropdown menu with 'Warning' selected, and the 'Add Recipients (Required)' field contains one email address: 'user_3@email.com'.

Alerting via Webhook:

Especifique o(s) webhook(s) para notificações de alerta. Se desejar, você pode escolher diferentes webhooks para alertas críticos ou alertas.

3 Set up team notification(s) (alert your team via email, or Webhook)

The screenshot shows three sections for setting up webhook notifications. Each section starts with 'By Webhook' and 'Slack'. The first section has a 'Notify team on' dropdown menu with 'Critical' selected, and a 'Use Webhook(s)' field with 'Slack' and 'Teams' selected. The second section has a 'Notify team on' dropdown menu with 'Resolved' selected, and a 'Use Webhook(s)' field with 'Slack' and 'Teams' selected. The third section has a 'Notify team on' dropdown menu with 'Warning' selected, and a 'Use Webhook(s)' field with 'Slack' and 'Teams' selected.



As notificações do ONTAP Data Collector têm precedência sobre quaisquer notificações específicas do Monitor que sejam relevantes para o cluster/coletor de dados. A lista de destinatários definida para o coletor de dados receberá os alertas do coletor de dados. Se não houver alertas ativos do coletor de dados, os alertas gerados pelo monitor serão enviados para destinatários específicos do monitor.

Definir ações corretivas ou informações adicionais

Você pode adicionar uma descrição opcional, bem como informações adicionais e/ou ações corretivas preenchendo a seção **Adicionar uma descrição de alerta**. A descrição pode ter até 1024 caracteres e será enviada com o alerta. O campo de insights/ação corretiva pode ter até 67.000 caracteres e será exibido na seção de resumo da página de destino de alerta.

Nesses campos, você pode fornecer notas, links ou etapas a serem tomadas para corrigir ou resolver o alerta.

4 Add an alert description (optional)

Add a description	<input type="text" value="Enter a description that will be sent with this alert (1024 character limit)"/>
Add insights and corrective actions	<input type="text" value="Enter a url or details about the suggested actions to fix the issue raised by the alert"/>

Guarde o monitor

1. Se desejar, pode adicionar uma descrição do monitor.
2. Dê ao Monitor um nome significativo e clique em **Salvar**.

O novo monitor é adicionado à lista de monitores ativos.

Lista de monitores

A página Monitor lista os monitores configurados atualmente, mostrando o seguinte:

- Nome do monitor
- Estado
- Objeto/métrica sendo monitorado
- Condições do monitor

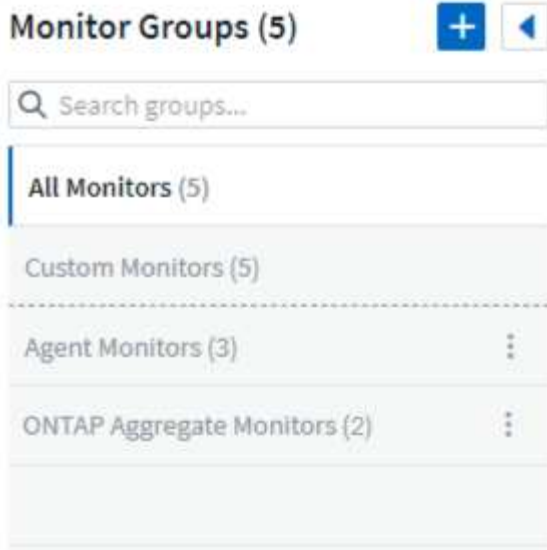
Você pode optar por pausar temporariamente o monitoramento de um tipo de objeto clicando no menu à direita do monitor e selecionando **Pausa**. Quando estiver pronto para retomar a monitorização, clique em **Resume**.

Você pode copiar um monitor selecionando **duplicar** no menu. Em seguida, você pode modificar o novo monitor e alterar o objeto/métrica, filtro, condições, destinatários de e-mail, etc.

Se um monitor não for mais necessário, você pode excluí-lo selecionando **Excluir** no menu.

Monitorar grupos

O agrupamento permite visualizar e gerir monitores relacionados. Por exemplo, você pode ter um grupo de monitores dedicado ao armazenamento no locatário ou monitores relevantes para uma determinada lista de destinatários.



São apresentados os seguintes grupos de monitorização. O número de monitores contidos em um grupo é mostrado ao lado do nome do grupo.

- **Todos os monitores** lista todos os monitores.
- **Monitores personalizados** lista todos os monitores criados pelo usuário.
- **Monitores suspensos** listarão todos os monitores do sistema que foram suspensos pelo Data Infrastructure Insights.
- Os Insights de infraestrutura de dados também mostrarão vários **grupos de Monitor do sistema**, que listarão um ou mais grupos de "monitores definidos pelo sistema", incluindo monitores de infraestrutura e carga de trabalho do ONTAP.



Os monitores personalizados podem ser pausados, retomados, excluídos ou movidos para outro grupo. Os monitores definidos pelo sistema podem ser colocados em pausa e retomados, mas não podem ser eliminados ou movidos.

Monitores suspensos

Esse grupo só será exibido se o Data Infrastructure Insights tiver suspenso um ou mais monitores. Um monitor pode ser suspenso se estiver gerando alertas excessivos ou contínuos. Se o monitor for um monitor personalizado, modifique as condições para evitar o alerta contínuo e, em seguida, retome o monitor. O monitor será removido do grupo de monitores suspensos quando o problema que causa a suspensão for resolvido.

Monitores definidos pelo sistema

Esses grupos mostrarão os monitores fornecidos pelo Data Infrastructure Insights, desde que seu ambiente contenha os dispositivos e/ou a disponibilidade de log exigida pelos monitores.

Os monitores definidos pelo sistema não podem ser modificados, movidos para outro grupo ou eliminados. No entanto, você pode duplicar um monitor do sistema e modificar ou mover a duplicata.

Os monitores do sistema podem incluir monitores para infraestrutura ONTAP (storage, volume, etc.) ou cargas de trabalho (ou seja, monitores de log) ou outros grupos. A NetApp está constantemente avaliando as necessidades do cliente e a funcionalidade do produto e atualizará ou adicionará aos monitores e grupos do sistema conforme necessário.

Grupos de monitores personalizados

Você pode criar seus próprios grupos para conter monitores com base em suas necessidades. Por exemplo, você pode querer um grupo para todos os monitores relacionados ao armazenamento.

Para criar um novo grupo de monitores personalizados, clique no botão criar novo grupo de monitores*. Digite um nome para o grupo e clique em **criar grupo**. Um grupo vazio é criado com esse nome.

Para adicionar monitores ao grupo, vá para o grupo *todos os monitores* (recomendado) e siga um destes procedimentos:

- Para adicionar um único monitor, clique no menu à direita do monitor e selecione *Adicionar ao grupo*. Escolha o grupo ao qual deseja adicionar o monitor.
- Clique no nome do monitor para abrir a visualização de edição do monitor e selecione um grupo na seção *associar a um grupo de monitores*.

5 Associate to a monitor group (optional)

A screenshot of a dropdown menu with a light gray border. The text 'ONTAP Monitors' is displayed in a dark gray font. A small downward-pointing triangle is visible on the right side of the menu, indicating it is a dropdown.

Remova os monitores clicando em um grupo e selecionando *Remover do Grupo* no menu. Não é possível remover monitores do grupo *todos os monitores* ou *monitores personalizados*. Para excluir um monitor desses grupos, você deve excluir o próprio monitor.

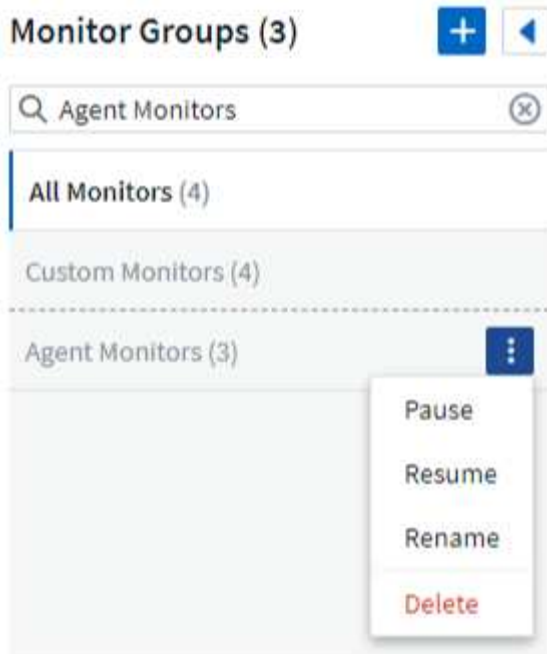


A remoção de um monitor de um grupo não exclui o monitor do Data Infrastructure Insights. Para remover completamente um monitor, selecione o monitor e clique em *Delete*. Isso também o remove do grupo ao qual pertencia e não está mais disponível para nenhum usuário.

Você também pode mover um monitor para um grupo diferente da mesma maneira, selecionando *mover para Grupo*.

Para pausar ou retomar todos os monitores em um grupo de uma vez, selecione o menu do grupo e clique em *Pausa* ou *Retomar*.

Use o mesmo menu para renomear ou excluir um grupo. A exclusão de um grupo não exclui os monitores do Data Infrastructure Insights; eles ainda estão disponíveis em *todos os monitores*.



Monitores definidos pelo sistema

O Data Infrastructure Insights inclui vários monitores definidos pelo sistema para métricas e logs. Os monitores do sistema disponíveis dependem dos coletores de dados presentes no localatário. Devido a isso, os monitores disponíveis no Data Infrastructure Insights podem mudar à medida que os coletores de dados são adicionados ou suas configurações alteradas.

Consulte "[Monitores definidos pelo sistema](#)" a página para obter descrições de monitores incluídos no Data Infrastructure Insights.

Mais informações

- "[Visualização e ausência de alertas](#)"

Visualizar e gerir alertas a partir de monitores

O Data Infrastructure Insights exibe alertas quando "[limites monitorados](#)" são excedidos.



Monitores e alertas estão disponíveis no Data Infrastructure Insights Standard Edition e versões posteriores.

Visualizar e gerir alertas

Para visualizar e gerenciar alertas, faça o seguinte.

1. Navegue até a página **Alertas > todos os Alertas**.
2. É apresentada uma lista de até 1.000 alertas mais recentes. Você pode classificar essa lista em qualquer campo clicando no cabeçalho da coluna do campo. A lista apresenta as seguintes informações. Observe que nem todas essas colunas são exibidas por padrão. Você pode selecionar colunas para exibir clicando no ícone "engrenagem":
 - **ID de alerta:** ID de alerta exclusivo gerado pelo sistema

- **Hora desencadeada:** A hora em que o Monitor relevante acionou o alerta
- **Gravidade atual** (guia alertas ativos): A gravidade atual do alerta ativo
- **Gravidade superior** (guia alertas resolvidos); a gravidade máxima do alerta antes de ser resolvido
- **Monitor:** O monitor configurado para acionar o alerta
- **Triggered on:** O objeto no qual o limite monitorado foi violado
- **Status:** Status de alerta atual, *novo* ou *em processo*
- **Status Ativo:** *Ativo* ou *resolvido*
- **Condição:** A condição limite que acionou o alerta
- **Metric:** A métrica do objeto na qual o limite monitorado foi violado
- **Status do monitor:** Status atual do monitor que acionou o alerta
- **Tem ação corretiva:** O alerta sugeriu ações corretivas. Abra a página de alerta para visualizá-los.

Você pode gerenciar um alerta clicando no menu à direita do alerta e escolhendo uma das seguintes opções:

- **Em processo** para indicar que o alerta está sob investigação ou precisa ser mantido aberto
- **Dismiss** para remover o alerta da lista de alertas ativos.

Você pode gerenciar vários alertas selecionando a caixa de seleção à esquerda de cada Alerta e clicando em *alterar Status dos Alertas selecionados*.

Clicar em um ID de alerta abre a página de detalhes de alerta.

Página de detalhes do alerta

A Página de Detalhes do alerta fornece detalhes adicionais sobre o alerta, incluindo um *Summary*, uma *Expert View* mostrando gráficos relacionados aos dados do objeto, quaisquer ativos relacionados_ e *Comments* inseridos pelos investigadores do alerta.

Alert Summary

Monitor:

Volume Total Data

Triggered On:

cluster_name: tawny
aggr_name: Multiple_Values

Duration / Time Triggered:

1d 6h / Jun 9, 2020 2:22 AM

Top Severity:

❗ Critical

Metric:

📊 netapp_ontap.workload_volume.total_data

Condition:

Average total_data is > (greater than) 0m and/or 0m all the time in 2-hour window.

Filters Applied:

cluster_name: Any

Status:

New

Expert View

Display Metrics ▾



Related Alerts

1 item found

Alert ID	Active Status	Triggered Time ↓	Top Severity	Monitor	Triggered On	Status
AL-46769	Resolved	a day ago Jun 9, 2020 2:22 AM	❗ Critical	Volume Total Data	cluster_name: tawny aggr_name: Multiple_Values	New

Comments

There are no comments yet on this alert.

[+ Comment](#)

Alerta quando os dados estão em falta

Em um sistema em tempo real, como o Data Infrastructure Insights, para acionar a análise de um Monitor para decidir se um Alerta deve ser gerado, contamos com uma de duas coisas:

- a próxima datapoint para chegar
- um temporizador para disparar quando não há datapoint e você esperou o suficiente

Como é o caso com chegada lenta de dados - ou sem chegada de dados - o mecanismo do temporizador precisa assumir o controle, pois a taxa de chegada de dados é insuficiente para acionar alertas em "tempo real". Então, a pergunta geralmente se torna "quanto tempo eu espero antes de fechar a janela de análise e olhar para o que eu tenho?" Se você esperar muito tempo, então você não está gerando os alertas rápido o suficiente para ser útil.

Se você tiver um Monitor com uma janela de 30 minutos que percebe que uma condição é violada pelo último ponto de dados antes de uma perda de dados a longo prazo, um Alerta será gerado porque o Monitor não recebeu outras informações para usar para confirmar uma recuperação da métrica ou notar que a condição persistiu.

Alertas "permanentemente ativos"

É possível configurar um monitor de tal forma que a condição **Always** exista no objeto monitorado - por exemplo, IOPS > 1 ou latência > 0. Estes são frequentemente criados como monitores de "teste" e depois

esquecidos. Esses monitores criam alertas que permanecem permanentemente abertos nos objetos constituintes, o que pode causar problemas de estresse e estabilidade do sistema ao longo do tempo.

Para evitar isso, o Data Infrastructure Insights fechará automaticamente qualquer alerta "permanentemente ativo" após 7 dias. Observe que as condições subjacentes do monitor podem (provavelmente) continuar a existir, fazendo com que um novo alerta seja emitido quase imediatamente, mas esse fechamento de alertas "sempre ativos" alivia algumas das tensões do sistema que podem ocorrer de outra forma.

Configurar notificações por e-mail

Você pode configurar uma lista de e-mail para notificações relacionadas a assinatura, bem como uma lista global de destinatários para notificação de violações de limite de política de desempenho.

Para configurar as configurações do destinatário de e-mail de notificação, vá para a página **Admin > notificações** e selecione a guia *e-mail*.

Subscription Notification Recipients

Send subscription related notifications to the following:

- All Account Owners
- All Monitor & Optimize Administrators
- Additional Email Addresses

name@email.com ×

Save

Global Monitor Notification Recipients

Default email recipients for monitor related notifications:

- All Account Owners
- All Monitor & Optimize Administrators
- Additional Email Addresses

Save

Destinatários da notificação de assinatura

Para configurar os destinatários para notificações de eventos relacionadas à assinatura, vá para a seção "destinatários de notificação de assinatura". Você pode optar por enviar notificações por e-mail para eventos relacionados à assinatura para qualquer um ou todos os seguintes destinatários:

- Todos os proprietários de contas
- Todos os administradores *Monitor & Optimize*
- Endereços de e-mail adicionais que você especificar

A seguir estão exemplos dos tipos de notificações que podem ser enviadas e as ações do usuário que você pode executar.

Notificação:	Ação do Usuário:
--------------	------------------

A versão de avaliação ou subscrição foi atualizada	Reveja os detalhes da subscrição " Subscrição " na página
A assinatura expirará em 90 dias. A assinatura expirará em 30 dias	Nenhuma ação necessária se a "renovação automática" estiver ativada, o Contato " Vendas da NetApp " para renovar a assinatura
O teste termina em 2 dias	Renove o teste a partir " Subscrição " da página. Você pode renovar um teste uma vez. " Vendas da NetApp " Contacte para adquirir uma subscrição
A conta de teste ou assinatura expirou deixará de coletar dados em 48 horas a conta será excluída após 48 horas	" Vendas da NetApp " Contacte para adquirir uma subscrição

Lista de destinatários globais para alertas

As notificações por e-mail de alertas são enviadas para a lista de destinatários de alerta para cada ação no alerta. Você pode optar por enviar notificações de alerta para uma lista global de destinatários.

Para configurar destinatários de alerta global, escolha os destinatários desejados na seção **destinatários de notificação do Monitor Global**.

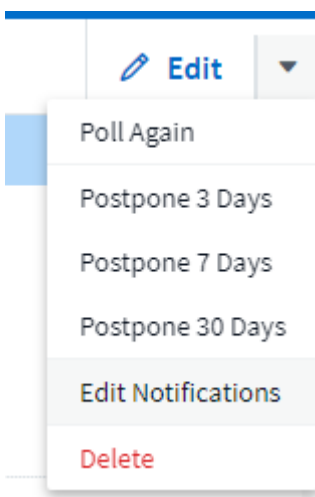
Você sempre pode substituir a lista de destinatários globais de um monitor individual ao criar ou modificar o monitor.



As notificações do ONTAP Data Collector têm precedência sobre quaisquer notificações específicas do Monitor que sejam relevantes para o cluster/coletor de dados. A lista de destinatários definida para o coletor de dados receberá os alertas do coletor de dados. Se não houver alertas ativos do coletor de dados, os alertas gerados pelo monitor serão enviados para destinatários específicos do monitor.

Editando notificações para ONTAP

Você pode modificar notificações para clusters do ONTAP selecionando *Editar notificações* na lista suspensa superior direita em uma página inicial do armazenamento.



A partir daqui, você pode definir notificações para alertas críticos, de aviso, informativos e/ou resolvidos. Cada cenário pode notificar a lista de destinatários globais ou outros destinatários que você escolher.

 By Email

Notify team on

Critical, Warn... ▾

Send to 

- Global Monitor Recipient List
- Other Email Recipients

email@email.one ✕

email2@email2.two ✕ |

Notify team on

Resolved ▾

Send to 

- Global Monitor Recipient List
- Other Email Recipients

 By Webhook

Enable webhook notification to add recipients

Monitores do sistema

O Data Infrastructure Insights inclui vários monitores definidos pelo sistema para métricas e logs. Os monitores do sistema disponíveis dependem dos coletores de dados presentes no local. Devido a isso, os monitores disponíveis no Data Infrastructure Insights podem mudar à medida que os coletores de dados são adicionados ou suas configurações alteradas.



Muitos monitores do sistema estão no estado *Pausado* por padrão. Você pode ativar um monitor de sistema selecionando a opção *Resume* para o monitor. Certifique-se de que *coleta avançada de dados de contador* e *enable ONTAP EMS log Collection* estão habilitados no coletor de dados. Essas opções podem ser encontradas no Coletor de dados do ONTAP em

 Enable ONTAP EMS log collection

Configuração Avançada: Opt in for Advanced Counter Data Collection rollout.

Descrições do monitor

Os monitores definidos pelo sistema são compostos por métricas e condições pré-definidas, bem como descrições padrão e ações corretivas, que não podem ser modificadas. Você *pode* modificar a lista de destinatários de notificação para monitores definidos pelo sistema. Para exibir as métricas, condições, descrição e ações corretivas ou modificar a lista de destinatários, abra um grupo de monitores definido pelo sistema e clique no nome do monitor na lista.

Os grupos de monitores definidos pelo sistema não podem ser modificados ou removidos.

Os seguintes monitores definidos pelo sistema estão disponíveis, nos grupos anotados.

- **A infraestrutura da ONTAP** inclui monitores para problemas relacionados à infraestrutura nos clusters do ONTAP.
- **Exemplos de carga de trabalho do ONTAP** inclui monitores para problemas relacionados à carga de trabalho.
- Os monitores em ambos os grupos são padrão para o estado *Pausado*.

Abaixo estão os monitores do sistema atualmente incluídos no Data Infrastructure Insights:

Monitores métricos

Nome do monitor	Gravidade	Descrição do monitor	Ação corretiva
-----------------	-----------	----------------------	----------------

<p>Utilização alta da porta do canal de fibra</p>	<p>CRÍTICO</p>	<p>As portas de protocolo Fibre Channel são usadas para receber e transferir o tráfego SAN entre o sistema host do cliente e os LUNs ONTAP. Se a utilização da porta for alta, ela se tornará um gargalo e, em última análise, afetará o desempenho de cargas de trabalho sensíveis do Protocolo de Canal de fibra. Um alerta indica que ações planejadas devem ser tomadas para equilibrar o tráfego de rede.... Um alerta crítico indica que a interrupção do serviço é iminente e medidas de emergência devem ser tomadas para equilibrar o tráfego da rede para garantir a continuidade do serviço.</p>	<p>Se o limite crítico for violado, considere ações imediatas para minimizar a interrupção do serviço:</p> <ol style="list-style-type: none"> 1. Mova workloads para outra porta FCP de baixa utilização. 2. Limite o tráfego de certos LUNs apenas ao trabalho essencial, seja por meio de políticas de QoS no ONTAP ou configuração do lado do host para aliviar a utilização das portas FCP. <p>Se o limite de aviso for violado, Planeje tomar as seguintes ações:</p> <ol style="list-style-type: none"> 1. Configure mais portas FCP para lidar com o tráfego de dados para que a utilização da porta seja distribuída entre mais portas. 2. Mova workloads para outra porta FCP de baixa utilização. 3. Limite o tráfego de certos LUNs apenas ao trabalho essencial, seja por meio de políticas de QoS no ONTAP ou configuração no lado do host para aliviar a utilização das portas FCP.
---	----------------	---	--

<p>Latência de LUN alta</p>	<p>CRÍTICO</p>	<p>LUNs são objetos que atendem ao tráfego de e/S geralmente orientados por aplicações sensíveis à performance, como bancos de dados. Altas latências de LUN significam que os próprios aplicativos podem sofrer e não podem realizar suas tarefas.... Um alerta de alerta indica que ações planejadas devem ser tomadas para mover o LUN para o nó ou agregado apropriado.... Um alerta crítico indica que a interrupção do serviço é iminente e medidas de emergência devem ser tomadas para garantir a continuidade do serviço. A seguir estão as latências esperadas com base no tipo de Mídia - SSD de até 1-2 milissegundos; SAS de até 8-10 milissegundos e HDD SATA de 17-20 milissegundos</p>	<p>Se o limite crítico for violado, considere as seguintes ações para minimizar a interrupção do serviço: Se o LUN ou seu volume tiver uma política de QoS associada a ele, avalie seus limites de limite e valide se eles estão fazendo com que a carga de trabalho LUN seja estrangulada. Se o limite de aviso for violado, Planeje tomar as seguintes ações: 1. Se o agregado também estiver tendo alta utilização, mova o LUN para outro agregado. 2. Se o nó também estiver com alta utilização, mova o volume para outro nó ou reduza o workload total do nó. 3. Se o LUN ou seu volume tiver uma política de QoS associada a ele, avalie seus limites de limite e valide se eles estão fazendo com que a carga de trabalho de LUN seja limitada.</p>
-----------------------------	----------------	--	---

<p>Alta utilização da porta de rede</p>	<p>CRÍTICO</p>	<p>As portas de rede são usadas para receber e transferir o tráfego de protocolos NFS, CIFS e iSCSI entre os sistemas host do cliente e os volumes ONTAP. Se a utilização da porta for alta, ela se tornará um gargalo e, em última análise, afetará o desempenho das cargas de trabalho NFS, CIFS e iSCSI.... Um alerta de aviso indica que ações planejadas devem ser tomadas para equilibrar o tráfego de rede.... Um alerta crítico indica que a interrupção do serviço é iminente e medidas de emergência devem ser tomadas para equilibrar o tráfego de rede para garantir a continuidade do serviço.</p>	<p>Se o limite crítico for violado, considere as seguintes ações imediatas para minimizar a interrupção do serviço: 1. Limite o tráfego de certos volumes apenas ao trabalho essencial, seja por meio de políticas de QoS no ONTAP ou análise do lado do host para diminuir a utilização das portas de rede. 2. Configure um ou mais volumes para usar outra porta de rede menos utilizada. Se o limite de aviso for violado, considere as seguintes ações imediatas: 1. Configure mais portas de rede para lidar com o tráfego de dados para que a utilização da porta seja distribuída entre mais portas. 2. Configure um ou mais volumes para usar outra porta de rede utilizada inferior.</p>
---	----------------	---	---

<p>Latência de namespace NVMe alta</p>	<p>CRÍTICO</p>	<p>Namespaces NVMe são objetos que atendem ao tráfego de e/S impulsionado por aplicações sensíveis à performance, como bancos de dados. Uma alta latência de namespaces NVMe significa que as próprias aplicações podem sofrer e não podem realizar suas tarefas.... Um alerta de aviso indica que ações planejadas devem ser tomadas para mover o LUN para o nó ou agregado apropriado.... Um alerta crítico indica que a interrupção do serviço é iminente e medidas de emergência devem ser tomadas para garantir a continuidade do serviço.</p>	<p>Se o limite crítico for violado, considere ações imediatas para minimizar a interrupção do serviço: Se o namespace do NVMe ou seu volume tiver uma política de QoS atribuída a eles, avalie seus limites de limite caso eles estejam fazendo com que o workload do namespace do NVMe seja estrangulado. Se o limite de aviso for violado, considere tomar as seguintes ações: 1. Se o agregado também estiver tendo alta utilização, mova o LUN para outro agregado. 2. Se o nó também estiver com alta utilização, mova o volume para outro nó ou reduza o workload total do nó. 3. Se o namespace do NVMe ou seu volume tiver uma política de QoS atribuída a eles, avalie seus limites de limite caso eles estejam fazendo com que o workload do namespace do NVMe seja estrangulado.</p>
--	----------------	---	---

QTree capacidade cheia	CRÍTICO	<p>Uma qtree é um sistema de arquivos logicamente definido que pode existir como um subdiretório especial do diretório raiz dentro de um volume. Cada qtree tem uma cota de espaço padrão ou uma cota definida por uma política de cota para limitar a quantidade de dados armazenados na árvore dentro da capacidade de volume.... Um alerta de alerta indica que a ação planejada deve ser tomada para aumentar o espaço.... Um alerta crítico indica que a interrupção do serviço é iminente e medidas de emergência devem ser tomadas para liberar espaço para garantir a continuidade do serviço.</p>	<p>Se o limite crítico for violado, considere ações imediatas para minimizar a interrupção do serviço:</p> <ol style="list-style-type: none"> 1. Aumentar o espaço da qtree para acomodar o crescimento. 2. Exclua dados indesejados para liberar espaço. <p>Se o limite de aviso for violado, Planeje tomar as seguintes ações imediatas:</p> <ol style="list-style-type: none"> 1. Aumentar o espaço da qtree para acomodar o crescimento. 2. Elimine dados indesejados para libertar espaço.
Limite rígido da capacidade do QTree	CRÍTICO	<p>Uma qtree é um sistema de arquivos logicamente definido que pode existir como um subdiretório especial do diretório raiz dentro de um volume. Cada qtree tem uma cota de espaço medida em KBytes que é usada para armazenar dados, a fim de controlar o crescimento de dados do usuário em volume e não exceder sua capacidade total.... Uma cota de capacidade de armazenamento suave que fornece alerta ao usuário proativamente antes de atingir o limite de cota de capacidade total na qtree e não ser mais capaz de armazenar dados. Monitorar a quantidade de dados armazenados em uma qtree garante que o usuário receba um serviço de dados ininterrupto.</p>	<p>Se o limite crítico for violado, considere as seguintes ações imediatas para minimizar a interrupção do serviço:</p> <ol style="list-style-type: none"> 1. Aumente a cota de espaço em árvore para acomodar o crescimento 2. Instrua o usuário a excluir dados indesejados na árvore para liberar espaço

<p>Limite macio da capacidade de QTree</p>	<p>AVISO</p>	<p>Uma qtree é um sistema de arquivos logicamente definido que pode existir como um subdiretório especial do diretório raiz dentro de um volume. Cada qtree tem uma cota de espaço medida em KBytes que pode ser usada para armazenar dados, a fim de controlar o crescimento de dados do usuário em volume e não exceder sua capacidade total... Uma qtree mantém uma cota de capacidade de armazenamento suave que fornece alerta ao usuário de forma proativa antes de atingir o limite de cota de capacidade total na qtree e não conseguir mais armazenar dados. Monitorar a quantidade de dados armazenados em uma qtree garante que o usuário receba um serviço de dados ininterrupto.</p>	<p>Se o limite de aviso for violado, considere as seguintes ações imediatas: 1. Aumente a cota de espaço em árvore para acomodar o crescimento. 2. Instrua o usuário a excluir dados indesejados na árvore para liberar espaço.</p>
<p>Limite rígido dos ficheiros QTree</p>	<p>CRÍTICO</p>	<p>Uma qtree é um sistema de arquivos logicamente definido que pode existir como um subdiretório especial do diretório raiz dentro de um volume. Cada qtree tem uma cota do número de arquivos que ele pode conter para manter um tamanho de sistema de arquivos gerenciável dentro do volume... Uma qtree mantém uma cota de número de arquivo rígido além da qual novos arquivos na árvore são negados. Monitorar o número de arquivos dentro de uma qtree garante que o usuário receba serviço de dados ininterrupto.</p>	<p>Se o limite crítico for violado, considere ações imediatas para minimizar a interrupção do serviço: 1. Aumente a cota de contagem de arquivos para a qtree. 2. Exclua arquivos indesejados do sistema de arquivos de qtree.</p>

<p>Limite suave dos ficheiros QTree</p>	<p>AVISO</p>	<p>Uma qtree é um sistema de arquivos logicamente definido que pode existir como um subdiretório especial do diretório raiz dentro de um volume. Cada qtree tem uma cota do número de arquivos que ele pode conter para manter um tamanho de sistema de arquivos gerenciável dentro do volume.... Uma qtree mantém uma cota de número de arquivo suave para fornecer alerta ao usuário de forma proativa antes de atingir o limite de arquivos na qtree e não conseguir armazenar arquivos adicionais. Monitorar o número de arquivos dentro de uma qtree garante que o usuário receba serviço de dados ininterrupto.</p>	<p>Se o limite de aviso for violado, Planeje tomar as seguintes ações imediatas: 1. Aumente a cota de contagem de arquivos para a qtree. 2. Exclua arquivos indesejados do sistema de arquivos de qtree.</p>
---	--------------	---	--

<p>Espaço de reserva instantâneo cheio</p>	<p>CRÍTICO</p>	<p>A capacidade de armazenamento de um volume é necessária para armazenar dados de aplicativos e clientes. Uma parte desse espaço, chamada de espaço reservado instantâneo, é usada para armazenar snapshots que permitem que os dados sejam protegidos localmente. Quanto mais dados novos e atualizados forem armazenados no volume ONTAP, mais capacidade de snapshot será usada e menos capacidade de storage snapshot estará disponível para dados novos ou atualizados futuros. Se a capacidade de dados do snapshot dentro de um volume atingir o espaço total de reserva do snapshot, isso pode levar o cliente a não conseguir armazenar novos dados do snapshot e a reduzir o nível de proteção dos dados no volume. O monitoramento do volume usado da capacidade do snapshot garante a continuidade dos serviços de dados.</p>	<p>Se o limite crítico for violado, considere ações imediatas para minimizar a interrupção do serviço:</p> <ol style="list-style-type: none"> 1. Configure instantâneos para usar o espaço de dados no volume quando a reserva de snapshot estiver cheia. 2. Elimine alguns instantâneos indesejados mais antigos para libertar espaço. <p>Se o limite de aviso for violado, Planeje tomar as seguintes ações imediatas:</p> <ol style="list-style-type: none"> 1. Aumente o espaço de reserva do snapshot dentro do volume para acomodar o crescimento. 2. Configure instantâneos para usar o espaço de dados no volume quando a reserva de snapshot estiver cheia.
--	----------------	--	--

<p>Limite de capacidade de armazenamento</p>	<p>CRÍTICO</p>	<p>Quando um pool de storage (agregado) está sendo enchido, as operações de e/S diminuem e, por fim, param de resultar em um incidente de interrupção do storage. Um alerta de aviso indica que a ação planejada deve ser tomada em breve para restaurar o espaço livre mínimo. Um alerta crítico indica que a interrupção do serviço é iminente e medidas de emergência devem ser tomadas para liberar espaço para garantir a continuidade do serviço.</p>	<p>Se o limite crítico for violado, considere imediatamente as seguintes ações para minimizar a interrupção do serviço: 1. Eliminar instantâneos em volumes não críticos. 2. Exclua volumes ou LUNs que são workloads não essenciais e que podem ser restaurados de cópias de armazenamento... se o limite de aviso for violado, Planeje as seguintes ações imediatas: 1. Mova um ou mais volumes para um local de armazenamento diferente. 2. Adicione mais capacidade de armazenamento. 3. Alterar as configurações de eficiência de storage ou categorizar dados inativos no storage de nuvem.</p>
--	----------------	---	---

<p>Limite de desempenho de storage</p>	<p>CRÍTICO</p>	<p>Quando um sistema de storage atinge seu limite de desempenho, as operações diminuem, a latência aumenta e os workloads e as aplicações podem começar a falhar. O ONTAP avalia a utilização do pool de armazenamento para cargas de trabalho e estima qual porcentagem de desempenho foi consumida.... Um alerta indica que deve ser tomada uma ação planejada para reduzir a carga do pool de armazenamento para garantir que haverá desempenho suficiente do pool de armazenamento deixado para os picos de carga de trabalho de serviço... Um alerta crítico indica que um brownout de desempenho é iminente e medidas de emergência devem ser tomadas para reduzir a carga do pool de armazenamento para garantir a fim de serviço.</p>	<p>Se o limite crítico for violado, considere as seguintes ações imediatas para minimizar a interrupção do serviço: 1. Suspender tarefas agendadas, como snapshots ou replicação do SnapMirror. 2. Cargas de trabalho não essenciais ociosas. Se o limite de aviso for violado, tome as seguintes ações imediatamente: 1. Mova um ou mais workloads para um local de storage diferente. 2. Adicionar mais nós de storage (AFF) ou compartimentos de disco (FAS) e redistribuir workloads 3. Alterar as características do workload (tamanho do bloco, armazenamento em cache do aplicativo).</p>
--	----------------	---	--

<p>Limite rígido da capacidade da quota do utilizador</p>	<p>CRÍTICO</p>	<p>O ONTAP reconhece os usuários de sistemas Unix ou Windows que têm os direitos de acessar volumes, arquivos ou diretórios dentro de um volume. Como resultado, o ONTAP permite que os clientes configurem a capacidade de armazenamento para seus usuários ou grupos de usuários de seus sistemas Linux ou Windows. A cota de política de usuário ou grupo limita a quantidade de espaço que o usuário pode utilizar para seus próprios dados.... Um limite rígido dessa cota permite a notificação do usuário quando a quantidade de capacidade usada dentro do volume é certa antes de atingir a cota de capacidade total. Monitorar a quantidade de dados armazenados dentro de uma cota de usuário ou grupo garante que o usuário receba um serviço de dados ininterrupto.</p>	<p>Se o limite crítico for violado, considere as seguintes ações imediatas para minimizar a interrupção do serviço: 1. Aumente o espaço da cota de usuário ou grupo para acomodar o crescimento. 2. Instrua o usuário ou grupo a excluir dados indesejados para liberar espaço.</p>
---	----------------	--	---

<p>Limite de capacidade da quota do utilizador</p>	<p>AVISO</p>	<p>O ONTAP reconhece os usuários de sistemas Unix ou Windows que têm os direitos de acessar volumes, arquivos ou diretórios dentro de um volume. Como resultado, o ONTAP permite que os clientes configurem a capacidade de armazenamento para seus usuários ou grupos de usuários de seus sistemas Linux ou Windows. A cota de política de usuário ou grupo limita a quantidade de espaço que o usuário pode utilizar para seus próprios dados.... Um limite suave dessa cota permite a notificação proativa ao usuário quando a quantidade de capacidade usada dentro do volume está atingindo a cota de capacidade total. Monitorar a quantidade de dados armazenados dentro de uma cota de usuário ou grupo garante que o usuário receba um serviço de dados ininterrupto.</p>	<p>Se o limite de aviso for violado, Planeje tomar as seguintes ações imediatas: 1. Aumente o espaço da cota de usuário ou grupo para acomodar o crescimento. 2. Elimine dados indesejados para libertar espaço.</p>
--	--------------	--	--

<p>Capacidade de volume cheia</p>	<p>CRÍTICO</p>	<p>A capacidade de armazenamento de um volume é necessária para armazenar dados de aplicativos e clientes. Quanto mais dados armazenados no volume ONTAP, menos disponibilidade de storage para dados futuros. Se a capacidade de armazenamento de dados dentro de um volume atingir a capacidade total de armazenamento pode levar o cliente a não conseguir armazenar dados devido à falta de capacidade de armazenamento. O monitoramento do volume usado de capacidade de armazenamento garante a continuidade dos serviços de dados.</p>	<p>Se o limite crítico for violado, considere as seguintes ações imediatas para minimizar a interrupção do serviço: 1. Aumente o espaço do volume para acomodar o crescimento. 2. Elimine dados indesejados para libertar espaço. 3. Se as cópias snapshot ocuparem mais espaço do que a reserva de snapshot, exclua snapshots antigos ou habilite o volume Snapshot Autodelete.. Se o limite de aviso for violado, Planeje executar as seguintes ações imediatas: 1. Aumentar o espaço do volume para acomodar o crescimento 2. Se as cópias snapshot ocuparem mais espaço do que a reserva de snapshot, exclua snapshots antigos ou ative o volume Snapshot Autodelete.</p>
-----------------------------------	----------------	---	---

<p>Limite de inodes de volume</p>	<p>CRÍTICO</p>	<p>Os volumes que armazenam arquivos usam nós de índice (inode) para armazenar metadados de arquivos. Quando um volume esgota sua alocação de inodes, não mais arquivos podem ser adicionados a ele.... Um alerta de alerta indica que a ação planejada deve ser tomada para aumentar o número de inodes disponíveis.... Um alerta crítico indica que a exaustão do limite do arquivo é iminente e medidas de emergência devem ser tomadas para liberar inodes para garantir a continuidade do serviço.</p>	<p>Se o limite crítico for violado, considere as seguintes ações imediatas para minimizar a interrupção do serviço: 1. Aumente o valor inodes para o volume. Se o valor inodes já estiver no valor máximo, divida o volume em dois ou mais volumes porque o sistema de arquivos cresceu além do tamanho máximo. 2. Use o FlexGroup, pois ajuda a acomodar grandes sistemas de arquivos. Se o limite de aviso for violado, Planeje tomar as seguintes ações imediatas: 1. Aumente o valor inodes para o volume. Se o valor inodes já estiver no máximo, divida o volume em dois ou mais volumes porque o sistema de arquivos cresceu além do tamanho máximo. 2. Use o FlexGroup, pois ajuda a acomodar grandes sistemas de arquivos</p>
-----------------------------------	----------------	---	--

Latência de volume alta	CRÍTICO	Os volumes são objetos que atendem ao tráfego de e/S geralmente orientados por aplicações sensíveis à performance, incluindo aplicações DevOps, diretórios base e bancos de dados. Com latências de alto volume, as próprias aplicações podem sofrer e não conseguir realizar suas tarefas. Monitorar latências de volume é essencial para manter a performance consistente com as aplicações. A seguir estão as latências esperadas com base no tipo de Mídia - SSD de até 1-2 milissegundos; SAS de até 8-10 milissegundos e HDD SATA de 17-20 milissegundos.	Se o limite crítico for violado, considere seguir ações imediatas para minimizar a interrupção do serviço: Se o volume tiver uma política de QoS atribuída a ele, avalie seus limites de limite caso eles estejam fazendo com que a carga de trabalho de volume seja limitada. Se o limite de aviso for violado, considere as seguintes ações imediatas: 1. Se o agregado também estiver tendo alta utilização, mova o volume para outro agregado. 2. Se o volume tiver uma política de QoS atribuída a ele, avalie seus limites de limite caso eles estejam fazendo com que o workload de volume seja estrangulado. 3. Se o nó também estiver com alta utilização, mova o volume para outro nó ou reduza o workload total do nó.
Nome do monitor	Gravidade	Descrição do monitor	Ação corretiva

Alta latência do nó	AVISO / CRÍTICO	<p>A latência do nó atingiu os níveis onde pode afetar o desempenho dos aplicativos no nó. A menor latência dos nós garante o desempenho consistente das aplicações. As latências esperadas com base no tipo de Mídia são: SSD de até 1-2 milissegundos; SAS de até 8-10 milissegundos e HDD SATA de 17-20 milissegundos.</p>	<p>Se o limite crítico for violado, ações imediatas devem ser tomadas para minimizar a interrupção do serviço: 1. Suspender tarefas agendadas, snapshots ou replicação do SnapMirror 2. Reduzir a demanda de workloads de prioridade mais baixa por meio dos limites de QoS 3. Inativar cargas de trabalho não essenciais considere ações imediatas quando o limite de aviso for violado: 1. Mova um ou mais workloads para um local de storage diferente 2. Reduzir a demanda de workloads de prioridade mais baixa por meio dos limites de QoS 3. Adicionar mais nós de storage (AFF) ou compartimentos de disco (FAS) e redistribuir workloads 4. Alterar as características da carga de trabalho (tamanho do bloco, armazenamento em cache do aplicativo, etc.)</p>
---------------------	-----------------	---	---

<p>Limite de desempenho do nó</p>	<p>AVISO / CRÍTICO</p>	<p>A utilização do desempenho do nó atingiu os níveis onde pode afetar o desempenho do iOS e dos aplicativos suportados pelo nó. A baixa utilização de performance de nós garante a performance consistente das aplicações.</p>	<p>Ações imediatas devem ser tomadas para minimizar a interrupção do serviço se o limite crítico for violado: 1. Suspender tarefas agendadas, snapshots ou replicação do SnapMirror 2. Reduzir a demanda de workloads de prioridade mais baixa por meio dos limites de QoS 3. Inativar cargas de trabalho não essenciais considere as seguintes ações se o limite de aviso for violado: 1. Mova um ou mais workloads para um local de storage diferente 2. Reduzir a demanda de workloads de prioridade mais baixa por meio dos limites de QoS 3. Adicionar mais nós de storage (AFF) ou shelves de disco (FAS) e redistribuir workloads 4. Alterar as características da carga de trabalho (tamanho do bloco, armazenamento em cache do aplicativo, etc.)</p>
-----------------------------------	------------------------	---	--

Storage VM alta latência	AVISO / CRÍTICO	<p>A latência da VM de storage (SVM) atingiu os níveis onde pode afetar a performance das aplicações na VM de storage. A menor latência da VM de storage garante a performance consistente das aplicações. As latências esperadas com base no tipo de Mídia são: SSD de até 1-2 milissegundos; SAS de até 8-10 milissegundos e HDD SATA de 17-20 milissegundos.</p>	<p>Se o limite crítico for violado, avalie imediatamente os limites de limite para volumes da VM de storage com uma política de QoS atribuída para verificar se eles estão fazendo com que os workloads de volume sejam estrangulados considere as seguintes ações imediatas quando o limite de aviso for violado:</p> <ol style="list-style-type: none"> 1. Se o agregado também estiver tendo alta utilização, mova alguns volumes da VM de storage para outro agregado. 2. No caso de volumes da VM de storage com uma política de QoS atribuída, avalie os limites de limite se eles estiverem fazendo com que os workloads de volume sejam 3 estrangulados. Se o nó estiver com alta utilização, mova alguns volumes da VM de storage para outro nó ou reduza o workload total do nó
Limite rígido dos ficheiros de quota de utilizador	CRÍTICO	<p>O número de arquivos criados dentro do volume atingiu o limite crítico e arquivos adicionais não podem ser criados. Monitorar o número de arquivos armazenados garante que o usuário receba serviço de dados ininterrupto.</p>	<p>Ações imediatas são necessárias para minimizar a interrupção do serviço se o limite crítico for violado. Considere tomar as seguintes ações:</p> <ol style="list-style-type: none"> 1. Aumente a cota de contagem de arquivos para o usuário específico 2. Exclua arquivos indesejados para reduzir a pressão na cota de arquivos para o usuário específico

<p>Limite de software dos ficheiros de quota do utilizador</p>	<p>AVISO</p>	<p>O número de arquivos criados dentro do volume atingiu o limite da cota e está próximo ao limite crítico. Você não pode criar arquivos adicionais se a cota atingir o limite crítico. Monitorar o número de arquivos armazenados por um usuário garante que o usuário receba serviço de dados ininterrupto.</p>	<p>Considere ações imediatas se o limite de aviso for violado: 1. Aumente a cota de contagem de arquivos para a cota de usuário específica 2. Exclua arquivos indesejados para reduzir a pressão na cota de arquivos para o usuário específico</p>
<p>Taxa de perda de cache de volume</p>	<p>AVISO / CRÍTICO</p>	<p>A taxa de perda de cache de volume é a porcentagem de solicitações de leitura dos aplicativos clientes que são retornados do disco em vez de serem retornados do cache. Isto significa que o volume atingiu o limite definido.</p>	<p>Se o limite crítico for violado, ações imediatas devem ser tomadas para minimizar a interrupção do serviço: 1. Mova alguns workloads para fora do nó do volume para reduzir a carga de e/S 2. Se ainda não estiver no nó do volume, aumente o cache WAFL comprando e adicionando um cache Flash 3. Reduzir a demanda de workloads de prioridade mais baixa no mesmo nó por limites de QoS considere ações imediatas quando o limite de aviso for violado: 1. Mova alguns workloads para fora do nó do volume para reduzir a carga de e/S 2. Se ainda não estiver no nó do volume, aumente o cache WAFL comprando e adicionando um cache Flash 3. Reduzir a demanda de workloads de prioridade mais baixa no mesmo nó por meio dos limites de QoS 4. Alterar as características da carga de trabalho (tamanho do bloco, armazenamento em cache do aplicativo, etc.)</p>

Volume Qtree quota comprometer em excesso	AVISO / CRÍTICO	Volume Qtree quota comprometer especifica a porcentagem em que um volume é considerado sobrecarregado pelas cotas de qtree. O limite definido para a cota de qtree é atingido para o volume. O monitoramento do volume de cota de qtree em excesso garante que o usuário receba um serviço de dados ininterrupto.	Se o limite crítico for violado, ações imediatas devem ser tomadas para minimizar a interrupção do serviço: 1. Aumente o espaço do volume 2. Exclua dados indesejados quando o limite de aviso é violado e considere aumentar o espaço do volume.
---	-----------------	---	---

[Voltar ao topo](#)

Monitores de registro

Nome do monitor	Gravidade	Descrição	Ação corretiva
Credenciais da AWS não inicializadas	INFORMAÇÕES	Esse evento ocorre quando um módulo tenta acessar credenciais baseadas em função do Amazon Web Services (AWS) Identity and Access Management (IAM) a partir do thread de credenciais da nuvem antes de serem inicializadas.	Aguarde que o thread de credenciais de nuvem, bem como o sistema, conclua a inicialização.

Nível de nuvem inaccessível	CRÍTICO	Um nó de storage não pode se conectar à API de armazenamento de objetos do Cloud Tier. Alguns dados ficarão inaccessíveis.	Se você usar produtos locais, execute as seguintes ações corretivas:... Verifique se o seu LIF está on-line e funcional usando o comando "network interface show".. Verifique a conectividade de rede com o servidor de armazenamento de objetos usando o comando "ping" sobre o nó de destino LIF entre clusters NetApp. Se você usar o Cloud Volumes ONTAP, execute as seguintes ações corretivas:... Certifique-se de que a configuração do seu armazenamento de objetos não foi alterada. Verifique se as informações de login e conectividade ainda são válidas. Contate o suporte técnico da NetApp se o problema persistir.
Disco fora de serviço	INFORMAÇÕES	Esse evento ocorre quando um disco é removido do serviço porque foi marcado como com falha, está sendo higienizado ou entrou no Centro de Manutenção.	Nenhum.
FlexGroup Constituinte completo	CRÍTICO	Um componente dentro de um volume FlexGroup está cheio, o que pode causar uma possível interrupção do serviço. Você ainda pode criar ou expandir arquivos no volume FlexGroup. No entanto, nenhum dos arquivos armazenados no componente pode ser modificado. Como resultado, você pode ver erros aleatórios fora do espaço quando você tenta executar operações de gravação no volume FlexGroup.	Recomenda-se que você adicione capacidade ao volume FlexGroup usando o comando "volume modificar -arquivos -X". Alternativamente, exclua arquivos do volume FlexGroup. No entanto, é difícil determinar quais arquivos aterraram no constituinte.

FlexGroup Constituinte quase cheio	AVISO	Um componente dentro de um volume FlexGroup está quase fora do espaço, o que pode causar uma possível interrupção do serviço. Os arquivos podem ser criados e expandidos. No entanto, se o constituinte ficar sem espaço, você pode não ser capaz de anexar ou modificar os arquivos no constituinte.	Recomenda-se que você adicione capacidade ao volume FlexGroup usando o comando "volume modificar -arquivos -X". Alternativamente, exclua arquivos do volume FlexGroup. No entanto, é difícil determinar quais arquivos aterraram no constituinte.
FlexGroup Constituinte quase fora de inodes	AVISO	Um constituinte dentro de um volume FlexGroup está quase fora de inodes, o que pode causar uma possível interrupção do serviço. O constituinte recebe solicitações de criação menores do que a média. Isso pode afetar o desempenho geral do volume FlexGroup, porque as solicitações são roteadas para componentes com mais inodes.	Recomenda-se que você adicione capacidade ao volume FlexGroup usando o comando "volume modificar -arquivos -X". Alternativamente, exclua arquivos do volume FlexGroup. No entanto, é difícil determinar quais arquivos aterraram no constituinte.
FlexGroup Constituinte fora de inodes	CRÍTICO	Um componente de um volume FlexGroup ficou sem inodes, o que pode causar uma possível interrupção do serviço. Você não pode criar novos arquivos neste constituinte. Isso pode levar a uma distribuição global desequilibrada de conteúdo pelo volume FlexGroup.	Recomenda-se que você adicione capacidade ao volume FlexGroup usando o comando "volume modificar -arquivos -X". Alternativamente, exclua arquivos do volume FlexGroup. No entanto, é difícil determinar quais arquivos aterraram no constituinte.
LUN Offline	INFORMAÇÕES	Este evento ocorre quando um LUN é colocado offline manualmente.	Coloque o LUN novamente online.

Falha na ventoinha da unidade principal	AVISO	Uma ou mais ventoinhas da unidade principal falharam. No entanto, se a condição persistir por muito tempo, a temperatura excessiva pode desencadear um desligamento automático.	Recoloque os ventiladores com falha. Se o erro persistir, substitua-os.
Ventoinha da unidade principal no estado de aviso	INFORMAÇÕES	Este evento ocorre quando uma ou mais ventoinhas da unidade principal estão num estado de aviso.	Substitua as ventoinhas indicadas para evitar o sobreaquecimento.
Bateria do NVRAM fraca	AVISO	A capacidade da bateria do NVRAM é extremamente baixa. Pode haver uma perda de dados potencial se a bateria ficar sem energia.... seu sistema gera e transmite uma mensagem AutoSupport ou "chamar para casa" para o suporte técnico da NetApp e os destinos configurados se estiver configurado para fazê-lo. A entrega bem-sucedida de uma mensagem AutoSupport melhora significativamente a determinação e resolução de problemas.	Execute as seguintes ações corretivas:... Veja o estado atual da bateria, a capacidade e o estado de carregamento usando o comando "show dos sensores de ambiente do nó do sistema".... se a bateria foi substituída recentemente ou o sistema não estava operacional por um longo período de tempo, monitore a bateria para verificar se está carregando corretamente NetApp.

<p>Processador de serviço não configurado</p>	<p>AVISO</p>	<p>Este evento ocorre semanalmente, para lembrá-lo de configurar o processador de serviço (SP). O SP é um dispositivo físico incorporado ao seu sistema para fornecer acesso remoto e recursos de gerenciamento remoto. Você deve configurar o SP para usar toda a sua funcionalidade.</p>	<p>Execute as seguintes ações corretivas:... Configurar o SP usando o comando "system Service-processor network modify". .. Opcionalmente, obtenha o endereço MAC do SP usando o comando "system Service-processor network show". .. Verifique a configuração da rede do SP usando o comando "system Service-processor network show". .. Verifique se o SP pode enviar um e-mail do AutoSupport usando o comando "System Service-processor AutoSupport invoke". OBSERVAÇÃO: Os hosts e destinatários de e-mail do AutoSupport devem ser configurados no ONTAP antes de emitir este comando.</p>
<p>Processador de serviço offline</p>	<p>CRÍTICO</p>	<p>O ONTAP não está mais recebendo batimentos cardíacos do processador de Serviço (SP), mesmo que todas as ações de recuperação do SP tenham sido tomadas. O ONTAP não pode monitorar a integridade do hardware sem o SP.... o sistema será desligado para evitar danos ao hardware e perda de dados. Configure um alerta de pânico para ser notificado imediatamente se o SP ficar offline.</p>	<p>Desligue o sistema executando as seguintes ações:... puxe o controlador para fora do chassi.... empurre o controlador novamente para dentro.... ligue o controlador novamente.... se o problema persistir, substitua o módulo do controlador.</p>

Falha nas ventoinhas da prateleira	CRÍTICO	A ventoinha de arrefecimento indicada ou o módulo do ventilador da prateleira falhou. Os discos na gaveta podem não receber fluxo de ar de resfriamento suficiente, o que pode resultar em falha de disco.	Execute as seguintes ações corretivas:... Verifique se o módulo da ventoinha está totalmente encaixado e fixo. NOTA: O ventilador está integrado ao módulo de fonte de alimentação em algumas prateleiras de disco.... se o problema persistir, substitua o módulo do ventilador.... se o problema persistir, entre em Contato com o suporte técnico da NetApp para obter assistência.
O sistema não pode operar devido a falha do ventilador da Unidade Principal	CRÍTICO	Uma ou mais ventoinhas da unidade principal falharam, interrompendo o funcionamento do sistema. Isso pode levar a uma possível perda de dados.	Substitua as ventoinhas com falha.
Discos não atribuídos	INFORMAÇÕES	O sistema tem discos não atribuídos - a capacidade está sendo desperdiçada e seu sistema pode ter alguma configuração incorreta ou alteração parcial de configuração aplicada.	Execute as seguintes ações corretivas: Determine quais discos não são atribuídos usando o comando "Disk show -n". Atribua os discos a um sistema usando o comando "Disk Assign".
Servidor antivírus ocupado	AVISO	O servidor antivírus está ocupado demais para aceitar novas solicitações de verificação.	Se essa mensagem ocorrer com frequência, verifique se há servidores antivírus suficientes para lidar com a carga de verificação de vírus gerada pelo SVM.

Credenciais da AWS para a função do IAM expiradas	CRÍTICO	O Cloud volume ONTAP tornou-se inacessível. As credenciais baseadas em função do Identity and Access Management (IAM) expiraram. As credenciais são adquiridas do servidor de metadados da Amazon Web Services (AWS) usando a função IAM e são usadas para assinar solicitações de API para o Amazon Simple Storage Service (Amazon S3).	Execute o seguinte:... Faça login no Console de Gerenciamento do AWS EC2. Navegue até a página instâncias.. Localize a instância para a implantação do Cloud Volumes ONTAP e verifique sua integridade. Verifique se a função do AWS IAM associada à instância é válida e recebeu Privileges adequado para a instância.
Credenciais da AWS para função do IAM não encontrada	CRÍTICO	O thread de credenciais de nuvem não pode adquirir as credenciais baseadas em função do Amazon Web Services (AWS) Identity and Access Management (IAM) do servidor de metadados da AWS. As credenciais são usadas para assinar solicitações de API para o Amazon Simple Storage Service (Amazon S3). O Cloud volume ONTAP tornou-se inacessível.	Execute o seguinte:... Faça login no Console de Gerenciamento do AWS EC2. Navegue até a página instâncias.. Localize a instância para a implantação do Cloud Volumes ONTAP e verifique sua integridade. Verifique se a função do AWS IAM associada à instância é válida e recebeu Privileges adequado para a instância.
Credenciais da AWS para função do IAM não válidas	CRÍTICO	As credenciais baseadas em função do Identity and Access Management (IAM) não são válidas. As credenciais são adquiridas do servidor de metadados da Amazon Web Services (AWS) usando a função IAM e são usadas para assinar solicitações de API para o Amazon Simple Storage Service (Amazon S3). O Cloud volume ONTAP tornou-se inacessível.	Execute o seguinte:... Faça login no Console de Gerenciamento do AWS EC2. Navegue até a página instâncias.. Localize a instância para a implantação do Cloud Volumes ONTAP e verifique sua integridade. Verifique se a função do AWS IAM associada à instância é válida e recebeu Privileges adequado para a instância.

Função do AWS IAM não encontrada	CRÍTICO	O thread de funções de gerenciamento de identidade e acesso (IAM) não consegue localizar uma função IAM do Amazon Web Services (AWS) no servidor de metadados da AWS. A função IAM é necessária para adquirir credenciais baseadas em funções usadas para assinar solicitações de API ao Amazon Simple Storage Service (Amazon S3). O Cloud volume ONTAP tornou-se inacessível.	Execute o seguinte:... entre no Console de Gerenciamento do AWS EC2. Navegue até a página instâncias.. Localize a instância para a implantação do Cloud Volumes ONTAP e verifique sua integridade. Verifique se a função do AWS IAM associada à instância é válida.
Função do AWS IAM não válida	CRÍTICO	A função do Amazon Web Services (AWS) Identity and Access Management (IAM) no servidor de metadados da AWS não é válida. O Cloud volume ONTAP tornou-se inacessível.	Execute o seguinte:... Faça login no Console de Gerenciamento do AWS EC2. Navegue até a página instâncias.. Localize a instância para a implantação do Cloud Volumes ONTAP e verifique sua integridade. Verifique se a função do AWS IAM associada à instância é válida e recebeu Privileges adequado para a instância.
Falha na conexão do servidor de metadados da AWS	CRÍTICO	O thread de funções de gerenciamento de identidade e acesso (IAM) não pode estabelecer um link de comunicação com o servidor de metadados da Amazon Web Services (AWS). A comunicação deve ser estabelecida para adquirir as credenciais baseadas em função do AWS IAM necessárias usadas para assinar solicitações de API ao Amazon Simple Storage Service (Amazon S3). O Cloud volume ONTAP tornou-se inacessível.	Execute o seguinte:... entre no Console de Gerenciamento do AWS EC2. Navegue até a página instâncias.. Localize a instância para a implantação do Cloud Volumes ONTAP e verifique sua integridade.

<p>Limite de uso do espaço FabricPool quase atingido</p>	<p>AVISO</p>	<p>O uso total de espaço FabricPool em todo o cluster de armazenamentos de objetos de fornecedores licenciados em capacidade quase atingiu o limite licenciado.</p>	<p>Execute as seguintes ações corretivas:...</p> <p>Verifique a porcentagem da capacidade licenciada usada por cada camada de storage do FabricPool usando o comando "storage agregado object-store show-space". ..</p> <p>Exclua cópias Snapshot de volumes com a política de disposição em camadas "snapshot" ou "backup" usando o comando "volume snapshot delete" para limpar espaço. ..</p> <p>Instale uma nova licença no cluster para aumentar a capacidade licenciada.</p>
<p>Limite de utilização do espaço FabricPool atingido</p>	<p>CRÍTICO</p>	<p>O uso total de espaço FabricPool em todo o cluster de armazenamentos de objetos de fornecedores licenciados em capacidade atingiu o limite de licença.</p>	<p>Execute as seguintes ações corretivas:...</p> <p>Verifique a porcentagem da capacidade licenciada usada por cada camada de storage do FabricPool usando o comando "storage agregado object-store show-space". ..</p> <p>Exclua cópias Snapshot de volumes com a política de disposição em camadas "snapshot" ou "backup" usando o comando "volume snapshot delete" para limpar espaço. ..</p> <p>Instale uma nova licença no cluster para aumentar a capacidade licenciada.</p>

<p>Falha de reembolso de agregado</p>	<p>CRÍTICO</p>	<p>Esse evento ocorre durante a migração de um agregado como parte de um failover de armazenamento (SFO), quando o nó de destino não pode alcançar os armazenamentos de objetos.</p>	<p>Execute as seguintes ações corretivas:...</p> <p>Verifique se o LIF entre clusters está on-line e funcional usando o comando "network interface show". ..</p> <p>Verifique a conectividade de rede com o servidor de armazenamento de objetos usando o comando "ping" sobre o LIF do nó de destino. ...</p> <p>Verifique se a configuração do seu armazenamento de objetos não foi alterada e que as informações de login e conectividade ainda são precisas usando o comando "agreed object-store config show"..</p> <p>Alternativamente, você pode substituir o erro especificando false para o parâmetro "require-Partner-waiting" do comando giveback NetApp.</p>
---------------------------------------	----------------	--	--

<p>Interconexão HA desativada</p>	<p>AVISO</p>	<p>A interconexão de alta disponibilidade (HA) está inativa. Risco de interrupção de serviço quando o failover não está disponível.</p>	<p>As ações corretivas dependem do número e do tipo de links de interconexão de HA suportados pela plataforma, bem como do motivo pelo qual a interconexão está inativa. ... Se os links estiverem inativos:... verifique se ambos os controladores no par HA estão operacionais... Para links conectados externamente, certifique-se de que os cabos de interconexão estão conectados corretamente e que os SFPs (Small Form-factor Pluggables), se aplicável, estão encaixados corretamente em ambos os controladores.. ...Se os links estiverem desativados, ative os links usando o comando "ic link on". ...Se um par não estiver conectado, desative e reative os links, um após o outro, usando os comandos "ic link off" e "ic link on". Entre em Contato com o suporte técnico da NetApp se o problema persistir.</p>
-----------------------------------	--------------	---	--

<p>Máximo de sessões por utilizador excedido</p>	<p>AVISO</p>	<p>Você excedeu o número máximo de sessões permitidas por usuário em uma conexão TCP. Qualquer solicitação para estabelecer uma sessão será negada até que algumas sessões sejam liberadas. ...</p>	<p>Execute as seguintes ações corretivas:... Inspeccione todos os aplicativos que são executados no cliente e termine qualquer um que não esteja funcionando corretamente.... reinicie o cliente.... Verifique se o problema é causado por um aplicativo novo ou existente:... se o aplicativo é novo, defina um limite mais alto para o cliente usando o comando "cifs Option Modify -Max -abre-same-file-per-tree". Em alguns casos, os clientes operam como esperado, mas exigem um limite mais alto. Você deve ter privilégios avançados para definir um limite mais alto para o cliente. ...Se o problema for causado por um aplicativo existente, pode haver um problema com o cliente. Entre em Contato com o suporte técnico da NetApp para obter mais informações ou assistência.</p>
--	--------------	---	---

<p>Máximo de vezes aberto por ficheiro excedido</p>	<p>AVISO</p>	<p>Excedeu o número máximo de vezes que pode abrir o ficheiro através de uma ligação TCP. Qualquer solicitação para abrir esse arquivo será negada até que você feche algumas instâncias abertas do arquivo. Isso normalmente indica comportamento anormal da aplicação.</p>	<p>Execute as seguintes ações corretivas:...</p> <p>Inspecione os aplicativos que são executados no cliente usando essa conexão TCP. O cliente pode estar operando incorretamente por causa do aplicativo em execução nele.... reinicie o cliente...</p> <p>. Verifique se o problema é causado por um aplicativo novo ou existente:... se o aplicativo é novo, defina um limite mais alto para o cliente usando o comando "cifs option modify -Max -abre-same-file-per-tree". Em alguns casos, os clientes operam como esperado, mas exigem um limite mais alto. Você deve ter privilégios avançados para definir um limite mais alto para o cliente. ...Se o problema for causado por um aplicativo existente, pode haver um problema com o cliente. Entre em Contato com o suporte técnico da NetApp para obter mais informações ou assistência.</p>
---	--------------	--	---

<p>Conflito de nomes NetBIOS</p>	<p>CRÍTICO</p>	<p>O serviço de nomes NetBIOS recebeu uma resposta negativa a uma solicitação de Registro de nomes de uma máquina remota. Isso geralmente é causado por um conflito no nome NetBIOS ou um alias. Como resultado, os clientes podem não conseguir acessar dados ou se conectar ao nó certo de fornecimento de dados no cluster.</p>	<p>Execute qualquer uma das seguintes ações corretivas:... se houver um conflito no nome NetBIOS ou um alias, execute uma das seguintes ações:... Excluir o alias NetBIOS duplicado usando o comando "vserver delete -aliases alias -vserver vserver vserver". ...Se não houver aliases configurados e houver um conflito no nome NetBIOS, renomeie o servidor CIFS usando os comandos "vserver cifs delete -vserver vserver" e "vserver CIFS create -cifs -server netbiosname". OBSERVAÇÃO: Excluir um servidor CIFS pode tornar os dados inacessíveis. ...Remova o nome NetBIOS ou renomeie o NetBIOS na máquina remota.</p>
<p>NFSv4 Store Pool esgotado</p>	<p>CRÍTICO</p>	<p>Uma piscina de loja NFSv4 foi esgotada.</p>	<p>Se o servidor NFS não responder por mais de 10 minutos após este evento, entre em Contato com o suporte técnico da NetApp.</p>
<p>Nenhum motor de digitalização registrado</p>	<p>CRÍTICO</p>	<p>O conector antivírus notificou o ONTAP de que ele não possui um mecanismo de verificação registrado. Isso pode causar indisponibilidade de dados se a opção "Scan-mandatory" (digitalização obrigatória) estiver ativada.</p>	<p>Execute as seguintes ações corretivas:... Certifique-se de que o software do mecanismo de verificação instalado no servidor antivírus é compatível com o ONTAP.... Certifique-se de que o software do mecanismo de verificação está em execução e configurado para se conectar ao conector antivírus por meio de loopback local.</p>

Sem ligação Vscan	CRÍTICO	O ONTAP não tem uma ligação Vscan a pedidos de verificação de vírus de serviço. Isso pode causar indisponibilidade de dados se a opção "Scan-mandatory" (digitalização obrigatória) estiver ativada.	Certifique-se de que o conjunto do scanner está configurado corretamente e que os servidores antivírus estão ativos e conetados ao ONTAP.
Espaço de volume de raiz do nó baixo	CRÍTICO	O sistema detetou que o volume raiz está perigosamente baixo no espaço. O nó não está totalmente operacional. As LIFs de dados podem ter falhado no cluster, por causa do qual o acesso NFS e CIFS é limitado no nó. A capacidade administrativa está limitada aos procedimentos de recuperação locais para que o nó limpe o espaço no volume raiz.	Execute as seguintes ações corretivas:... limpe o espaço no volume raiz excluindo cópias Snapshot antigas, excluindo arquivos que você não precisa mais do diretório /mroot ou expandindo a capacidade do volume raiz.... reinicie o controlador....entre em Contato com o suporte técnico da NetApp para obter mais informações ou assistência.
Compartilhamento Admin inexistente	CRÍTICO	Problema Vscan: Um cliente tentou se conetar a um compartilhamento inexistente do ONTAP_ADMIN.	Certifique-se de que o Vscan esteja habilitado para o ID SVM mencionado. Ativar o Vscan em um SVM faz com que o compartilhamento ONTAP_ADMIN seja criado automaticamente para o SVM.
Namespace NVMe fora do espaço	CRÍTICO	Um namespace NVMe foi colocado off-line devido a uma falha de gravação causada pela falta de espaço.	Adicione espaço ao volume e, em seguida, coloque o namespace NVMe on-line usando o comando "vserver nvme namespace modify".

Período de carência NVMe-of Ativo	AVISO	Esse evento ocorre diariamente quando o protocolo NVMe sobre Fabrics (NVMe-of) está em uso e o período de carência da licença está ativo. O recurso NVMe-of requer uma licença após o período de carência da licença expirar. O recurso NVMe-of é desativado quando o período de carência da licença terminar.	Entre em Contato com seu representante de vendas para obter uma licença NVMe-of e adicioná-la ao cluster ou remover todas as instâncias de configuração NVMe-of do cluster.
O período de carência do NVMe-of expirou	AVISO	O período de carência da licença NVMe over Fabrics (NVMe-of) acabou e o recurso NVMe-of é desativado.	Entre em Contato com seu representante de vendas para obter uma licença NVMe-of e adicioná-la ao cluster.
Início do período de carência do NVMe-of	AVISO	A configuração NVMe over Fabrics (NVMe-of) foi detetada durante a atualização para o software ONTAP 9.5. O recurso NVMe-of requer uma licença após o período de carência da licença expirar.	Entre em Contato com seu representante de vendas para obter uma licença NVMe-of e adicioná-la ao cluster.
Host de armazenamento de objetos não resolvível	CRÍTICO	O nome do host do servidor de armazenamento de objetos não pode ser resolvido para um endereço IP. O cliente de armazenamento de objetos não pode se comunicar com o servidor de armazenamento de objetos sem resolver um endereço IP. Como resultado, os dados podem estar inacessíveis.	Verifique a configuração DNS para verificar se o nome do host está configurado corretamente com um endereço IP.

Object Store Intercluster LIF para baixo	CRÍTICO	O cliente de armazenamento de objetos não consegue encontrar um LIF operacional para se comunicar com o servidor de armazenamento de objetos. O nó não permitirá o tráfego do cliente de armazenamento de objetos até que o LIF entre clusters esteja operacional. Como resultado, os dados podem estar inacessíveis.	Execute as seguintes ações corretivas:... Verifique o status de clusters de LIF usando o comando "network interface show -role"... Verifique se o LIF entre clusters está configurado corretamente e operacional.... se um LIF entre clusters não estiver configurado, adicione-o usando o comando "network interface create -role".
Incompatibilidade de assinatura do armazenamento de objetos	CRÍTICO	A assinatura de solicitação enviada ao servidor de armazenamento de objetos não corresponde à assinatura calculada pelo cliente. Como resultado, os dados podem estar inacessíveis.	Verifique se a chave de acesso secreto está configurada corretamente. Se estiver configurado corretamente, contacte o suporte técnico da NetApp para obter assistência.
Tempo limite READDIR	CRÍTICO	Uma operação de ARQUIVO READDIR excedeu o tempo limite que é permitido executar no WAFL. Isso pode ser por causa de diretórios muito grandes ou esparsos. Recomenda-se a ação corretiva.	Execute as seguintes ações corretivas:... Encontre informações específicas para diretórios recentes que tiveram operações de arquivo READDIR expiram usando o seguinte comando 'dag' privilegiar nodeshell CLI: WAFL readdir notice show.... Verifique se os diretórios são indicados como esparsos ou não:... se um diretório é indicado como esparsos, é recomendado que você copie o conteúdo do diretório para um novo para remover a frouxidão do diretório. ... Se um diretório não for indicado como esparsos e o diretório for grande, é recomendável que você reduza o tamanho do arquivo de diretório reduzindo o número de entradas de arquivo no diretório.

Falha na realocação do agregado	CRÍTICO	Esse evento ocorre durante a realocação de um agregado, quando o nó de destino não pode alcançar os armazenamentos de objetos.	<p>Execute as seguintes ações corretivas:...</p> <p>Verifique se o LIF entre clusters está on-line e funcional usando o comando "network interface show". ..</p> <p>Verifique a conectividade de rede com o servidor de armazenamento de objetos usando o comando "ping" sobre o LIF do nó de destino. ...</p> <p>Verifique se a configuração do seu armazenamento de objetos não foi alterada e se as informações de login e conectividade ainda são precisas usando o comando "Aggregate object-store config show". ..</p> <p>Alternativamente, você pode substituir o erro usando o parâmetro "override-destination-checks" do comando relocation. ..</p> <p>Entre em Contato com o suporte técnico da NetApp para obter mais informações ou assistência.</p>
Cópia sombra falhou	CRÍTICO	Um serviço de cópia de sombra de volume (VSS), uma operação de serviço de backup e restauração do Microsoft Server, falhou.	<p>Verifique o seguinte usando as informações fornecidas na mensagem de evento:...</p> <p>a configuração de cópia de sombra está ativada?...</p> <p>as licenças apropriadas estão instaladas? Em que compartilhamentos é realizada a operação de cópia sombra?...</p> <p>o nome da ação está correto?...</p> <p>o caminho da ação existe?...</p> <p>quais são os estados do conjunto de cópias sombra e suas cópias de sombra?</p>

Falha nas fontes de alimentação do interruptor de armazenamento	AVISO	Existe uma fonte de alimentação em falta no interruptor do painel de instrumentos. A redundância é reduzida, o risco de interrupção com quaisquer outras falhas de energia.	Execute as seguintes ações corretivas:... Certifique-se de que a rede elétrica da fonte de alimentação, que fornece energia ao switch do cluster, esteja ligada.... Certifique-se de que o cabo de alimentação está conectado à fonte de alimentação. Contate o suporte técnico da NetApp se o problema persistir.
Demasiadas Autenticação CIFS	AVISO	Muitas negociações de autenticação ocorreram simultaneamente. Existem 256 solicitações de nova sessão incompletas deste cliente.	Investigue por que o cliente criou 256 ou mais solicitações de conexão novas. Você pode ter que entrar em Contato com o fornecedor do cliente ou do aplicativo para determinar por que o erro ocorreu.
Acesso não autorizado ao Admin Share	AVISO	Um cliente tentou se conectar ao compartilhamento privilegiado do ONTAP_ADMIN, mesmo que seu usuário conectado não seja um usuário permitido.	Execute as seguintes ações corretivas:... Certifique-se de que o nome de usuário e o endereço IP mencionados estão configurados em um dos pools de scanner Vscan ativos. .. Verifique a configuração do pool de scanner que está atualmente ativa usando o comando "vserver vscan pool show-active".
Vírus detetado	AVISO	Um servidor Vscan comunicou um erro ao sistema de armazenamento. Isso normalmente indica que um vírus foi encontrado. No entanto, outros erros no servidor Vscan podem causar esse evento.... o acesso do cliente ao arquivo é negado. O servidor Vscan pode, dependendo de suas configurações e configurações, limpar o arquivo, colocá-lo em quarentena ou excluí-lo.	Verifique o log do servidor Vscan relatado no evento "syslog" para ver se ele foi capaz de limpar, colocar em quarentena ou excluir o arquivo infectado com sucesso. Se não conseguir fazê-lo, um administrador de sistema poderá ter de eliminar manualmente o ficheiro.

Volume off-line	INFORMAÇÕES	Esta mensagem indica que um volume está offline.	Traga o volume de volta online.
Volume restrito	INFORMAÇÕES	Este evento indica que um volume flexível é restringido.	Traga o volume de volta online.
Parada da VM de armazenamento bem-sucedida	INFORMAÇÕES	Esta mensagem ocorre quando uma operação 'vserver stop' é bem-sucedida.	Use o comando 'vserver start' para iniciar o acesso a dados em uma VM de armazenamento.
Pânico de nó	AVISO	Este evento é emitido quando ocorre um pânico	Entre em Contato com o suporte ao cliente da NetApp.

[Voltar ao topo](#)

Monitores de log anti-ransomware

Nome do monitor	Gravidade	Descrição	Ação corretiva
Monitoramento anti-ransomware de storage VM desativado	AVISO	O monitoramento anti-ransomware da VM de storage é desativado. Habilite o anti-ransomware para proteger a VM de storage.	Nenhum
Monitoramento anti-ransomware da VM de storage ativado (modo de aprendizado)	INFORMAÇÕES	O monitoramento anti-ransomware da VM de storage é ativado no modo de aprendizado.	Nenhum
Monitoramento de volume Anti-ransomware habilitado	INFORMAÇÕES	O monitoramento anti-ransomware do volume está ativado.	Nenhum
Monitoramento de volume Anti-ransomware desativado	AVISO	O monitoramento anti-ransomware do volume está desativado. Habilite o anti-ransomware para proteger o volume.	Nenhum
Monitoramento anti-ransomware de volume ativado (modo de aprendizado)	INFORMAÇÕES	O monitoramento anti-ransomware do volume é ativado no modo de aprendizado.	Nenhum
Monitoramento de volume Anti-ransomware em pausa (modo de aprendizado)	AVISO	O monitoramento anti-ransomware para o volume é pausado no modo de aprendizado.	Nenhum

Monitoramento de volume Anti-ransomware pausado	AVISO	O monitoramento anti-ransomware do volume é pausado.	Nenhum
Desativação da monitorização de volume Anti-ransomware	AVISO	O monitoramento anti-ransomware do volume está desabilitado.	Nenhum
Atividade de ransomware detetada	CRÍTICO	Para proteger os dados contra o ransomware detetado, foi feita uma cópia Snapshot que pode ser usada para restaurar os dados originais. O seu sistema gera e transmite uma mensagem AutoSupport ou "Call Home" para o suporte técnico da NetApp e para quaisquer destinos configurados. A mensagem AutoSupport melhora a determinação e resolução de problemas.	Consulte o "NOME DO DOCUMENTO FINAL" para tomar medidas corretivas para a atividade de ransomware.

[Voltar ao topo](#)

FSX para monitores NetApp ONTAP

Nome do monitor	Limites	Descrição do monitor	Ação corretiva
-----------------	---------	----------------------	----------------

<p>A capacidade de volume do FSX é cheia</p>	<p>Aviso a > 85 %... crítico a > 95 %</p>	<p>A capacidade de armazenamento de um volume é necessária para armazenar dados de aplicativos e clientes. Quanto mais dados armazenados no volume ONTAP, menos disponibilidade de storage para dados futuros. Se a capacidade de armazenamento de dados dentro de um volume atingir a capacidade total de armazenamento pode levar o cliente a não conseguir armazenar dados devido à falta de capacidade de armazenamento. O monitoramento do volume usado de capacidade de armazenamento garante a continuidade dos serviços de dados.</p>	<p>Ações imediatas são necessárias para minimizar a interrupção do serviço se o limite crítico for violado:...1. Considere excluir dados que não são mais necessários para liberar espaço</p>
<p>FSX volume alta latência</p>	<p>Aviso a > 1000 µs...crítico a > 2000 µs</p>	<p>Os volumes são objetos que atendem ao tráfego de e/S geralmente orientados por aplicações sensíveis à performance, incluindo aplicações DevOps, diretórios base e bancos de dados. Com latências de alto volume, as próprias aplicações podem sofrer e não conseguir realizar suas tarefas. Monitorar latências de volume é essencial para manter a performance consistente com as aplicações.</p>	<p>Ações imediatas são necessárias para minimizar a interrupção do serviço se o limite crítico for violado:...1. Se o volume tiver uma política de QoS atribuída a ele, avalie seus limites de limite caso eles estejam fazendo com que a carga de trabalho de volume seja estrangulada... Planeje tomar as seguintes ações em breve se o limite de aviso for violado:...1. Se o volume tiver uma política de QoS atribuída a ele, avalie seus limites de limite caso eles estejam fazendo com que a carga de trabalho de volume seja limitada... 2. Se o nó também estiver com alta utilização, mova o volume para outro nó ou reduza o workload total do nó.</p>

<p>Limite de inodes de volume FSX</p>	<p>Aviso a > 85 %... crítico a > 95 %</p>	<p>Os volumes que armazenam arquivos usam nós de índice (inode) para armazenar metadados de arquivos. Quando um volume esgota sua alocação de inode não mais arquivos podem ser adicionados a ele. Um alerta de alerta indica que deve ser tomada uma ação planejada para aumentar o número de inodes disponíveis. Um alerta crítico indica que o esgotamento do limite de arquivos é iminente e medidas de emergência devem ser tomadas para liberar inodes para garantir a continuidade do serviço</p>	<p>Ações imediatas são necessárias para minimizar a interrupção do serviço se o limite crítico for violado:... 1. Considere aumentar o valor inodes para o volume. Se o valor inodes já estiver no máximo, considere dividir o volume em dois ou mais volumes porque o sistema de arquivos cresceu além do tamanho máximo... Planeje tomar as seguintes ações em breve se o limite de aviso for violado:... 1. Considere aumentar o valor inodes para o volume. Se o valor inodes já estiver no máximo, considere dividir o volume em dois ou mais volumes porque o sistema de arquivos cresceu além do tamanho máximo</p>
<p>Comprometer a cota do FSX volume Qtree</p>	<p>Aviso a > 95 %... crítico a > 100 %</p>	<p>Volume Qtree quota comprometer especifica a porcentagem em que um volume é considerado sobrecarregado pelas cotas de qtree. O limite definido para a cota de qtree é atingido para o volume. O monitoramento do volume de cota de qtree em excesso garante que o usuário receba um serviço de dados ininterrupto.</p>	<p>Se o limite crítico for violado, ações imediatas devem ser tomadas para minimizar a interrupção do serviço: 1. Quando o limite de aviso é violado, considere aumentar o espaço do volume.</p>

<p>O FSX Snapshot Reserve Space está cheio</p>	<p>Aviso a > 90 %... crítico a > 95 %</p>	<p>A capacidade de armazenamento de um volume é necessária para armazenar dados de aplicativos e clientes. Uma parte desse espaço, chamada de espaço reservado instantâneo, é usada para armazenar snapshots que permitem que os dados sejam protegidos localmente. Quanto mais dados novos e atualizados forem armazenados no volume ONTAP, mais capacidade de snapshot será usada e menos capacidade de storage snapshot estarão disponíveis para dados novos ou atualizados futuros. Se a capacidade de dados do snapshot dentro de um volume atingir o espaço total de reserva do snapshot, isso pode levar o cliente a não conseguir armazenar novos dados do snapshot e a reduzir o nível de proteção para os dados no volume. O monitoramento do volume usado da capacidade do snapshot garante a continuidade dos serviços de dados.</p>	<p>Ações imediatas são necessárias para minimizar a interrupção do serviço se o limite crítico for violado:... 1. Considere configurar snapshots para usar espaço de dados no volume quando a reserva de snapshot estiver cheia... 2. Considere excluir alguns snapshots mais antigos que podem não ser mais necessários para liberar espaço... Planeje tomar as seguintes ações em breve se o limite de aviso for violado:... 1. Considere aumentar o espaço de reserva de snapshot dentro do volume para acomodar o crescimento... 2. Considere configurar snapshots para usar espaço de dados no volume quando a reserva de snapshot estiver cheia</p>
--	---	--	---

Taxa de perda de cache de volume FSX	Aviso a > 95 %... crítico a > 100 %	A taxa de perda de cache de volume é a percentagem de solicitações de leitura dos aplicativos clientes que são retornados do disco em vez de serem retornados do cache. Isto significa que o volume atingiu o limite definido.	Se o limite crítico for violado, ações imediatas devem ser tomadas para minimizar a interrupção do serviço: 1. Mova alguns workloads para fora do nó do volume para reduzir a carga de e/S 2. Reduza a demanda de workloads de prioridade mais baixa no mesmo nó por meio de limites de QoS... considere ações imediatas quando o limite de aviso for violado: 1. Mova alguns workloads para fora do nó do volume para reduzir a carga de e/S 2. Reduzir a demanda de workloads de prioridade mais baixa no mesmo nó por meio dos limites de QoS 3. Alterar as características da carga de trabalho (tamanho do bloco, armazenamento em cache do aplicativo, etc.)
--------------------------------------	-------------------------------------	--	--

[Voltar ao topo](#)

K8s monitores

Nome do monitor	Descrição	Ações corretivas	Gravidade/limiar
-----------------	-----------	------------------	------------------

<p>Latência de volume persistente alta</p>	<p>Com latências de volume persistentes altas significa que as próprias aplicações podem sofrer e não podem realizar suas tarefas. O monitoramento de latências de volume persistentes é essencial para manter a performance consistente com as aplicações. A seguir estão as latências esperadas com base no tipo de Mídia - SSD de até 1-2 milissegundos; SAS de até 8-10 milissegundos e HDD SATA de 17-20 milissegundos.</p>	<p>Ações imediatas se o limite crítico for violado, considere ações imediatas para minimizar a interrupção do serviço: Se o volume tiver uma política de QoS atribuída a ele, avalie seus limites de limite caso eles estejam fazendo com que a carga de trabalho de volume seja limitada.</p> <p>Ações a serem feitas em breve se o limite de aviso for violado, Planeje as seguintes ações imediatas: 1. Se o pool de storage também estiver com alta utilização, mova o volume para outro pool de storage. 2. Se o volume tiver uma política de QoS atribuída a ele, avalie seus limites de limite caso eles estejam fazendo com que o workload de volume seja estrangulado. 3. Se o controlador também estiver tendo alta utilização, mova o volume para outro controlador ou reduza a carga de trabalho total do controlador.</p>	<p>Aviso a > 6.000 µs crítico a > 12.000 µs</p>
<p>Saturação de memória de cluster alta</p>	<p>A saturação de memória alocável do cluster é alta. A saturação da CPU do cluster é calculada como a soma do uso da memória dividida pela soma da memória alocável em todos os K8s nós.</p>	<p>Adicionar nós. Corrija todos os nós não programados. Pods do tamanho direito para liberar memória em nós.</p>	<p>Aviso a > 80 % crítico a > 90 %</p>
<p>Falha na ligação DO POD</p>	<p>Este alerta ocorre quando um anexo de volume com POD falha.</p>		<p>Aviso</p>

Alta taxa de retransmissão	Alta taxa de retransmissão TCP	Verifique se há congestionamento de rede - identifique cargas de trabalho que consomem muita largura de banda da rede. Verifique se há alta utilização da CPU do Pod. Verifique o desempenho da rede de hardware.	Aviso a > 10 % crítico a > 25 %
Alta capacidade do sistema de arquivos de nó	Alta capacidade do sistema de arquivos de nó	- Aumente o tamanho dos discos do nó para garantir que haja espaço suficiente para os arquivos do aplicativo. - Diminuir o uso do arquivo do aplicativo.	Aviso a > 80 % crítico a > 90 %
Fluxo de trabalho de rede alta	Alta TCP Jitter (alta latência/variações de tempo de resposta)	Verifique o congestionamento da rede. Identifique cargas de trabalho que consomem muita largura de banda da rede. Verifique se há alta utilização da CPU do Pod. Verifique o desempenho da rede de hardware	Aviso a > 30 ms crítico a > 50 ms

Taxa de transferência de volume persistente	Os limites DE MBPS em volumes persistentes podem ser usados para alertar um administrador quando os volumes persistentes excederem as expectativa de desempenho predefinidas, o que pode afetar outros volumes persistentes. A ativação desse monitor gerará alertas apropriados para o perfil de taxa de transferência típica de volumes persistentes em SSDs. Esse monitor cobrirá todos os volumes persistentes em seu localatário. Os valores de limite críticos e de aviso podem ser ajustados com base em suas metas de monitoramento duplicando esse monitor e definindo limites apropriados para sua classe de armazenamento. Um monitor duplicado pode ser direcionado ainda mais para um subconjunto dos volumes persistentes em seu localatário.	Ações imediatas se o limite crítico for violado, Planeje ações imediatas para minimizar a interrupção do serviço: 1. Introduzir limites de QoS MBPS para o volume. 2. Revise a aplicação que conduz o workload no volume para verificar se há anomalias. Ações a serem feitas em breve se o limite de aviso for violado, Planeje tomar as seguintes ações imediatas: 1. Introduzir limites de QoS MBPS para o volume. 2. Revise a aplicação que conduz o workload no volume para verificar se há anomalias.	Aviso a > 10.000 MB/s crítico a > 15.000 MB/s
Recipiente em risco de ir OOM morto	Os limites de memória do recipiente estão definidos demasiado baixos. O contentor está em risco de despejo (out of Memory Kill).	Aumente os limites de memória do recipiente.	Aviso a > 95 %
Carga de trabalho reduzida	O workload não tem pods íntegros.		Crítico a menos de 1
Falha na vinculação da reclamação de volume persistente	Este alerta ocorre quando uma ligação é falhou em um PVC.		Aviso
ResourceQuota Mem limites prestes a exceder	Os limites de memória para namespace estão prestes a exceder o ResourceQuota		Aviso a > 80 % crítico a > 90 %
ResourceQuota Mem pedidos prestes a exceder	As solicitações de memória para namespace estão prestes a exceder o ResourceQuota		Aviso a > 80 % crítico a > 90 %

Falha na criação do nó	Não foi possível agendar o nó devido a um erro de configuração.	Verifique o log de eventos do Kubernetes para ver a causa da falha de configuração.	Crítico
Falha na gravação de volume persistente	O volume falhou a sua recuperação automática.		Aviso a > 0 B
Limitação da CPU do contêiner	Os limites de CPU do contentor estão definidos demasiado baixos. Os processos de contentor são lentos.	Aumente os limites da CPU do contentor.	Aviso a > 95 % crítico a > 98 %
Falha ao eliminar o Service Load Balancer			Aviso
IOPS do volume persistente	Os limites de IOPS em volumes persistentes podem ser usados para alertar um administrador quando os volumes persistentes excederem as expectativas de desempenho predefinidas. A ativação deste monitor gerará alertas apropriados para o perfil IOPS típico dos volumes de persistência. Esse monitor cobrirá todos os volumes persistentes em seu localatário. Os valores de limite críticos e de aviso podem ser ajustados com base em suas metas de monitoramento duplicando esse monitor e definindo limites apropriados para sua carga de trabalho.	Ações imediatas se o limite crítico for violado, Planeje ações imediatas para minimizar a interrupção do serviço : 1. Introduza limites de IOPS de QoS para o volume. 2. Revise a aplicação que conduz o workload no volume para verificar se há anomalias. Ações a serem feitas em breve se o limite de aviso for violado, Planeje as seguintes ações imediatas: 1. Introduza limites de IOPS de QoS para o volume. 2. Revise a aplicação que conduz o workload no volume para verificar se há anomalias.	Aviso a > 20.000 IO/s críticos a > 25.000 IO/s
Falha ao atualizar o Service Load Balancer			Aviso
Falha na montagem DO POD	Este alerta ocorre quando uma montagem falha em um POD.		Aviso

Pressão PID do nó	Os identificadores de processo disponíveis no nó (Linux) caíram abaixo de um limite de despejo.	Encontre e corrija pods que geram muitos processos e passam fome no nó das IDs de processo disponíveis. Configure o PodPidsLimit para proteger seu nó contra pods ou contentores que geram muitos processos.	Crítico a > 0
Falha na tração da imagem do pod	O Kubernetes não conseguiu extrair a imagem de contêiner de pod.	- Certifique-se de que a imagem do pod está escrita corretamente na configuração do pod. - Verifique a etiqueta de imagem existe no seu Registro. - Verifique as credenciais para o Registro de imagem. - Verifique se há problemas de conectividade do Registro. - Verifique se você não está atingindo os limites de taxa impostos pelos provedores de Registro público.	Aviso
Trabalho em execução demasiado longo	O trabalho está em execução por muito tempo		Aviso a > 1 h crítico a > 5 h
Memória do nó alta	O uso da memória do nó é alto	Adicionar nós. Corrija todos os nós não programados. Pods do tamanho direito para liberar memória em nós.	Aviso a > 85 % crítico a > 90 %
ResourceQuota limites de CPU prestes a exceder	Os limites de CPU para namespace estão prestes a exceder o ResourceQuota		Aviso a > 80 % crítico a > 90 %
Pod Crash Loop backoff	O pod travou e tentou reiniciar várias vezes.		Crítico a > 3
CPU do nó alta	O uso da CPU do nó é alto.	Adicionar nós. Corrija todos os nós não programados. Pods do tamanho direito para liberar a CPU nos nós.	Aviso a > 80 % crítico a > 90 %

Latência de rede de carga de trabalho RTT alta	Alta latência TCP RTT (Round Trip Time)	Verificar congestionamento de rede e identificar cargas de trabalho que consomem muita largura de banda de rede. Verifique se há alta utilização da CPU do Pod. Verifique o desempenho da rede de hardware.	Aviso a > 150 ms crítico a > 300 ms
Falha no trabalho	A tarefa não foi concluída com êxito devido a uma falha ou reinicialização do nó, esgotamento de recursos, tempo limite da tarefa ou falha no agendamento do pod.	Verifique os logs de eventos do Kubernetes quanto a causas de falha.	Aviso a > 1
Volume persistente cheio em alguns dias	O volume persistente ficará sem espaço em alguns dias	-Aumente o tamanho do volume para garantir que haja espaço suficiente para os arquivos do aplicativo. -Reduzir a quantidade de dados armazenados em aplicações.	Aviso a menos de 8 dia crítico a menos de 3 dia
Pressão da memória do nó	O nó está ficando sem memória. A memória disponível atingiu o limite de despejo.	Adicionar nós. Corrija todos os nós não programados. Pods do tamanho direito para liberar memória em nós.	Crítico a > 0
Nó despronto	O nó está despronto por 5 minutos	Verifique se o nó tem recursos suficientes de CPU, memória e disco. Verifique a conectividade de rede do nó. Verifique os logs de eventos do Kubernetes quanto a causas de falha.	Crítico a menos de 1
Capacidade de volume persistente alta	A capacidade usada no back-end de volume persistente é alta.	- Aumentar o tamanho do volume para garantir que haja espaço suficiente para os arquivos do aplicativo. - Reduzir a quantidade de dados armazenados nas aplicações.	Aviso a > 80 % crítico a > 90 %
Falha ao criar o Service Load Balancer	Falha na criação do Service Load Balancer		Crítico

Incompatibilidade da réplica do workload	Alguns pods atualmente não estão disponíveis para uma implantação ou DaemonSet.		Aviso a > 1
ResourceQuota CPU requests prestes a exceder	As solicitações de CPU para namespace estão prestes a exceder o ResourceQuota		Aviso a > 80 % crítico a > 90 %
Alta taxa de retransmissão	Alta taxa de retransmissão TCP	Verifique se há congestionamento de rede - identifique cargas de trabalho que consomem muita largura de banda da rede. Verifique se há alta utilização da CPU do Pod. Verifique o desempenho da rede de hardware.	Aviso a > 10 % crítico a > 25 %
Pressão do disco do nó	Espaço em disco disponível e inodes no sistema de arquivos raiz do nó ou no sistema de arquivos de imagem satisfizeram um limite de despejo.	- Aumente o tamanho dos discos do nó para garantir que haja espaço suficiente para os arquivos do aplicativo. - Diminuir o uso do arquivo do aplicativo.	Crítico a > 0
Saturação alta da CPU do cluster	A saturação alocável da CPU do cluster é alta. A saturação da CPU do cluster é calculada como a soma do uso da CPU dividida pela soma alocável da CPU em todos os K8s nós.	Adicionar nós. Corrija todos os nós não programados. Pods do tamanho direito para liberar a CPU nos nós.	Aviso a > 80 % crítico a > 90 %

[Voltar ao topo](#)

Alterar monitores de registo

Nome do monitor	Gravidade	Descrição do monitor
Volume interno descoberto	Informativo	Esta mensagem ocorre quando um volume interno é descoberto.
Volume interno modificado	Informativo	Esta mensagem ocorre quando um volume interno é modificado.
Nó de storage descoberto	Informativo	Esta mensagem ocorre quando um nó de storage é descoberto.
Nó de storage removido	Informativo	Esta mensagem ocorre quando um nó de armazenamento é removido.

Pool de armazenamento descoberto	Informativo	Esta mensagem ocorre quando um pool de armazenamento é descoberto.
Máquina virtual de armazenamento descoberta	Informativo	Esta mensagem ocorre quando uma máquina virtual de storage é descoberta.
Máquina virtual de armazenamento Modificada	Informativo	Esta mensagem ocorre quando uma máquina virtual de storage é modificada.

[Voltar ao topo](#)

Monitores de coleta de dados

Nome do monitor	Descrição	Ação corretiva
Desativação da unidade de aquisição	As unidades de aquisição do Data Infrastructure Insights são reiniciadas periodicamente como parte das atualizações para introduzir novos recursos. Isso acontece uma vez por mês ou menos em um ambiente típico. Um alerta de aviso de que uma unidade de aquisição foi desligada deve ser seguido logo após por uma resolução, observando que a unidade de aquisição recém-reiniciada concluiu um registro com o Data Infrastructure Insights. Normalmente, este ciclo de desligamento para Registro leva de 5 a 15 minutos.	Se o alerta ocorrer com frequência ou durar mais de 15 minutos, verifique o funcionamento do sistema que hospeda a Unidade de aquisição, a rede e qualquer proxy que conete a AU à Internet.
O coletor falhou	A pesquisa de um coletor de dados encontrou uma situação de falha inesperada.	Visite a página do coletor de dados em Data Infrastructure Insights para saber mais sobre a situação.

Aviso do coletor	Este alerta normalmente pode surgir devido a uma configuração incorreta do coletor de dados ou do sistema de destino. Revisite as configurações para evitar alertas futuros. Também pode ser devido a uma recuperação de dados menos que completos, onde o coletor de dados reuniu todos os dados que ele poderia. Isso pode acontecer quando as situações mudam durante a coleta de dados (por exemplo, uma máquina virtual presente no início da coleta de dados é excluída durante a coleta de dados e antes que seus dados sejam capturados).	Verifique a configuração do coletor de dados ou do sistema de destino. Observe que o monitor de Aviso de Coletor pode enviar mais alertas do que outros tipos de monitor, por isso é recomendável não definir destinatários de alerta, a menos que você esteja solucionando problemas.
------------------	---	--

[Voltar ao topo](#)

Monitores de segurança

Nome do monitor	Limite	Descrição do monitor	Ação corretiva
Transporte HTTPS AutoSupport desativado	Aviso a menos de 1	O AutoSupport suporta HTTPS, HTTP e SMTP para protocolos de transporte. Devido à natureza sensível das mensagens AutoSupport, a NetApp recomenda fortemente o uso de HTTPS como o protocolo de transporte padrão para enviar mensagens AutoSupport para o suporte ao NetApp.	Para definir o HTTPS como o protocolo de transporte para mensagens AutoSupport, execute o seguinte comando ONTAP:... system node AutoSupport modify -transport https
Cifras inseguras de cluster para SSH	Aviso a menos de 1	Indica que o SSH está usando cifras inseguras, por exemplo cifras que começam com *cbc.	Para remover as cifras CBC, execute o seguinte comando ONTAP:... security ssh remove -vserver <admin vserver> -ciphers AES256-cbc,aes192-cbc,AES128-cbc,3DES-cbc

Banner de login de cluster desativado	Aviso a menos de 1	Indica que o banner Login está desativado para usuários que acessam o sistema ONTAP. A exibição de um banner de login é útil para estabelecer expectativa de acesso e uso do sistema.	Para configurar o banner de login para um cluster, execute o seguinte comando ONTAP:... security login banner modificar -vserver <admin svm> -mensagem "Acesso restrito a usuários autorizados"
Comunicação por pares de cluster não encriptada	Aviso a menos de 1	Ao replicar dados para recuperação de desastre, armazenamento em cache ou backup, você precisa proteger esses dados durante o transporte por cabo de um cluster ONTAP para outro. A criptografia deve ser configurada nos clusters de origem e destino.	Para habilitar a criptografia em relacionamentos de pares de cluster criados antes do ONTAP 9.6, o cluster de origem e destino deve ser atualizado para 9,6. Em seguida, use o comando "cluster peer Modify" para alterar os pares de cluster de origem e destino para usar a criptografia de peering de cluster. Consulte o Guia de endurecimento de segurança do NetApp para ONTAP 9 para obter detalhes.
Utilizador Admin local predefinido ativado	Aviso a > 0	O NetApp recomenda bloquear (desativar) quaisquer contas de usuário administrador padrão (internas) desnecessárias com o comando LOCK. São principalmente contas padrão para as quais as senhas nunca foram atualizadas ou alteradas.	Para bloquear a conta "admin" interna, execute o seguinte comando ONTAP:... security login lock -username admin
Modo FIPS desativado	Aviso a menos de 1	Quando a conformidade com o FIPS 140-2 está ativada, o TLSv1 e o SSLv3 são desativados e apenas o TLSv1,1 e o TLSv1,2 permanecem ativados. O ONTAP impede que você ative o TLSv1 e o SSLv3 quando a conformidade com o FIPS 140-2 estiver habilitada.	Para habilitar a conformidade com o FIPS 140-2 em um cluster, execute o seguinte comando ONTAP no modo de privilégio avançado:... security config modifique -interface SSL -is-fips-enabled true

Encaminhamento de registo não encriptado	Aviso a menos de 1	O descarregamento de informações do syslog é necessário para limitar o escopo ou a pegada de uma violação a um único sistema ou solução. Portanto, a NetApp recomenda descarregar com segurança as informações do syslog para um local seguro de armazenamento ou retenção.	Uma vez criado um destino de encaminhamento de registo, o respetivo protocolo não pode ser alterado. Para mudar para um protocolo criptografado, exclua e recrie o destino de encaminhamento de log usando o seguinte comando ONTAP:... cluster log-forwarding create -destination <destination ip> -Protocol tcp-Encrypted
MD5 Palavra-passe com hash	Aviso a > 0	A NetApp recomenda fortemente usar a função hash SHA-512 mais segura para senhas de contas de usuário do ONTAP. As contas que usam a função hash MD5 menos segura devem migrar para a função hash SHA-512.	O NetApp recomenda fortemente que as contas de usuário migrem para a solução SHA-512 mais segura, fazendo com que os usuários alterem suas senhas.... para bloquear contas com senhas que usam a função hash MD5, execute o seguinte comando ONTAP:... security login lock -vserver * -username * -hash -function md5
Nenhum servidor NTP está configurado	Aviso a menos de 1	Indica que o cluster não tem servidores NTP configurados. Para redundância e serviço ideal, a NetApp recomenda que você associe pelo menos três servidores NTP ao cluster.	Para associar um servidor NTP ao cluster, execute o seguinte comando ONTAP: Cluster time-service servidor ntp create -Server [Nome do host do servidor ntp ou endereço ip>
A contagem do servidor NTP é baixa	Aviso a menos de 3	Indica que o cluster tem menos de 3 servidores NTP configurados. Para redundância e serviço ideal, a NetApp recomenda que você associe pelo menos três servidores NTP ao cluster.	Para associar um servidor NTP ao cluster, execute o seguinte comando ONTAP

Shell remoto ativado	Aviso a > 0	O Shell remoto não é um método seguro para estabelecer acesso de linha de comando à solução ONTAP. O Shell remoto deve ser desativado para acesso remoto seguro.	Para desativar o shell remoto em um cluster, execute o seguinte comando ONTAP no modo de privilégio avançado:...Protocolo de segurança modificar -application rsh- enabled false NetApp
Registo de auditoria da VM de armazenamento desativado	Aviso a menos de 1	Indica que o log de auditoria está desativado para SVM.	Para configurar o log de auditoria para um vserver, execute o seguinte comando ONTAP:... vserver audit enable -vserver <svm>
Armazenamento VM cifras inseguras para SSH	Aviso a menos de 1	Indica que o SSH está usando cifras inseguras, por exemplo cifras que começam com *cbc.	Para remover as cifras CBC, execute o seguinte comando ONTAP:... security ssh remove -vserver <vserver> -ciphers AES256-cbc,aes192-cbc,AES128-cbc,3DES-cbc
Banner de login da VM de armazenamento desativado	Aviso a menos de 1	Indica que o banner Login está desativado para usuários que acessam SVMs no sistema. A exibição de um banner de login é útil para estabelecer expectativa de acesso e uso do sistema.	Para configurar o banner de login para um cluster, execute o seguinte comando ONTAP:... security login banner modificar -vserver <svm> -mensagem "Acesso restrito a usuários autorizados"
Protocolo Telnet ativado	Aviso a > 0	O Telnet não é um método seguro para estabelecer acesso à linha de comando à solução ONTAP. O Telnet deve ser desativado para acesso remoto seguro.	A NetApp recomenda o Shell seguro (SSH) para acesso remoto seguro. Para desativar o Telnet em um cluster, execute o seguinte comando ONTAP no modo de privilégio avançado: .. Protocolo de segurança modificar -Application telnet -enabled false

[Voltar ao topo](#)

Monitores de proteção de dados

Nome do monitor	Limites	Descrição do monitor	Ação corretiva
-----------------	---------	----------------------	----------------

<p>Espaço insuficiente para cópia Snapshot LUN</p>	<p>(O filtro contém_luns: Sim) Aviso a > 95 %... crítico a > 100 %</p>	<p>A capacidade de armazenamento de um volume é necessária para armazenar dados de aplicativos e clientes. Uma parte desse espaço, chamada de espaço reservado instantâneo, é usada para armazenar snapshots que permitem que os dados sejam protegidos localmente. Quanto mais dados novos e atualizados forem armazenados no volume ONTAP, mais capacidade de snapshot será usada e menos capacidade de storage snapshot estarão disponíveis para dados novos ou atualizados futuros. Se a capacidade de dados do snapshot dentro de um volume atingir o espaço total de reserva do snapshot, isso pode levar o cliente a não conseguir armazenar novos dados do snapshot e a reduzir o nível de proteção dos dados nos LUNs no volume. O monitoramento do volume usado da capacidade do snapshot garante a continuidade dos serviços de dados.</p>	<p>Ações imediatas se o limite crítico for violado, considere ações imediatas para minimizar a interrupção do serviço: 1. Configure instantâneos para usar o espaço de dados no volume quando a reserva de snapshot estiver cheia. 2. Elimine alguns instantâneos indesejados mais antigos para libertar espaço.</p> <p>Ações a serem feitas em breve se o limite de aviso for violado, Planeje tomar as seguintes ações imediatas: 1. Aumente o espaço de reserva do snapshot dentro do volume para acomodar o crescimento. 2. Configure instantâneos para usar o espaço de dados no volume quando a reserva de snapshot estiver cheia.</p>
--	--	---	---

Atraso no relacionamento com o SnapMirror	Aviso a > 150%... crítico a > 300%	O atraso no relacionamento do SnapMirror é a diferença entre o carimbo de data/hora do snapshot e a hora no sistema de destino. O lag_time_percent é a relação entre o tempo de atraso e o intervalo de programação da Política SnapMirror. Se o tempo de atraso for igual ao intervalo de programação, o lag_time_percent será de 100%. Se a política SnapMirror não tiver um agendamento, lag_time_percent não será calculado.	Monitore o status do SnapMirror usando o comando "SnapMirror show". Verifique o histórico de transferência do SnapMirror usando o comando "SnapMirror show-history"
---	------------------------------------	--	---

[Voltar ao topo](#)

Monitores do volume de nuvem (CVO)

Nome do monitor	Gravidade do IC	Descrição do monitor	Ação corretiva
Disco CVO fora de serviço	INFORMAÇÕES	Esse evento ocorre quando um disco é removido do serviço porque foi marcado como com falha, está sendo higienizado ou entrou no Centro de Manutenção.	Nenhum

<p>CVO Giveback do pool de armazenamento falhou</p>	<p>CRÍTICO</p>	<p>Esse evento ocorre durante a migração de um agregado como parte de um failover de armazenamento (SFO), quando o nó de destino não pode alcançar os armazenamentos de objetos.</p>	<p>Execute as seguintes ações corretivas: Verifique se o LIF entre clusters está on-line e funcional usando o comando "network interface show". Verifique a conectividade de rede ao servidor de armazenamento de objetos usando o comando "ping" sobre o LIF entre clusters de nó de destino. Verifique se a configuração do seu armazenamento de objetos não foi alterada e se as informações de login e conectividade ainda são precisas usando o comando "Aggregate object-store config show". Alternativamente, você pode substituir o erro especificando false para o parâmetro "require-Partner-waiting" do comando giveback. Entre em Contato com o suporte técnico da NetApp para obter mais informações ou assistência.</p>
---	----------------	--	---

<p>Interconexão do CVO HA desativada</p>	<p>AVISO</p>	<p>A interconexão de alta disponibilidade (HA) está inativa. Risco de interrupção de serviço quando o failover não está disponível.</p>	<p>As ações corretivas dependem do número e do tipo de links de interconexão de HA suportados pela plataforma, bem como do motivo pelo qual a interconexão está inativa. Se os links estiverem inativos: Verifique se ambas as controladoras no par de HA estão operacionais. Para links conectados externamente, verifique se os cabos de interconexão estão conectados corretamente e se os SFPs (Small Form-factor Pluggables), se aplicável, estão encaixados corretamente em ambos os controladores. Para ligações ligadas internamente, desative e volte a ativar as ligações, uma após a outra, utilizando os comandos "ic link Off" (ligação ic desligada) e "ic link ON" (ligação ic ligada). Se as ligações estiverem desativadas, ative as ligações utilizando o comando "ic link ON". Se um par não estiver conectado, desative e reative os links, um após o outro, usando os comandos "ic link off" e "ic link on". Contacte o suporte técnico da NetApp se o problema persistir.</p>
--	--------------	---	---

<p>Sessões máx. CVO por utilizador excedidas</p>	<p>AVISO</p>	<p>Você excedeu o número máximo de sessões permitidas por usuário em uma conexão TCP. Qualquer solicitação para estabelecer uma sessão será negada até que algumas sessões sejam liberadas.</p>	<p>Execute as seguintes ações corretivas: Inspeccione todos os aplicativos que são executados no cliente e encerre qualquer um que não esteja funcionando corretamente. Reinicie o cliente. Verifique se o problema é causado por um aplicativo novo ou existente: Se o aplicativo for novo, defina um limite mais alto para o cliente usando o comando "cifs option modificar -Max -abre-same-file-per-tree". Em alguns casos, os clientes operam como esperado, mas exigem um limite mais alto. Você deve ter privilégios avançados para definir um limite mais alto para o cliente. Se o problema for causado por um aplicativo existente, pode haver um problema com o cliente. Entre em Contato com o suporte técnico da NetApp para obter mais informações ou assistência.</p>
--	--------------	---	--

<p>Conflito de nomes NetBIOS CVO</p>	<p>CRÍTICO</p>	<p>O serviço de nomes NetBIOS recebeu uma resposta negativa a uma solicitação de Registro de nomes de uma máquina remota. Isso geralmente é causado por um conflito no nome NetBIOS ou um alias. Como resultado, os clientes podem não conseguir acessar dados ou se conectar ao nó certo de fornecimento de dados no cluster.</p>	<p>Execute qualquer uma das seguintes ações corretivas: Se houver um conflito no nome NetBIOS ou um alias, execute uma das seguintes ações: Exclua o alias NetBIOS duplicado usando o comando "vserver cifs delete -aliases alias -vserver vserver vserver". Renomeie um alias NetBIOS excluindo o nome duplicado e adicionando um alias com um novo nome usando o comando "vserver cifs create -aliases alias -vserver vserver". Se não houver aliases configurados e houver um conflito no nome NetBIOS, renomeie o servidor CIFS usando os comandos "vserver cifs delete -vserver vserver" e "vserver cifs create -cifs -server netbiosname". OBSERVAÇÃO: Excluir um servidor CIFS pode tornar os dados inacessíveis. Remova o nome NetBIOS ou renomeie o NetBIOS na máquina remota.</p>
<p>CVO NFSv4 Store Pool esgotado</p>	<p>CRÍTICO</p>	<p>Uma piscina de loja NFSv4 foi esgotada.</p>	<p>Se o servidor NFS não responder por mais de 10 minutos após este evento, entre em Contato com o suporte técnico da NetApp.</p>
<p>Pânico do nó CVO</p>	<p>AVISO</p>	<p>Este evento é emitido quando ocorre um pânico</p>	<p>Entre em Contato com o suporte ao cliente da NetApp.</p>

Espaço de volume raiz do nó CVO baixo	CRÍTICO	O sistema detetou que o volume raiz está perigosamente baixo no espaço. O nó não está totalmente operacional. As LIFs de dados podem ter falhado no cluster, por causa do qual o acesso NFS e CIFS é limitado no nó. A capacidade administrativa está limitada aos procedimentos de recuperação locais para que o nó limpe o espaço no volume raiz.	Execute as seguintes ações corretivas: Limpe o espaço no volume raiz excluindo cópias Snapshot antigas, excluindo arquivos que você não precisa mais do diretório /mroot ou expandindo a capacidade do volume raiz. Reinicie o controlador. Entre em Contato com o suporte técnico da NetApp para obter mais informações ou assistência.
Compartilhamento Admin inexistente do CVO	CRÍTICO	Problema Vscan: Um cliente tentou se conectar a um compartilhamento inexistente do ONTAP_ADMIN.	Certifique-se de que o Vscan esteja habilitado para o ID SVM mencionado. Ativar o Vscan em um SVM faz com que o compartilhamento ONTAP_ADMIN seja criado automaticamente para o SVM.
Host do armazenamento de objetos CVO não resolvível	CRÍTICO	O nome do host do servidor de armazenamento de objetos não pode ser resolvido para um endereço IP. O cliente de armazenamento de objetos não pode se comunicar com o servidor de armazenamento de objetos sem resolver um endereço IP. Como resultado, os dados podem estar inacessíveis.	Verifique a configuração DNS para verificar se o nome do host está configurado corretamente com um endereço IP.

LIF entre clusters do armazenamento de objetos CVO inativo	CRÍTICO	O cliente de armazenamento de objetos não consegue encontrar um LIF operacional para se comunicar com o servidor de armazenamento de objetos. O nó não permitirá o tráfego do cliente de armazenamento de objetos até que o LIF entre clusters esteja operacional. Como resultado, os dados podem estar inacessíveis.	Execute as seguintes ações corretivas: Verifique o status de clusters de LIF usando o comando "network interface show -role". Verifique se o LIF entre clusters está configurado corretamente e operacional. Se um LIF entre clusters não estiver configurado, adicione-o usando o comando "network interface create -role".
Incompatibilidade da assinatura do armazenamento de objetos CVO	CRÍTICO	A assinatura de solicitação enviada ao servidor de armazenamento de objetos não corresponde à assinatura calculada pelo cliente. Como resultado, os dados podem estar inacessíveis.	Verifique se a chave de acesso secreto está configurada corretamente. Se estiver configurado corretamente, contacte o suporte técnico da NetApp para obter assistência.
Memória do monitor QoS CVO maximizada	CRÍTICO	A memória dinâmica do subsistema QoS atingiu seu limite para o hardware atual da plataforma. Alguns recursos de QoS podem operar em uma capacidade limitada.	Exclua algumas cargas de trabalho ou fluxos ativos para liberar memória. Use o comando "statistics show -object Workload -counter OPS" para determinar quais cargas de trabalho estão ativas. Workloads ativos mostram operações que não são zero. Em seguida, use o comando "Workload DELETE <workload_name>" várias vezes para remover cargas de trabalho específicas. Como alternativa, use o comando "stream delete -Workload <workload name> *" para excluir os fluxos associados da carga de trabalho ativa.

<p>Tempo limite DE LEITURA do CVO</p>	<p>CRÍTICO</p>	<p>Uma operação de ARQUIVO READDIR excedeu o tempo limite que é permitido executar no WAFL. Isso pode ser por causa de diretórios muito grandes ou esparsos. Recomenda-se a ação corretiva.</p>	<p>Execute as seguintes ações corretivas: Encontre informações específicas para diretórios recentes que tiveram operações de ARQUIVO READDIR expiram usando o seguinte comando 'deag' Privilege nodeshell CLI: WAFL readdir notice show. Verifique se os diretórios são indicados como esparsos ou não: Se um diretório é indicado como esparsos, é recomendável que você copie o conteúdo do diretório para um novo diretório para remover a frouxidão do arquivo de diretório. Se um diretório não for indicado como esparsos e o diretório for grande, é recomendável reduzir o tamanho do arquivo de diretório reduzindo o número de entradas de arquivo no diretório.</p>
---------------------------------------	----------------	---	--

Falha na realocação do CVO do pool de storage	CRÍTICO	Esse evento ocorre durante a realocação de um agregado, quando o nó de destino não pode alcançar os armazenamentos de objetos.	Execute as seguintes ações corretivas: Verifique se o LIF entre clusters está on-line e funcional usando o comando "network interface show". Verifique a conectividade de rede ao servidor de armazenamento de objetos usando o comando "ping" sobre o LIF entre clusters de nó de destino. Verifique se a configuração do seu armazenamento de objetos não foi alterada e se as informações de login e conectividade ainda são precisas usando o comando "Aggregate object-store config show". Alternativamente, você pode substituir o erro usando o parâmetro "override-destination-checks" do comando relocation. Entre em Contato com o suporte técnico da NetApp para obter mais informações ou assistência.
Cópia sombra CVO falhou	CRÍTICO	Um serviço de cópia de sombra de volume (VSS), uma operação de serviço de backup e restauração do Microsoft Server, falhou.	Verifique o seguinte usando as informações fornecidas na mensagem de evento: A configuração de cópia de sombra está ativada? As licenças apropriadas estão instaladas? Em que compartilhamentos é realizada a operação de cópia sombra? O nome da partilha está correto? O caminho de compartilhamento existe? Quais são os estados do conjunto de cópias de sombra e suas cópias de sombra?
Interrupção da VM de armazenamento do CVO com êxito	INFORMAÇÕES	Esta mensagem ocorre quando uma operação 'vserver stop' é bem-sucedida.	Use o comando 'vserver start' para iniciar o acesso a dados em uma VM de armazenamento.

Autenticação CIFS do CVO demais	AVISO	Muitas negociações de autenticação ocorreram simultaneamente. Existem 256 solicitações de nova sessão incompletas deste cliente.	Investigue por que o cliente criou 256 ou mais solicitações de conexão novas. Você pode ter que entrar em Contato com o fornecedor do cliente ou do aplicativo para determinar por que o erro ocorreu.
Discos não atribuídos CVO	INFORMAÇÕES	O sistema tem discos não atribuídos - a capacidade está sendo desperdiçada e seu sistema pode ter alguma configuração incorreta ou alteração parcial de configuração aplicada.	Execute as seguintes ações corretivas: Determine quais discos não são atribuídos usando o comando "Disk show -n". Atribua os discos a um sistema usando o comando "Disk Assign" (atribuir disco).
CVO Acesso não autorizado do Usuário ao Admin Share	AVISO	Um cliente tentou se conectar ao compartilhamento privilegiado do ONTAP_ADMIN, mesmo que seu usuário conectado não seja um usuário permitido.	Execute as seguintes ações corretivas: Certifique-se de que o nome de usuário e o endereço IP mencionados estão configurados em um dos conjuntos de scanners Vscan ativos. Verifique a configuração do conjunto do scanner que está atualmente ativa usando o comando "vserver vscan pool show-active".
Vírus CVO detetado	AVISO	Um servidor Vscan comunicou um erro ao sistema de armazenamento. Isso normalmente indica que um vírus foi encontrado. No entanto, outros erros no servidor Vscan podem causar este evento. O acesso do cliente ao ficheiro é negado. O servidor Vscan pode, dependendo de suas configurações e configurações, limpar o arquivo, colocá-lo em quarentena ou excluí-lo.	Verifique o log do servidor Vscan relatado no evento "syslog" para ver se ele foi capaz de limpar, colocar em quarentena ou excluir o arquivo infetado com sucesso. Se não conseguir fazê-lo, um administrador de sistema poderá ter de eliminar manualmente o ficheiro.

CVO volume Offline	INFORMAÇÕES	Esta mensagem indica que um volume está offline.	Traga o volume de volta online.
Volume CVO restrito	INFORMAÇÕES	Este evento indica que um volume flexível é restringido.	Traga o volume de volta online.

[Voltar ao topo](#)

Monitores de log do mediador da continuidade de negócios (SnapMirror for Business Continuity)

Nome do monitor	Gravidade	Descrição do monitor	Ação corretiva
ONTAP Mediador adicionado	INFORMAÇÕES	Esta mensagem ocorre quando o Mediador ONTAP é adicionado com sucesso em um cluster.	Nenhum
Mediador ONTAP não acessível	CRÍTICO	Esta mensagem ocorre quando o Mediador ONTAP é reutilizado ou o pacote Mediador não é mais instalado no servidor Mediador. Como resultado, o failover do SnapMirror não é possível.	Remova a configuração do Mediador ONTAP atual usando o comando "SnapMirror Mediator remove". Reconfigure o acesso ao Mediador ONTAP usando o comando "SnapMirror Mediator add".
ONTAP Mediador removido	INFORMAÇÕES	Esta mensagem ocorre quando o Mediador ONTAP é removido com sucesso de um cluster.	Nenhum
ONTAP Mediador inalcançável	AVISO	Esta mensagem ocorre quando o Mediador ONTAP não está acessível em um cluster. Como resultado, o failover do SnapMirror não é possível.	Verifique a conectividade de rede ao Mediador ONTAP usando os comandos "Network ping" e "network traceroute". Se o problema persistir, remova a configuração do Mediador ONTAP atual usando o comando "SnapMirror Mediator remove". Reconfigure o acesso ao Mediador ONTAP usando o comando "SnapMirror Mediator add".

Certificado CA SMBC expirado	CRÍTICO	Esta mensagem ocorre quando o certificado de autoridade de certificação do mediador (CA) do ONTAP expirou. Como resultado, não será possível qualquer comunicação adicional com o Mediador ONTAP.	Remova a configuração do Mediador ONTAP atual usando o comando "SnapMirror Mediator remove". Atualize um novo certificado de CA no servidor do ONTAP Mediator. Reconfigure o acesso ao Mediador ONTAP usando o comando "SnapMirror Mediator add".
Certificado SMBC CA expirando	AVISO	Esta mensagem ocorre quando o certificado de autoridade de certificação do mediador (CA) da ONTAP expira nos próximos 30 dias.	Antes que esse certificado expire, remova a configuração do Mediador ONTAP atual usando o comando "SnapMirror Mediator remove". Atualize um novo certificado de CA no servidor do ONTAP Mediator. Reconfigure o acesso ao Mediador ONTAP usando o comando "SnapMirror Mediator add".
Certificado Cliente SMBC expirado	CRÍTICO	Esta mensagem ocorre quando o certificado de cliente do Mediador ONTAP expirou. Como resultado, não será possível qualquer comunicação adicional com o Mediador ONTAP.	Remova a configuração do Mediador ONTAP atual usando o comando "SnapMirror Mediator remove". Reconfigure o acesso ao Mediador ONTAP usando o comando "SnapMirror Mediator add".
Certificado Cliente SMBC a expirar	AVISO	Esta mensagem ocorre quando o certificado de cliente do Mediador ONTAP expira nos próximos 30 dias.	Antes que esse certificado expire, remova a configuração do Mediador ONTAP atual usando o comando "SnapMirror Mediator remove". Reconfigure o acesso ao Mediador ONTAP usando o comando "SnapMirror Mediator add".

<p>Relação SMBC fora de sincronização Nota: O UM não tem este</p>	<p>CRÍTICO</p>	<p>Esta mensagem ocorre quando uma relação SnapMirror for Business Continuity (SMBC) muda o status de "in-Sync" para "out-of-Sync". Devido a essa proteção de dados RPO igual a 0 será interrompida.</p>	<p>Verifique a conexão de rede entre os volumes de origem e destino. Monitore o status do relacionamento SMBC usando o comando "SnapMirror show" no destino e usando o comando "SnapMirror list-destinations" na origem. A ressincronização automática tentará trazer a relação de volta ao status "in-sync". Se a ressincronização falhar, verifique se todos os nós no cluster estão em quórum e estão em bom estado.</p>
<p>Certificado do servidor SMBC expirou</p>	<p>CRÍTICO</p>	<p>Esta mensagem ocorre quando o certificado do servidor do Mediador ONTAP expirou. Como resultado, não será possível qualquer comunicação adicional com o Mediador ONTAP.</p>	<p>Remova a configuração do Mediador ONTAP atual usando o comando "SnapMirror Mediator remove". Atualize um novo certificado de servidor no servidor do ONTAP Mediator. Reconfigure o acesso ao Mediador ONTAP usando o comando "SnapMirror Mediator add".</p>
<p>O certificado do servidor SMBC está a expirar</p>	<p>AVISO</p>	<p>Esta mensagem ocorre quando o certificado do servidor do Mediador ONTAP expira nos próximos 30 dias.</p>	<p>Antes que esse certificado expire, remova a configuração do Mediador ONTAP atual usando o comando "SnapMirror Mediator remove". Atualize um novo certificado de servidor no servidor do ONTAP Mediator. Reconfigure o acesso ao Mediador ONTAP usando o comando "SnapMirror Mediator add".</p>

[Voltar ao topo](#)

Monitores adicionais de alimentação, Heartbeat e diversos do sistema

Nome do monitor	Gravidade	Descrição do monitor	Ação corretiva
Fonte de alimentação do compartimento de disco descoberta	INFORMATIVO	Esta mensagem ocorre quando uma unidade de fonte de alimentação é adicionada ao compartimento de disco.	NENHUM
Fonte de alimentação de prateleiras de disco removida	INFORMATIVO	Esta mensagem ocorre quando uma unidade de fonte de alimentação é removida do compartimento de disco.	NENHUM
Switchover não planejado automático da MetroCluster desativado	CRÍTICO	Esta mensagem ocorre quando a capacidade de comutação não planejada automática é desativada.	Execute o comando "MetroCluster Modify -node-name <nodename> -automatic-switchover -onfailure true" para cada nó no cluster para habilitar o switchover automático.
Ponte de armazenamento MetroCluster inacessível	CRÍTICO	A ponte de armazenamento não é acessível através da rede de gerenciamento	1) se a ponte for monitorada pelo SNMP, verifique se o LIF de gerenciamento do nó está ativo usando o comando "network interface show". Verifique se a ponte está viva usando o comando "ping de rede". 2) se a ponte for monitorada na banda, verifique o cabeamento da malha para a ponte e verifique se a ponte está ligada.
Temperatura da ponte do MetroCluster anormal - abaixo de crítico	CRÍTICO	O sensor na ponte Fibre Channel está relatando uma temperatura abaixo do limite crítico.	1) Verifique o status operacional dos ventiladores na ponte de armazenamento. 2) Verifique se a ponte está operando sob condições de temperatura recomendadas.

Nome do monitor	Gravidade	Descrição do monitor	Ação corretiva
Temperatura da ponte do MetroCluster anormal - acima de crítico	CRÍTICO	O sensor na ponte Fibre Channel está relatando uma temperatura acima do limite crítico.	1) verificar o estado operacional do sensor de temperatura do chassis na ponte de armazenamento utilizando o comando "Storage bridge show -cooling". 2) Verifique se a ponte de armazenamento está operando sob condições de temperatura recomendadas.
Agregado de MetroCluster deixado para trás	AVISO	O agregado foi deixado para trás durante o switchback.	1) Verifique o estado agregado usando o comando "aggr show". 2) se o agregado estiver online, devolva-o ao seu proprietário original usando o comando "MetroCluster switchback".
Todos os links entre parceiros da MetroCluster para baixo	CRÍTICO	Os adaptadores de interconexão RDMA e os LIFs entre clusters têm conexões quebradas com o cluster de peering ou o cluster de peering está inativo.	1) assegurar que os LIFs entre clusters estão em funcionamento. Repare os LIFs entre clusters se estiverem inativos. 2) Verifique se o cluster com peering está funcionando usando o comando "cluster peer ping". Consulte o Guia de recuperação de desastres do MetroCluster se o cluster com peering estiver inativo. 3) para o Fabric MetroCluster, verifique se os ISLs de malha back-end estão funcionando. Repare as ISLs de tecido back-end se estiverem inoperantes. 4) para configurações MetroCluster que não sejam de malha, verifique se o cabeamento está correto entre os adaptadores de interconexão RDMA. Reconfigure o cabeamento se os links estiverem inativos.

Nome do monitor	Gravidade	Descrição do monitor	Ação corretiva
Parceiros MetroCluster não alcançáveis através da rede de peering	CRÍTICO	A conectividade com o cluster de pares está quebrada.	1) Certifique-se de que a porta está conectada à rede/switch correto. 2) garantir que o LIF entre clusters esteja conectado com o cluster de peered. 3) Certifique-se de que o cluster de peered está ativo e em execução usando o comando "cluster peer ping". Consulte o Guia de recuperação de desastres do MetroCluster se o cluster com peering estiver inativo.
Todos os links para baixo são MetroCluster Inter	CRÍTICO	Todos os ISLs (Inter-Switch Links) no comutador de armazenamento estão inativos.	1) reparar os ISLs de tecido back-end no interruptor de armazenamento. 2) Certifique-se de que o switch do parceiro está ativo e seus ISLs estão operacionais. 3) garantir que os equipamentos intermediários, como os dispositivos xWDM, estejam operacionais.
Nó MetroCluster para a ligação SAS da pilha de armazenamento para baixo	AVISO	O adaptador SAS ou seu cabo conectado podem estar com falha.	1. Verifique se o adaptador SAS está on-line e em execução. 2. Verifique se a conexão do cabo físico está segura e funcionando e substitua o cabo, se necessário. 3. Se o adaptador SAS estiver conectado às gavetas de disco, verifique se os IOMs e os discos estão corretamente assentados.
O iniciador do MetroClusterFC liga para baixo	CRÍTICO	O adaptador do iniciador FC está com falha.	1. Certifique-se de que o link do iniciador FC não foi adulterado. 2. Verifique o status operacional do adaptador do iniciador FC usando o comando "system node run -node local -command storage show adapter".

Nome do monitor	Gravidade	Descrição do monitor	Ação corretiva
Ligação de interligação FC-VI descendente	CRÍTICO	O link físico na porta FC-VI está offline.	1. Certifique-se de que a ligação FC-VI não foi adulterada. 2. Verifique se o status físico do adaptador FC-VI é "Up" usando o comando "MetroCluster interconnect adapter show". 3. Se a configuração incluir switches de malha, verifique se eles estão cabeados e configurados corretamente.
Discos de reserva MetroCluster deixados para trás	AVISO	O disco sobressalente foi deixado para trás durante o switchback.	Se o disco não falhar, devolva-o ao proprietário original usando o comando "MetroCluster switchback".
Porta de ponte de armazenamento MetroCluster para baixo	CRÍTICO	A porta na ponte de armazenamento está offline.	1) Verifique o status operacional das portas na ponte de armazenamento usando o comando "storage bridge show -ports". 2) Verifique a conectividade lógica e física à porta.
Falha nas ventoinhas do interruptor de armazenamento do MetroCluster	CRÍTICO	A ventoinha no interruptor de armazenamento falhou.	1) assegurar-se de que os ventiladores do contactor estão a funcionar corretamente, utilizando o comando "interruptor de memorização show -refrigeração". 2) Certifique-se de que as FRUs do ventilador estão inseridas corretamente e operacionais.

Nome do monitor	Gravidade	Descrição do monitor	Ação corretiva
Comutador de armazenamento MetroCluster inalcançável	CRÍTICO	O comutador de armazenamento não é acessível através da rede de gestão.	1) Certifique-se de que o LIF de gerenciamento do nó esteja ativo usando o comando "network interface show". 2) Certifique-se de que o switch está ativo usando o comando "network ping". 3) Certifique-se de que o switch está acessível através de SNMP, verificando suas configurações SNMP depois de fazer login no switch.
As fontes de alimentação do interruptor MetroCluster falharam	CRÍTICO	Uma unidade de fonte de alimentação no interruptor de armazenamento não está operacional.	1) Verifique os detalhes do erro usando o comando "storage switch show -error -switch-name <switch name>". 2) identificar a unidade de fonte de alimentação defeituosa usando o comando "interruptor de armazenamento show -POWER -switch-name <switch name>". 3) assegurar que o unite da fonte de alimentação inserido corretamente no chassi do interruptor de armazenamento e totalmente operacional.
Sensores de temperatura do interruptor MetroCluster falharam	CRÍTICO	O sensor no interruptor Fibre Channel falhou.	1) verificar o estado de funcionamento dos sensores de temperatura no contactor de memorização, utilizando o comando "interruptor de memorização indicar -refrigeração". 2) Verifique se o interruptor está operando sob condições de temperatura recomendadas.

Nome do monitor	Gravidade	Descrição do monitor	Ação corretiva
Temperatura do interruptor do MetroCluster anormal	CRÍTICO	O sensor de temperatura no interruptor do canal de fibra comunicou uma temperatura anormal.	1) verificar o estado de funcionamento dos sensores de temperatura no contactor de memorização, utilizando o comando "interruptor de memorização indicar -refrigeração". 2) Verifique se o interruptor está operando sob condições de temperatura recomendadas.
Falha no Heartbeat do processador de serviço	INFORMATIVO	Esta mensagem ocorre quando o ONTAP não recebe um sinal de "heartbeat" esperado do processador de serviço (SP). Junto com esta mensagem, os arquivos de log do SP serão enviados para depuração. O ONTAP repõe o SP para tentar restaurar a comunicação. O SP estará indisponível por até dois minutos enquanto ele for reinicializado.	Entre em Contato com o suporte técnico da NetApp.

Nome do monitor	Gravidade	Descrição do monitor	Ação corretiva
O Heartbeat do processador de serviço parou	AVISO	Esta mensagem ocorre quando o ONTAP não está mais recebendo batimentos cardíacos do processador de Serviço (SP). Dependendo do design do hardware, o sistema pode continuar fornecendo dados ou pode determinar o desligamento para evitar perda de dados ou danos ao hardware. O sistema continua a fornecer dados, mas como o SP pode não estar funcionando, o sistema não pode enviar notificações de dispositivos inativos, erros de inicialização ou erros de autoteste de inicialização (POST) de firmware aberto. Se o seu sistema estiver configurado para o fazer, ele gera e transmite uma mensagem AutoSupport (ou "Call Home") para o suporte técnico da NetApp e para os destinos configurados. A entrega bem-sucedida de uma mensagem AutoSupport melhora significativamente a determinação e resolução de problemas.	Se o sistema tiver desligado, tente um ciclo de alimentação rígido: Puxe o controlador para fora do chassis, empurre-o de volta e, em seguida, ligue o sistema. Entre em Contato com o suporte técnico da NetApp se o problema persistir após o ciclo de energia ou para qualquer outra condição que possa justificar atenção.

[Voltar ao topo](#)

Mais informações

- ["Visualização e ausência de alertas"](#)

Notificação usando Webhooks

Webhooks permitem que os usuários enviem notificações de alerta para vários aplicativos usando um canal de webhook personalizado.

Muitos aplicativos comerciais suportam webhooks como uma interface de entrada padrão, por exemplo: Slack, PagerDuty, Teams e discord todos suportam webhooks. Ao suportar um canal de webhook genérico e

personalizável, o Data Infrastructure Insights pode suportar muitos desses canais de entrega. Informações sobre webhooks podem ser encontradas nesses sites de aplicativos. Por exemplo, o Slack fornece "[este guia útil](#)".

Você pode criar vários canais de webhook, cada canal direcionado para um propósito diferente; aplicativos separados, destinatários diferentes, etc.

A instância do canal webhook é composta pelos seguintes elementos:

Nome	Nome único
URL	URL de destino do webhook, incluindo o prefixo <i>http://</i> ou <i>https://</i> junto com os parâmetros de url
Método	GET, POST - o padrão é POST
Cabeçalho personalizado	Especifique aqui quaisquer linhas de cabeçalho personalizadas
Corpo da mensagem	Coloque o corpo da sua mensagem aqui
Parâmetros de alerta predefinidos	Lista os parâmetros padrão para o webhook
Parâmetros e segredos personalizados	Parâmetros e segredos personalizados permitem que você adicione parâmetros exclusivos e elementos seguros, como senhas

Criando um Webhook

Para criar um webhook do Data Infrastructure Insights, vá para **Admin > notificações** e selecione a guia **Webhooks**.

A imagem a seguir mostra um exemplo de webhook configurado para o Slack:

Edit a Webhook

Name

Slack Test

Template Type

Slack

URL

https://hooks.slack.com/services/<token>

Method

POST

Custom Header

Content-Type: application/json
Accept: application/json

Message Body

```
{
  "blocks": [
    {
      "type": "section",
      "text": {
        "type": "mrkdwn",
        "text": "**Cloud Insights Alert - %%alertid%%**  
Severity - *%%severity%%*"
      }
    }
  ],
}
```

Cancel

Test Webhook

Save Webhook

Introduza as informações adequadas para cada um dos campos e clique em "Guardar" quando terminar.

Você também pode clicar no botão "testar Webhook" para testar a conexão. Observe que isso enviará o "corpo da mensagem" (sem substituições) para a URL definida de acordo com o método selecionado.

Os webhooks do Data Infrastructure Insights incluem vários parâmetros padrão. Além disso, você pode criar seus próprios parâmetros personalizados ou segredos.

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](#)

Parâmetros: O que são e como os utilizo?

Os parâmetros de alerta são valores dinâmicos preenchidos por alerta. Por exemplo, o parâmetro %%TriggeredOn%% será substituído pelo objeto no qual o alerta foi acionado.

Note que nesta seção, as substituições são *não* executadas ao clicar no botão "testar Webhook"; o botão envia uma carga útil que mostra as substituições %, mas não as substitui por dados.

Parâmetros e segredos personalizados

Nesta seção, você pode adicionar quaisquer parâmetros personalizados e / ou segredos que desejar. Por razões de segurança, se um segredo é definido, apenas o criador do webhook pode modificar este canal do webhook. É somente leitura para os outros. Você pode usar segredos em URL/cabeçalhos como `%%<secret_name>%%`.

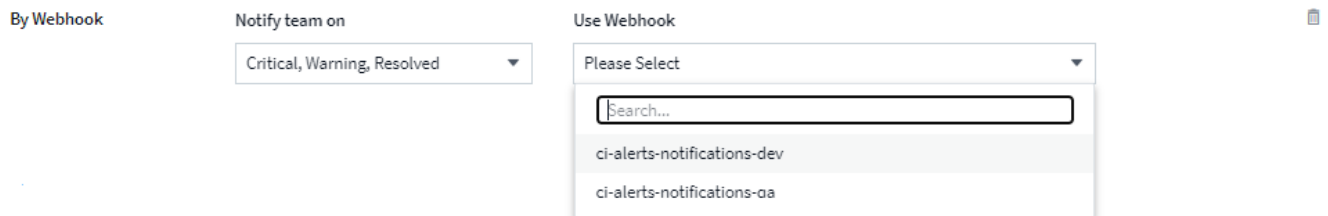
Página de Lista de webhooks

Na página da lista Webhooks, são exibidos os campos Nome, criado por, criado em, Status, seguro e último relatório.

Escolhendo a notificação do Webhook em um monitor

Para escolher a notificação do webhook em um "monitorar", vá para **Alertas > Gerenciar monitores** e selecione o monitor desejado ou adicione um novo monitor. Na seção *Configurar notificações da equipe*, escolha *Webhook* como o método de entrega. Selecione os níveis de alerta (crítico, Aviso, resolvido) e, em seguida, escolha o webhook desejado.

3 Set up team notification(s) (alert your team via email, or Webhook)



Exemplos de webhook:

Webhooks "Folga" para Webhooks para Webhooks "PagerDuty" "Equipas" para "Discórdia"

Trabalhando com Anotações

Definir anotações

Ao personalizar o Data Infrastructure Insights para rastrear dados para seus requisitos corporativos, você pode definir notas especializadas, chamadas de anotações e atribuí-las aos seus ativos.

Você pode atribuir anotações a ativos com informações como fim de vida útil do ativo, data center, local de criação, camada de storage ou nível de serviço de volume.

O uso de anotações para ajudar a monitorar seu ambiente inclui as seguintes tarefas de alto nível:

- Criar ou editar definições para todos os tipos de anotação.
- Exibindo páginas de ativos e associando cada ativo com uma ou mais anotações.

Por exemplo, se um ativo estiver sendo alugado e o leasing expirar dentro de dois meses, você pode querer aplicar uma anotação de fim de vida útil ao ativo. Isso ajuda a evitar que outros usem esse ativo

por um tempo prolongado.

- Criando regras para aplicar automaticamente anotações a vários ativos do mesmo tipo.
- Filtrar ativos por suas anotações.

Tipos de anotação predefinidos

O Data Infrastructure Insights fornece alguns tipos de anotação padrão. Essas anotações podem ser usadas para filtrar ou agrupar dados.

Você pode associar ativos a tipos de anotação padrão, como os seguintes:

- Ciclo de vida do ativo, como aniversário, pôr do sol ou fim da vida
- Informações de localização sobre um dispositivo, como data center, prédio ou piso
- Classificação de ativos, como por qualidade (níveis), por dispositivos conectados (nível de switch) ou por nível de serviço
- Status, como quente (alta utilização)

A tabela a seguir lista os tipos de anotação fornecidos pelo Data Infrastructure Insights.

Tipos de anotação	Descrição	Tipo
Alias	Nome amigável para um recurso	Texto
Grupo de recursos de computação	Atribuição de grupo usada pelo coletor de dados de sistemas de arquivos Host e VM	Lista
Data center	Localização física	Lista
Quente	Dispositivos em uso intensivo regularmente ou no limite da capacidade	Booleano
Nota	Comentários associados a um recurso	Teste
Nível de serviço	Um conjunto de níveis de serviço compatíveis que você pode atribuir a recursos. Fornece uma lista de opções ordenadas para volumes internos, qtree e volumes. Edite níveis de serviço para definir políticas de desempenho para diferentes níveis.	Lista
Pôr do sol	Limiar definido após o qual não é possível efetuar novas alocações para esse dispositivo. Útil para migrações planejadas e outras alterações de rede pendentes.	Data
Nível do interruptor	Opções predefinidas para configurar categorias para switches. Normalmente, essas designações permanecem durante a vida útil do dispositivo, embora você possa editá-las. Disponível apenas para interruptores.	Lista
Nível	Pode ser usado para definir diferentes níveis de serviço em seu ambiente. As camadas podem definir o tipo de nível, como a velocidade necessária (por exemplo, ouro ou prata). Esse recurso está disponível somente em volumes internos, qtrees, matrizes de armazenamento, pools de armazenamento e volumes.	Lista

Gravidade da violação	Classificação (por exemplo, maior) de uma violação (por exemplo, portas de host ausentes ou redundância ausente), em uma hierarquia de maior a menor importância.	Lista
-----------------------	---	-------



Alias, Data Center, Hot, Service Level, Sunset, Switch Level, Tier, and violation severity são anotações no nível do sistema, que você não pode excluir ou renomear; você pode alterar apenas os valores atribuídos.

Criar anotações personalizadas

Usando anotações, você pode adicionar dados personalizados específicos de negócios que correspondem às necessidades da sua empresa aos ativos. Embora o Data Infrastructure Insights forneça um conjunto de anotações padrão, você pode descobrir que deseja exibir dados de outras maneiras. Os dados em anotações personalizadas complementam os dados do dispositivo já coletados, como fabricante de armazenamento, volumes de número e estatísticas de desempenho. Os dados que você adiciona usando anotações não são descobertos pelo Data Infrastructure Insights.

Passos

1. No menu Data Infrastructure Insights, clique em **Manage > Annotations**.

A página Anotações apresenta a lista de anotações.

2. Clique em * Adicionar*
3. Introduza um **Nome** e **Descrição** da anotação.

Pode introduzir até 255 caracteres nestes campos.

4. Clique em **Type** e, em seguida, selecione uma das seguintes opções que representa o tipo de dados permitidos nesta anotação:

Tipos de anotação

Booleano

Cria uma lista suspensa com as opções de sim e não. Por exemplo, a anotação "Direct Attached" é booleana.

Data

Isso cria um campo que contém uma data. Por exemplo, se a anotação for uma data, selecione esta.

Lista

Cria uma das seguintes opções:

- Uma lista fixa suspensa

Quando outros estão atribuindo esse tipo de anotação em um dispositivo, eles não podem adicionar mais valores à lista.

- Uma lista suspensa flexível

Se selecionar a opção Adicionar novos valores em tempo real ao criar esta lista, quando outros estiverem a atribuir este tipo de anotação num dispositivo, poderão adicionar mais valores à lista.

Número

Cria um campo onde o utilizador que atribui a anotação pode introduzir um número. Por exemplo, se o tipo de anotação for "Floor" (Piso), o utilizador pode selecionar o valor Type (tipo de valor) de "Number" (número) e introduzir o número do piso.

Texto

Cria um campo que permite texto de forma livre. Por exemplo, pode introduzir "Idioma" como tipo de anotação, selecionar "texto" como tipo de valor e introduzir um idioma como valor.



Depois de definir o tipo e guardar as alterações, não pode alterar o tipo da anotação. Se você precisar alterar o tipo, você terá que excluir a anotação e criar uma nova.

1. Se selecionar List (Lista) como tipo de anotação, faça o seguinte:
 - a. Selecione **Adicionar novos valores em tempo real** se quiser a capacidade de adicionar mais valores à anotação quando estiver em uma página de ativo, o que cria uma lista flexível.

Por exemplo, suponha que você esteja em uma página de ativo e o ativo tenha a anotação Cidade com os valores Detroit, Tampa e Boston. Se você selecionou a opção **Adicionar novos valores em tempo real**, você pode adicionar valores adicionais a Cidade como São Francisco e Chicago diretamente na página do ativo em vez de ter que ir para a página Anotações para adicioná-los. Se não selecionar esta opção, não pode adicionar novos valores de anotação ao aplicar a anotação; isto cria uma lista fixa.

- b. Insira um valor e uma descrição nos campos **valor** e **Descrição**.
- c. Clique em * Adicionar * para adicionar valores adicionais.
- d. Clique no ícone Lixeira para excluir um valor.

2. Clique em **Salvar**

As suas anotações aparecem na lista na página Anotações.

Depois de terminar

Na IU, a anotação está disponível imediatamente para utilização.

Usando anotações

Você cria anotações e as atribui a ativos que monitora. Anotações são anotações que fornecem informações sobre um ativo, como local físico, fim de vida útil, camada de storage ou níveis de serviço de volume.

Definir anotações

Usando anotações, você pode adicionar dados personalizados específicos de negócios que correspondem às necessidades da sua empresa aos ativos. Embora o Data Infrastructure Insights forneça um conjunto de anotações padrão, como ciclo de vida do ativo (aniversário ou fim da vida útil), localização do prédio ou do data center e nível, você pode achar que deseja exibir dados de outras maneiras.

Os dados em anotações personalizadas complementam os dados do dispositivo já coletados, como fabricante do switch, número de portas e estatísticas de desempenho. Os dados que você adiciona usando anotações não são descobertos pelo Data Infrastructure Insights.

Antes de começar

- Liste qualquer terminologia do setor à qual os dados do ambiente devem ser associados.
- Listar a terminologia corporativa à qual os dados do ambiente devem ser associados.
- Identifique quaisquer tipos de anotação padrão que você possa ser capaz de usar.
- Identifique quais anotações personalizadas você precisa criar. Você precisa criar a anotação antes que ela possa ser atribuída a um ativo.

Utilize os seguintes passos para criar uma anotação.

Passos

1. No menu Data Infrastructure Insights, clique em **Observability > Enrich > Annotations**
2. Clique em * Annotation* para criar uma nova anotação.
3. Introduza um Nome, Descrição e tipo para a nova anotação.

Por exemplo, digite o seguinte para criar uma anotação de texto que define a localização física de um ativo no Data Center 4:

- Introduza um nome para a anotação, tal como "Location" (localização)
- Introduza uma descrição do que a anotação está a descrever, tal como "a localização física é o Data Center 4"
- Introduza o 'tipo' da anotação que é, como por exemplo "texto".

Atribuir manualmente anotações a ativos

A atribuição de anotações a ativos ajuda a classificar, agrupar e gerar relatórios sobre ativos de maneiras relevantes para o seu negócio. Embora seja possível atribuir anotações a ativos de um tipo específico automaticamente usando regras de anotação, você pode atribuir anotações a um ativo individual usando sua página de ativo.

Antes de começar

- Tem de ter criado a anotação que pretende atribuir.

Passos

1. Faça login no seu ambiente Data Infrastructure Insights.
2. Localize o ativo ao qual pretende aplicar a anotação.
 - Você pode localizar ativos consultando, escolhendo um widget dashboard ou pesquise. Quando tiver localizado o ativo desejado, clique no link para abrir a página de destino do ativo.
3. Na página de ativos, na seção dados do usuário, clique em * Annotation*.
4. A caixa de diálogo Adicionar anotação é exibida.
5. Selecione uma anotação na lista.
6. Clique em valor e efetue uma das seguintes ações, dependendo do tipo de anotação selecionado:
 - Se o tipo de anotação for lista, data ou Booleano, selecione um valor na lista.
 - Se o tipo de anotação for texto, introduza um valor.
7. Clique em **Salvar**.

Se pretender alterar o valor da anotação depois de a atribuir, clique no campo de anotação e selecione um valor diferente. Se a anotação for do tipo de lista para o qual a opção *Add new values on the fly* está

selecionada, você pode digitar um novo valor além de selecionar um valor existente.

Atribuir anotações usando regras de anotação

Para atribuir automaticamente anotações a ativos com base nos critérios definidos, configure regras de anotação. O Data Infrastructure Insights atribui as anotações aos ativos com base nessas regras. O Data Infrastructure Insights também fornece duas regras de anotação padrão, que você pode modificar para atender às suas necessidades ou remover se não quiser usá-las.

Criando regras de anotação

Como alternativa à aplicação manual de anotações a ativos individuais, você pode aplicar automaticamente anotações a vários ativos usando regras de anotação. Anotações definidas manualmente em páginas de ativos individuais têm precedência sobre anotações baseadas em regras quando o Insight avalia as regras de anotação.

Antes de começar

Você deve ter criado uma consulta para a regra de anotação.

Sobre esta tarefa

Embora possa editar os tipos de anotação enquanto cria as regras, deve ter definido os tipos com antecedência.

Passos

1. Clique em **Manage > Annotation rules** (gerir > regras de anotação)

A página regras de anotação exibe a lista de regras de anotação existentes.

2. Clique em Adicionar*.

3. Faça o seguinte:

- a. Na caixa **Nome**, insira um nome exclusivo que descreva a regra.

Este nome aparecerá na página regras de anotação.

- b. Clique em **consulta** e selecione a consulta que é usada para aplicar a anotação aos ativos.

- c. Clique em **Annotation** e selecione a anotação que pretende aplicar.

- d. Clique em **value** e selecione um valor para a anotação.

Por exemplo, se você escolher aniversário como anotação, especifique uma data para o valor.

- e. Clique em **Salvar**

- f. Clique em **Executar todas as regras** se quiser executar todas as regras imediatamente; caso contrário, as regras são executadas em um intervalo programado regularmente.

Criando regras de anotação

Pode utilizar regras de anotação para aplicar automaticamente anotações a vários ativos com base nos critérios definidos. O Data Infrastructure Insights atribui as anotações aos ativos com base nessas regras. Anotações definidas manualmente em páginas de ativos individuais têm precedência sobre anotações baseadas em regras quando o Cloud Insight avalia as regras de anotação.

Antes de começar

Você deve ter criado uma consulta para a regra de anotação.

Passos

1. No menu Data Infrastructure Insights, clique em **Manage > Annotation rules**.
2. Clique em * regra* para adicionar uma nova regra de anotação.

A caixa de diálogo Adicionar regra é exibida.

3. Faça o seguinte:

- a. Na caixa **Nome**, insira um nome exclusivo que descreva a regra.

O nome aparece na página regras de anotação.

- b. Clique em **consulta** e selecione a consulta que o Data Infrastructure Insights usa para identificar os ativos aos quais a anotação se aplica.
- c. Clique em **Annotation** e selecione a anotação que pretende aplicar.
- d. Clique em **value** e selecione um valor para a anotação.

Por exemplo, se você escolher aniversário como anotação, especifique uma data para o valor.

- e. Clique em **Salvar**

- f. Clique em **Executar todas as regras** se quiser executar todas as regras imediatamente; caso contrário, as regras são executadas em um intervalo programado regularmente.



Em um ambiente de Insights de infraestrutura de dados grande, você pode notar que a execução de regras de anotação parece demorar um pouco para ser concluída. Isso ocorre porque o indexador é executado primeiro e deve ser concluído antes de executar as regras. O indexador é o que dá ao Data Infrastructure Insights a capacidade de pesquisar ou filtrar por objetos e contadores novos ou atualizados nos dados. O mecanismo de regras aguarda até que o indexador conclua sua atualização antes de aplicar as regras.

Modificar regras de anotação

É possível modificar uma regra de anotação para alterar o nome da regra, sua anotação, o valor da anotação ou a consulta associada à regra.

Passos

1. No menu Data Infrastructure Insights, clique em **Manage > Annotation rules**.

A página regras de anotação exibe a lista de regras de anotação existentes.

2. Localize a regra de anotação que deseja modificar.

Pode filtrar as regras de anotação introduzindo um valor na caixa de filtro ou clicar num número de página para navegar pelas regras de anotação por página.

3. Clique no ícone de menu da regra que você deseja modificar.
4. Clique em **Editar**

A caixa de diálogo Editar regra é exibida.

5. Modifique o nome, anotação, valor ou consulta da regra de anotação.

Alterar a ordem das regras

As regras de anotação são processadas a partir da parte superior da lista de regras para a parte inferior. Para alterar a ordem em que uma regra é processada, faça o seguinte:

Passos

1. Clique no ícone do menu da regra que deseja mover.
2. Clique em **mover para cima** ou **mover para baixo** conforme necessário até que a regra apareça no local desejado.

Observe que ao executar várias regras que atualizam a mesma anotação em um ativo, a primeira regra (como executada de cima para baixo) aplica a anotação e atualiza o ativo, então a segunda regra se aplica, mas não altera nenhuma anotação que já foi definida pela regra anterior.

Eliminar regras de anotação

Pode pretender eliminar regras de anotação que já não são utilizadas.

Passos

1. No menu Data Infrastructure Insights, clique em **Manage > Annotation rules**.

A página regras de anotação exibe a lista de regras de anotação existentes.

2. Localize a regra de anotação que deseja excluir.

Pode filtrar as regras de anotação introduzindo um valor na caixa de filtro ou clicar num número de página para navegar pelas regras de anotação por página.

3. Clique no ícone de menu da regra que você deseja excluir.
4. Clique em **Excluir**

Uma mensagem de confirmação é exibida, solicitando se deseja excluir a regra.

5. Clique em **OK**

Importar anotações

O Data Infrastructure Insights inclui uma API para importar anotações ou aplicativos de um arquivo CSV e atribuí-los a objetos especificados.



A API Data Infrastructure Insights está disponível em **Data Infrastructure Insights Premium Edition**.

A importar

Os links **Admin > API Access** contêm "[documentação](#)" para a API **Assets/Import**. Esta documentação contém informações sobre o formato de arquivo .CSV.

ASSETS.import

PUT /assets/import Import assets from a CSV file.

Import annotations and applications from the given CSV file. The format of the CSV file is following:

```
Project
<Object Type Value 1>, <Object Name or Key 1>, <Annotation Value> [, <Annotation Type> ...] [, <Application>] [, <Tenant>] [, <Line_Of_Business>] [, <Business_Unit>] [,
<Project>]
<Object Type Value 2>, <Object Name or Key 2>, <Annotation Value> [, <Annotation Type> ...] [, <Application>] [, <Tenant>] [, <Line_Of_Business>] [, <Business_Unit>] [,
<Project>]
<Object Type Value 3>, <Object Name or Key 3>, <Annotation Value> [, <Annotation Type> ...] [, <Application>] [, <Tenant>] [, <Line_Of_Business>] [, <Business_Unit>] [,
<Project>]
...
<Object Type Value N>, <Object Name or Key N>, <Annotation Value> [, <Annotation Type> ...] [, <Application>] [, <Tenant>] [, <Line_Of_Business>] [, <Business_Unit>] [,
<Project>]
```

Formato de arquivo .CSV

O formato geral do arquivo CSV é o seguinte. A primeira linha do arquivo define os campos de importação e especifica a ordem dos campos. Isto é seguido por linhas separadas para cada anotação ou aplicação. Não é necessário definir todos os campos. No entanto, as linhas de anotação subsequentes devem seguir a mesma ordem que a linha de definição.

```
[Object Type] , [Object Name or ID] , Annotation Type [, Annotation
Type, ...] [, Application] [, Tenant] [, Line_Of_Business] [,
Business_Unit] [, Project]
```

Consulte a Documentação da API para obter exemplos de arquivos .CSV.

Você pode importar e atribuir anotações de um arquivo .CSV de dentro do próprio Swagger da API. Basta escolher o arquivo a ser usado e clicar no botão *execute*:

Parameters Cancel

No parameters

Request body multipart/form-data

CSV file to import

data
string(\$binary) Choose File No file chosen

Execute Clear

Responses

Comportamento de importação

Durante a operação de importação, os dados são adicionados, mesclados ou substituídos, dependendo dos objetos e tipos de objetos que estão sendo importados. Durante a importação, tenha em mente os seguintes comportamentos.

- Adiciona uma anotação ou aplicação se não existir nenhuma com o mesmo nome no sistema de destino.
- Mescla uma anotação se o tipo de anotação for uma lista e existir uma anotação com o mesmo nome no sistema de destino.
- Substitui uma anotação se o tipo de anotação for diferente de uma lista e existir uma anotação com o mesmo nome no sistema de destino.

Nota: Se existir uma anotação com o mesmo nome, mas com um tipo diferente no sistema de destino, a importação falhará. Se os objetos dependerem da anotação com falha, esses objetos podem mostrar informações incorretas ou indesejadas. Você deve verificar todas as dependências de anotação depois que a operação de importação estiver concluída.

- Se um valor de anotação estiver vazio, essa anotação será removida do objeto. Anotações herdadas não são afetadas.
- Os valores de anotação do tipo de data devem ser passados como tempo unix em milissegundos.
- Ao anotar volumes ou volumes internos, o nome do objeto é uma combinação de nome de armazenamento e nome do volume usando o separador "→". Por exemplo: <Storage Name>→<Volume Name>
- Se um nome de objeto contiver uma vírgula, o nome inteiro deve estar em aspas duplas. Por exemplo: "NetApp1,NetApp2"→023F
- Ao anexar anotações a storages, switches e portas, a coluna 'Application' será ignorada.
- O locatário, Line_of_Business, Business_Unit e/ou Project faz uma entidade de negócio. Tal como acontece com todas as entidades empresariais, qualquer um dos valores pode estar vazio.

Os seguintes tipos de objeto podem ser anotados.

TIPO DE OBJETO	NOME OU CHAVE
Host	id --><id> ou <Name> ou <IP>
VM	id --><id> ou <Name>
StoragePool	id --><id> ou <Storage Name> → Nome do conjunto de armazenamento de dados
Internalvolume	id --><id> ou <Storage Name> → Nome do volume Interno do cliente
Volume	id --><id> ou <Storage Name> --><Volume Name>
Armazenamento	id --><id> ou <Name> ou <IP>
Interrutor	id --><id> ou <Name> ou <IP>
Porta	id --><id> ou <WWN>
Qtree	id --><id> ou <Storage Name> → Nome do volume interno>> --><Qtree Name>
Partilhar	id --><id> ou <Storage Name> → Nome do volume interno do cliente> --><Share Name> --><Protocol>[→ Nome do cliente (opcional no caso de Qtree predefinido)>]

Trabalhar com aplicações

Rastreamento do uso de ativos por aplicativo

Antes de rastrear dados associados aos aplicativos em execução no locatário, primeiro é necessário definir esses aplicativos e associá-los aos ativos apropriados. Você pode associar aplicativos aos seguintes ativos: Hosts, máquinas virtuais, volumes, volumes internos, qtrees, compartilhamentos e hipervisores.

Este tópico fornece um exemplo de rastreamento do uso de máquinas virtuais que a equipe de marketing usa para seu e-mail do Exchange.

Talvez você queira criar uma tabela semelhante à seguinte para identificar aplicativos usados no locatário e observar o grupo ou a unidade de negócios usando cada aplicativo.

Locatário	Linha de negócio	Unidade de negócio	Projeto	Aplicações
NetApp	Storage de dados	Legal	Patentes	Oracle Identity Manager, Oracle On Demand, PatentWiz
NetApp	Storage de dados	Marketing	Eventos de vendas	Exchange, Oracle Shared Database, Blastoff Event Planner

A tabela mostra que a equipe de marketing usa o aplicativo Exchange. Queremos acompanhar a utilização da máquina virtual para o Exchange, para que possamos prever quando precisaremos adicionar mais armazenamento. Podemos associar o aplicativo Exchange a todas as máquinas virtuais de Marketing:

1. Crie um aplicativo chamado *Exchange*
2. Vá para **consultas > Nova consulta** para criar uma nova consulta para máquinas virtuais (ou selecione uma consulta de VM existente, se aplicável).

Supondo que as VMs da equipe de Marketing tenham um nome contendo a string "mkt", crie sua consulta para filtrar o nome da VM para "mkt".

3. Selecione as VMs.
4. Associe as VMs ao aplicativo *Exchange* usando **ações em massa > Adicionar aplicativos**.
5. Selecione o aplicativo desejado e clique em **Salvar**.
6. Quando terminar, **Salvar** a consulta.

Criando aplicativos

Para rastrear dados associados a aplicativos específicos em execução no locatário, é possível definir os aplicativos no Data Infrastructure Insights.

Antes de começar

Se você quiser associar o aplicativo a uma entidade de negócios, você deve criar a entidade de negócios antes de definir o aplicativo.

Sobre esta tarefa

O Data Infrastructure Insights permite rastrear dados de ativos associados a aplicativos para coisas como relatórios de uso ou custos.

Passos

1. No menu Data Infrastructure Insights, clique em **observabilidade > Enrich > Applications**. Selecione a caixa de diálogo Adicionar aplicativo é exibida.
2. Introduza um nome exclusivo para a aplicação.

3. Selecione uma prioridade para a aplicação.
4. Clique em **Salvar**.

Depois de definir um aplicativo, ele pode ser atribuído aos ativos.

Atribuindo aplicativos aos ativos

Este procedimento atribui o aplicativo a um host como um exemplo. Você pode atribuir host, máquina virtual, volume ou volumes internos a um aplicativo.

Passos

1. Localize o ativo ao qual você deseja atribuir ao aplicativo:
2. Clique em **consultas > Nova consulta** e procure por Host.
3. Clique na caixa de verificação à esquerda do anfitrião que pretende associar à aplicação.
4. Clique em **ações em massa > Adicionar aplicativo**.
5. Selecione a aplicação à qual está a atribuir o ativo.

Quaisquer novos aplicativos que você atribuir substituem quaisquer aplicativos no ativo que foram derivados de outro ativo. Por exemplo, os volumes herdam aplicativos de hosts e, quando novos aplicativos são atribuídos a um volume, o novo aplicativo tem precedência sobre o aplicativo derivado.



Para ambientes com grandes quantidades de ativos relacionados, a herança de atribuições de aplicativos para esses ativos pode levar vários minutos. Por favor, aguarde mais tempo para que a herança ocorra se você tiver muitos ativos relacionados.

Depois de terminar

Depois de atribuir o host ao aplicativo, você pode atribuir os ativos restantes ao aplicativo. Para acessar a página de destino do aplicativo, clique em **Gerenciar > aplicativo** e selecione o aplicativo que você criou.

Resolução automática do dispositivo

Visão geral da resolução automática do dispositivo

Você precisa identificar todos os dispositivos que deseja monitorar com o Data Infrastructure Insights. A identificação é necessária para acompanhar com precisão o desempenho e o inventário no seu inquilino. Normalmente, a maioria dos dispositivos descobertos no seu localatário são identificados através de *Resolução automática de dispositivos*.

Depois de configurar coletores de dados, os dispositivos no localatário, incluindo switches, arrays de armazenamento e sua infraestrutura virtual de hipervisores e VMs, são identificados. No entanto, isso normalmente não identifica 100% dos dispositivos no localatário.

Depois que os dispositivos do tipo coletor de dados tiverem sido configurados, a melhor prática é aproveitar as regras de resolução do dispositivo para ajudar a identificar os dispositivos desconhecidos restantes no seu localatário. A resolução do dispositivo pode ajudá-lo a resolver dispositivos desconhecidos como os seguintes tipos de dispositivos:

- Hosts físicos

- Storage arrays
- Fitas

Os dispositivos que permanecem como desconhecidos após a resolução do dispositivo são considerados dispositivos genéricos, que também podem ser exibidos em consultas e em painéis.

As regras criadas, por sua vez, identificarão automaticamente novos dispositivos com atributos semelhantes à medida que forem adicionados ao seu ambiente. Em alguns casos, a resolução do dispositivo também permite a identificação manual ignorando as regras de resolução do dispositivo para dispositivos não descobertos no Data Infrastructure Insights.

A identificação incompleta dos dispositivos pode resultar em problemas, incluindo:

- Caminhos incompletos
- Conexões multipath não identificadas
- A incapacidade de agrupar aplicações
- Visualizações de topologia imprecisas
- Dados imprecisos no Data warehouse e relatórios

A funcionalidade de resolução do dispositivo (gerir > Resolução do dispositivo) inclui os seguintes separadores, cada um dos quais desempenha um papel no planejamento da resolução do dispositivo e na visualização dos resultados:

- **O Fibre Channel Identify** contém uma lista de WWNs e informações de porta de dispositivos Fibre Channel que não foram resolvidos por meio da resolução automática do dispositivo. A guia também identifica a porcentagem de dispositivos que foram identificados.
- **Identificação de endereço IP** contém uma lista de dispositivos que acessam compartilhamentos CIFS e compartilhamentos NFS que não foram identificados por meio da resolução automática do dispositivo. A guia também identifica a porcentagem de dispositivos que foram identificados.
- **Regras de resolução automática** contém a lista de regras que são executadas ao executar a resolução do dispositivo Fibre Channel. Estas são regras criadas para resolver dispositivos Fibre Channel não identificados.
- **Preferências** fornece opções de configuração que você usa para personalizar a resolução do dispositivo para o seu ambiente.

Antes de começar

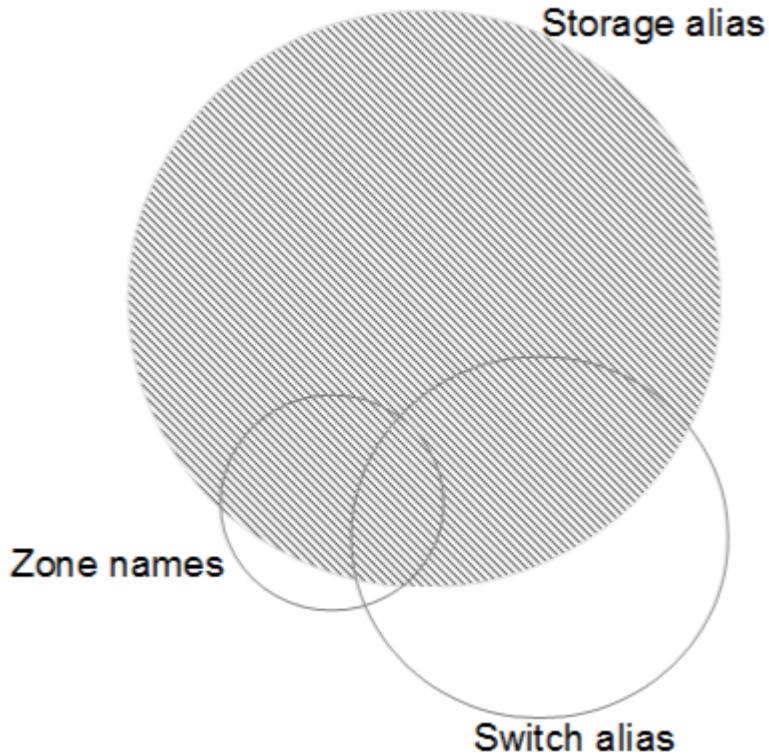
Você precisa saber como seu ambiente é configurado antes de definir as regras para identificar dispositivos. Quanto mais você souber sobre seu ambiente, mais fácil será identificar dispositivos.

Você precisa responder perguntas semelhantes às seguintes para ajudá-lo a criar regras precisas:

- Seu ambiente tem padrões de nomenclatura para zonas ou hosts e qual porcentagem deles são precisos?
- O seu ambiente usa um alias de switch ou alias de armazenamento e eles correspondem ao nome do host?
- Com que frequência os esquemas de nomenclatura mudam no seu inquilino?
- Houve alguma aquisição ou fusão que introduziu diferentes esquemas de nomeação?

Depois de analisar seu ambiente, você deve ser capaz de identificar quais padrões de nomenclatura existem que você pode esperar encontrar com confiabilidade. As informações coletadas podem ser representadas

graficamente em uma figura semelhante à seguinte:



Neste exemplo, o maior número de dispositivos é representado de forma confiável por aliases de armazenamento. As regras que identificam hosts usando aliases de armazenamento devem ser escritas primeiro, as regras que usam aliases de switch devem ser escritas em seguida e as últimas regras criadas devem usar aliases de zona. Devido à sobreposição do uso de aliases de zona e aliases de switch, algumas regras de alias de armazenamento podem identificar dispositivos adicionais, deixando menos regras necessárias para aliases de zona e aliases de switch.

Passos para identificar dispositivos

Normalmente, você usaria um fluxo de trabalho semelhante ao seguinte para identificar dispositivos no local. A identificação é um processo iterativo e pode exigir várias etapas de Planejamento e regras de refino.

- Ambiente de pesquisa
- Regras do plano
- Criar/rever regras
- Reveja os resultados
- Crie regras adicionais ou identifique dispositivos manualmente
- Concluído



Se você tiver dispositivos não identificados (também conhecidos como dispositivos desconhecidos ou genéricos) em seu local e, posteriormente, configurar uma fonte de dados que identifique esses dispositivos ao fazer polling, eles não serão mais exibidos ou contados como dispositivos genéricos.

Relacionado: "Criando regras de resolução de dispositivo" "Resolução do dispositivo Fibre Channel" "Resolução do dispositivo IP" "Definir preferências de resolução do dispositivo"

Regras de resolução do dispositivo

Você cria regras de resolução de dispositivo para identificar hosts, storage e fitas que não são identificadas automaticamente no momento pelo Data Infrastructure Insights. As regras que você cria identificam dispositivos atualmente em seu ambiente e também identificam dispositivos semelhantes à medida que são adicionados ao seu ambiente.

Criando regras de resolução de dispositivo

Quando você cria regras, você começa identificando a origem das informações contra as quais a regra é executada, o método usado para extrair informações e se a pesquisa DNS é aplicada aos resultados da regra.

Fonte utilizada para identificar o dispositivo	* Alias SRM para hosts * alias de armazenamento contendo um nome de host ou fita incorporado * alias de switch contendo um nome de host ou fita incorporado * nomes de zona contendo um nome de host incorporado
Método usado para extrair o nome do dispositivo da origem	* Como está (extraia um nome de um SRM) * delimitadores * expressões regulares
Pesquisa DNS	Especifica se você usa DNS para verificar o nome do host

Você cria regras na guia regras de resolução automática. As etapas a seguir descrevem o processo de criação de regras.

Procedimento

1. Clique em **Manage > Device Resolution** (gerir > Resolução do dispositivo)
2. Na guia **regras de resolução automática**, clique em * regra de host* ou * regra de fita*.

É apresentado o ecrã **Resolution Rule** (regra de resolução).



Clique no link *View Matching Criteria* para obter ajuda e exemplos para criar expressões regulares.

3. Na lista **tipo**, selecione o dispositivo que deseja identificar.

Você pode selecionar *Host* ou *Tape*.

4. Na lista **fonte**, selecione a fonte que deseja usar para identificar o host.

Dependendo da fonte escolhida, o Data Infrastructure Insights exibe a seguinte resposta:

- a. **Zones** lista as zonas e WWN que precisam ser identificadas pelo Data Infrastructure Insights.
- b. **SRM** lista os aliases não identificados que precisam ser identificados pelo Data Infrastructure Insights
- c. **Alias de armazenamento** lista aliases de armazenamento e WWN que precisam ser identificados pelo Data Infrastructure Insights

d. **O alias de switch** lista os aliases de switch que precisam ser identificados pelo Data Infrastructure Insights

5. Na lista **método**, selecione o método que deseja empregar para identificar o host.

Fonte	Método
SRM	Como é, delimitadores, expressões regulares
Alias de armazenamento	Delimitadores, expressões regulares
Alternar alias	Delimitadores, expressões regulares
Zonas	Delimitadores, expressões regulares

- As regras que usam delimitadores exigem os delimitadores e o comprimento mínimo do nome do host. O tamanho mínimo do nome do host é o número de caracteres que o Data Infrastructure Insights deve usar para identificar um host. O Data Infrastructure Insights executa pesquisas de DNS apenas para nomes de host que são longos ou longos.

Para regras que usam delimitadores, a cadeia de caracteres de entrada é tokenizada pelo delimitador e uma lista de candidatos de nome de host é criada fazendo várias combinações do token adjacente. A lista é então classificada, maior para menor. Por exemplo, para um anel de entrada de *vipsnq03_hba3_emc3_12ep0* a lista resultaria no seguinte:

- vipsnq03_hba3_emc3_12ep0
- vipsnq03_hba3_emc3
- hba3 emc3_12ep0
- vipsnq03_hba3
- emc3_12ep0
- hba3_emc3
- vipsnq03
- 12ep0
- emc3
- hba3

- Regras que usam expressões regulares exigem uma expressão regular, o formato e seleção de sensibilidade de casos.

6. Clique em **Executar ar** para executar todas as regras ou clique na seta para baixo no botão para executar a regra que você criou (e quaisquer outras regras que foram criadas desde a última execução completa de ar).

Os resultados da execução de regras são exibidos na guia **FC Identify**.

Iniciar uma atualização automática da resolução do dispositivo

Uma atualização de resolução do dispositivo confirma alterações manuais que foram adicionadas desde a última execução automática completa da resolução do dispositivo. A execução de uma atualização pode ser usada para confirmar e executar apenas as novas entradas manuais feitas na configuração de resolução do dispositivo. Nenhuma resolução completa do dispositivo é executada.

Procedimento

1. Faça login na IU da Web do Data Infrastructure Insights.
2. Clique em **Manage > Device Resolution** (gerir > Resolução do dispositivo)
3. Na tela **Resolução do dispositivo**, clique na seta para baixo no botão **Executar ar**.
4. Clique em **Atualizar** para iniciar a atualização.

Identificação manual assistida por regras

Esse recurso é usado para casos especiais em que você deseja executar uma regra específica ou uma lista de regras (com ou sem um reordenamento único) para resolver hosts, armazenamento e dispositivos de fita desconhecidos.

Antes de começar

Você tem vários dispositivos que não foram identificados e você também tem várias regras que identificaram com êxito outros dispositivos.



Se a origem contiver apenas parte do nome de um host ou dispositivo, use uma regra de expressão regular e formate-a para adicionar o texto em falta.

Procedimento

1. Faça login na IU da Web do Data Infrastructure Insights.
2. Clique em **Manage > Device Resolution** (gerir > Resolução do dispositivo)
3. Clique na guia **Fibre Channel Identify**.

O sistema apresenta os dispositivos juntamente com o respetivo estado de resolução.

4. Selecione vários dispositivos não identificados.
5. Clique em **ações em massa** e selecione **Definir resolução de host** ou **Definir resolução de fita**.

O sistema exibe a tela identificar que contém uma lista de todas as regras que identificaram dispositivos com êxito.

6. Altere a ordem das regras para uma ordem que atenda às suas necessidades.

A ordem das regras é alterada na tela identificar, mas não é alterada globalmente.

7. Selecione o método que atenda às suas necessidades.

O Data Infrastructure Insights executa o processo de resolução do host na ordem em que os métodos aparecem, começando pelos que estão no topo.

Quando as regras aplicáveis são encontradas, os nomes das regras são mostrados na coluna regras e identificados como manual.

Relacionado: ["Resolução do dispositivo Fibre Channel"](#) ["Resolução do dispositivo IP"](#) ["Definir preferências de resolução do dispositivo"](#)

Resolução do dispositivo Fibre Channel

O ecrã Fibre Channel Identify (identificação de canal de fibra) apresenta a WWN e WWPN de dispositivos de canal de fibra cujos anfitriões não foram identificados pela

resolução automática do dispositivo. O ecrã também apresenta quaisquer dispositivos que tenham sido resolvidos pela resolução manual do dispositivo.

Os dispositivos que foram resolvidos por resolução manual contêm um status de *OK* e identificam a regra usada para identificar o dispositivo. Os dispositivos em falta têm um status de *não identificados*. Os dispositivos especificamente excluídos da identificação têm um status de *excluídos*. A cobertura total para identificação de dispositivos está listada nesta página.

Você executa ações em massa selecionando vários dispositivos no lado esquerdo da tela Fibre Channel Identify (identificação de canal de fibra). As ações podem ser executadas em um único dispositivo, passando o Mouse sobre um dispositivo e selecionando os botões *Identify* ou *Unidentify* na extrema direita da lista.

O link *Total Coverage* exibe uma lista do número de dispositivos identificados/número de dispositivos disponíveis para sua configuração:

- Alias SRM
- Alias de armazenamento
- Alternar alias
- Zonas
- Definido pelo utilizador

Adicionar um dispositivo Fibre Channel manualmente

Você pode adicionar manualmente um dispositivo de canal de fibra ao Data Infrastructure Insights usando o recurso *Manual Add* disponível na guia identificação de canal de fibra de resolução do dispositivo. Este processo pode ser usado para pré-identificação de um dispositivo que se espera que seja descoberto no futuro.

Antes de começar

Para adicionar com êxito uma identificação de dispositivo ao sistema, é necessário saber o endereço WWN ou IP e o nome do dispositivo.

Sobre esta tarefa

Pode adicionar manualmente um dispositivo anfitrião, armazenamento, fita ou canal de fibra desconhecido.

Procedimento

1. Faça login na IU da Web do Data Infrastructure Insights
2. Clique em **Manage > Device Resolution** (gerir > Resolução do dispositivo)
3. Clique na guia **Fibre Channel Identify**.
4. Clique no botão **Add**.

É apresentada a caixa de diálogo **Add Device** (Adicionar dispositivo)

5. Introduza o endereço WWN ou IP, o nome do dispositivo e selecione o tipo de dispositivo.

O dispositivo inserido é adicionado à lista de dispositivos na guia identificação de canal de fibra. A regra é identificada como *Manual*.

Importando a identificação do dispositivo Fibre Channel de um arquivo .CSV

Você pode importar manualmente a identificação do dispositivo de canal de fibra para a resolução do dispositivo Data Infrastructure Insights usando uma lista de dispositivos em um arquivo .CSV.

1. Antes de começar

Você deve ter um arquivo .CSV formatado corretamente para importar as identificações do dispositivo diretamente para a resolução do dispositivo. O arquivo .CSV para dispositivos de canal de fibra requer as seguintes informações:

WWN	IP	Nome	Tipo
-----	----	------	------

Os campos de dados devem estar entre aspas, como mostrado no exemplo abaixo.

```
"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"
```



Como prática recomendada, recomenda-se primeiro exportar as informações de identificação do Fibre Channel para um arquivo .CSV, fazer as alterações desejadas nesse arquivo e, em seguida, importar o arquivo de volta para o Fibre Channel Identify. Isso garante que as colunas esperadas estejam presentes e na ordem correta.

Para importar informações de identificação de canal de fibra:

1. Faça login na IU da Web do Data Infrastructure Insights.
2. Clique em **Manage > Device Resolution** (gerir > Resolução do dispositivo)
3. Selecione a guia **Fibre Channel Identify**.
4. Clique no botão **Identify > Identify from file**.
5. Navegue até a pasta que contém os arquivos .CSV para importação e selecione o arquivo desejado.

Os dispositivos inseridos são adicionados à lista de dispositivos na guia identificação de canal de fibra. A "regra" é identificada como Manual.

Exportar identificações de dispositivos Fibre Channel para um arquivo .CSV

Você pode exportar identificações de dispositivos Fibre channel existentes para um arquivo .CSV a partir do recurso de resolução de dispositivo Data Infrastructure Insights. Você pode querer exportar uma identificação de dispositivo para que você possa modificá-la e depois importá-la de volta para o Data Infrastructure Insights, onde ela é usada para identificar dispositivos que são semelhantes aos que correspondem originalmente à identificação exportada.

Sobre esta tarefa


Esse cenário pode ser usado quando os dispositivos têm atributos semelhantes que podem ser facilmente editados no arquivo .CSV e, em seguida, importados de volta para o sistema.

Ao exportar uma identificação de dispositivo Fibre Channel para um arquivo .CSV, o arquivo contém as

seguintes informações na ordem mostrada:

WWN	IP	Nome	Tipo
-----	----	------	------

Procedimento

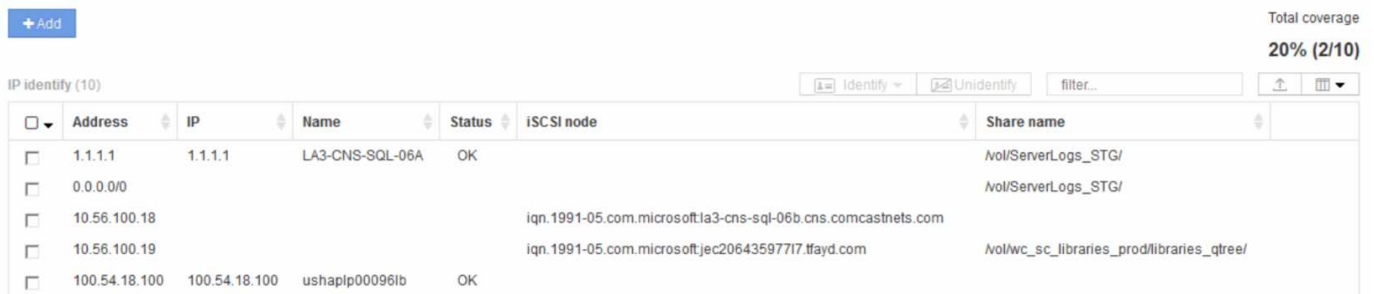
1. Faça login na IU da Web do Data Infrastructure Insights.
2. Clique em **Manage > Device Resolution** (gerir > Resolução do dispositivo)
3. Selecione a guia **Fibre Channel Identify**.
4. Selecione o dispositivo Fibre Channel ou os dispositivos cuja identificação deseja exportar.
5. Clique no botão *Exportar* .

Selecione se deseja abrir o arquivo .CSV ou salvar o arquivo.

Relacionado: ["Resolução do dispositivo IP"](#) ["Criando regras de resolução de dispositivo"](#) ["Definir preferências de resolução do dispositivo"](#)

Resolução do dispositivo IP

O ecrã IP Identify (identificação de IP) apresenta quaisquer compartilhamentos iSCSI e CIFS ou NFS identificados pela resolução automática do dispositivo ou pela resolução manual do dispositivo. Dispositivos não identificados também são exibidos. O ecrã inclui o endereço IP, Nome, Estado, nó iSCSI e nome de partilha para dispositivos. Também é apresentada a percentagem de dispositivos que foram identificados com sucesso.



IP identify (10) Total coverage
20% (2/10)

<input type="checkbox"/>	Address	IP	Name	Status	iSCSI node	Share name
<input type="checkbox"/>	1.1.1.1	1.1.1.1	LA3-CNS-SQL-06A	OK		/vol/ServerLogs_STG/
<input type="checkbox"/>	0.0.0.0/0					/vol/ServerLogs_STG/
<input type="checkbox"/>	10.56.100.18				iqn.1991-05.com.microsoft:ia3-cns-sql-06b.cns.comcastnets.com	
<input type="checkbox"/>	10.56.100.19				iqn.1991-05.com.microsoft:jec20643597717.tfayd.com	/vol/wc_sc_libraries_prod/libraries_qtree/
<input type="checkbox"/>	100.54.18.100	100.54.18.100	ushapp000961b	OK		

Adicionar dispositivos IP manualmente

Você pode adicionar manualmente um dispositivo IP ao Data Infrastructure Insights usando o recurso de adição manual disponível na tela identificação IP.

Procedimento

1. Faça login na IU da Web do Data Infrastructure Insights.
2. Clique em **Manage > Device resolution** (gerir > Resolução do dispositivo)
3. Clique no separador **IP Address Identify** (identificação do endereço IP).
4. Clique no botão **Add**.

É apresentada a caixa de diálogo Adicionar dispositivo

5. Introduza o endereço, o endereço IP e um nome de dispositivo exclusivo.

Resultado

O dispositivo inserido é adicionado à lista de dispositivos na guia identificação de endereço IP.

Importando a identificação do dispositivo IP de um arquivo .CSV

Você pode importar manualmente identificações de dispositivo IP para o recurso Resolução de dispositivo usando uma lista de identificações de dispositivo em um arquivo .CSV.

1. Antes de começar

Você deve ter um arquivo .CSV formatado corretamente para importar as identificações do dispositivo diretamente para o recurso Resolução do dispositivo. O arquivo .CSV para dispositivos IP requer as seguintes informações:

Endereço	IP	Nome
----------	----	------

Os campos de dados devem estar entre aspas, como mostrado no exemplo abaixo.

```
"Address", "IP", "Name"
"ADDRESS6447", "IP6447", "NAME-6447"
"ADDRESS3211", "IP3211", "NAME-3211"
"ADDRESS593", "IP593", "NAME-593"
```



Como prática recomendada, é recomendável primeiro exportar as informações de identificação de endereço IP para um arquivo .CSV, fazer as alterações desejadas nesse arquivo e, em seguida, importar o arquivo de volta para identificação de endereço IP. Isso garante que as colunas esperadas estejam presentes e na ordem correta.

Exportando a identificação do dispositivo IP para um arquivo .CSV

Você pode exportar identificações de dispositivo IP existentes para um arquivo .CSV a partir do recurso de resolução de dispositivo Data Infrastructure Insights. Você pode querer exportar uma identificação de dispositivo para que você possa modificá-la e depois importá-la de volta para o Data Infrastructure Insights, onde ela é usada para identificar dispositivos que são semelhantes aos que correspondem originalmente à identificação exportada.

Sobre esta tarefa


1. Esse cenário pode ser usado quando os dispositivos têm atributos semelhantes que podem ser facilmente editados no arquivo .CSV e, em seguida, importados de volta para o sistema.

Quando você exporta uma identificação de dispositivo IP para um arquivo .CSV, o arquivo contém as seguintes informações na ordem mostrada:

Endereço	IP	Nome
----------	----	------

Procedimento

1. Faça login na IU da Web do Data Infrastructure Insights.
2. Clique em **Manage > Device Resolution** (gerir > Resolução do dispositivo)
3. Selecione a guia **IP Address Identify** (identificação do endereço IP).

4. Selecione o dispositivo IP ou os dispositivos cuja identificação pretende exportar.
5. Clique no botão *Exportar* .

Selecione se deseja abrir o arquivo .CSV ou salvar o arquivo.

Relacionado: ["Resolução do dispositivo Fibre Channel"](#) ["Criando regras de resolução de dispositivo"](#) ["Definir preferências de resolução do dispositivo"](#)

Opções de configuração na guia Preferências

A guia Preferências de resolução do dispositivo permite criar um agendamento de resolução automática, especificar armazenamentos e dispositivos de fita para incluir ou excluir da identificação e definir opções de pesquisa DNS.

Agendamento de resolução automática

Uma programação de resolução automática pode especificar quando a resolução automática do dispositivo é executada:

Opção	Descrição
A cada	Utilize esta opção para executar a resolução automática do dispositivo em intervalos de dias, horas ou minutos.
Todos os dias	Use esta opção para executar a resolução automática do dispositivo diariamente em um horário específico.
Manualmente	Utilize esta opção para executar apenas a resolução automática do dispositivo manualmente.
Em cada mudança de ambiente	Use esta opção para executar a resolução automática do dispositivo sempre que houver uma alteração no ambiente.

Se você especificar *manualmente*, a resolução automática noturna do dispositivo será desativada.

Opções de processamento de DNS

As opções de processamento DNS permitem selecionar as seguintes funcionalidades:

- Quando o processamento de resultados de pesquisa DNS estiver ativado, você poderá adicionar uma lista de nomes DNS a serem anexados a dispositivos resolvidos.
- Você pode selecionar Resolução automática de IPs: Para ativar a resolução automática de host para iniciadores iSCSI e hosts que acessam compartilhamentos NFS usando a pesquisa DNS. Se isso não for especificado, somente a resolução baseada em FC será executada.
- Você pode optar por permitir sublinhados em nomes de host e usar um alias "conetado a" em vez do alias de porta padrão nos resultados.

Incluindo ou excluindo fornecedores específicos de armazenamento e fita

Você pode incluir ou excluir fornecedores específicos de armazenamento e fita para resolução automática. Você pode querer excluir fornecedores específicos se souber, por exemplo, que um host específico se tornará

um host legado e deve ser excluído do seu novo ambiente. Você também pode adicionar novamente fornecedores que você excluiu anteriormente, mas não deseja mais excluídos.



As regras de resolução do dispositivo para fita funcionam apenas para WWNs em que o Fornecedor para essa WWN está definido como *incluído como apenas fita* nas preferências dos fornecedores.

Veja também: "[Exemplos de expressão regular](#)"

Exemplos de expressão regular

Se você selecionou a abordagem de expressão regular como sua estratégia de nomenclatura de origem, você pode usar os exemplos de expressão regular como guias para suas próprias expressões usadas nos métodos de resolução automática Data Infrastructure Insights.

Formatando expressões regulares

Ao criar expressões regulares para a resolução automática do Data Infrastructure Insights, você pode configurar o formato de saída inserindo valores em um campo chamado *FORMAT*.

A configuração padrão é 1, o que significa que um nome de zona que corresponde à expressão regular é substituído pelo conteúdo da primeira variável criada pela expressão regular. Em uma expressão regular, os valores das variáveis são criados por declarações parênteses. Se ocorrerem várias frases entre parênteses, as variáveis são referenciadas numericamente, da esquerda para a direita. As variáveis podem ser usadas no formato de saída em qualquer ordem. Texto constante também pode ser inserido na saída, adicionando-o ao campo *FORMATO*.

Por exemplo, você pode ter os seguintes nomes de zona para esta convenção de nomenclatura de zona:

```
[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
```

E você pode querer que a saída esteja no seguinte formato:

```
[hostname]-[data center]-[device type]
Para fazer isso, você precisa capturar os campos de nome do host, data center e tipo de dispositivo em variáveis e usá-los na saída. A seguinte expressão regular faria isso:
```

```
.*_([a-zA-Z0-9]+)_([a-zA-Z0-9]+)_([a-zA-Z0-9]+)_.*
Como existem três conjuntos de parênteses, as variáveis 1, 2 e 3 seriam preenchidas.
```

Em seguida, você pode usar o seguinte formato para receber a saída em seu formato preferido:

```
\2-\1-\3  
Sua saída seria a seguinte:
```

```
hostname1-Miami-filer  
hostname2-Tampa-switch  
hostname3-Boston-windows2K  
hostname4-Raleigh-solaris
```

Os hífen entre as variáveis fornecem um exemplo de texto constante que é inserido na saída formatada.

Exemplos

Exemplo 1 mostrando nomes de zona

Neste exemplo, você usa a expressão regular para extrair um nome de host do nome da zona. Você pode criar uma expressão regular se tiver algo semelhante aos seguintes nomes de zona:

- S0032_myComputer1Name-HBA0
- S0434_myComputer1Name-HBA1
- S0432_myComputer1Name-HBA3

A expressão regular que você poderia usar para capturar o nome do host seria:

```
S[0-9]+_([a-zA-Z0-9]*)[_-]HBA[0-9]
```

O resultado é uma correspondência de todas as zonas que começam com S que são seguidas por qualquer combinação de dígitos , seguido por um sublinhado, o nome de host alfanumérico (myComputer1Name), um sublinhado ou hífen, as letras maiúsculas HBA e um único dígito (0-9). O nome de host sozinho é armazenado na variável * 1*.

A expressão regular pode ser dividida em seus componentes:

- "S" representa o nome da zona e inicia a expressão. Isto corresponde apenas a um "S" no início do nome da zona.
- Os caracteres [0-9] entre parênteses indicam que o seguinte "S" deve ser um dígito entre 0 e 9, inclusive.
- O sinal indica que a ocorrência das informações nos parênteses anteriores deve existir 1 ou mais vezes.
- O _ (sublinhado) significa que os dígitos após S devem ser seguidos imediatamente por apenas um caractere sublinhado no nome da zona. Neste exemplo, a convenção de nomenclatura de zona usa o sublinhado para separar o nome da zona do nome do host.
- Após o sublinhado necessário, os parênteses indicam que o padrão contido dentro será armazenado na variável 1.
- Os caracteres entre colchetes [a-zA-Z0-9] indicam que os caracteres correspondentes são todas as letras

(independentemente do caso) e números.

- O * (asterisco) que segue os colchetes indica que os caracteres entre colchetes ocorrem 0 ou mais vezes.
- Os caracteres entre colchetes [-] (sublinhado e traço) indicam que o padrão alfanumérico deve ser seguido por um sublinhado ou um traço.
- As letras HBA na expressão regular indicam que esta sequência exata de caracteres deve ocorrer no nome da zona.
- O conjunto final de caracteres entre colchetes [0-9] corresponde a um único dígito de 0 a 9, inclusive.

Exemplo 2

Neste exemplo, pule para o primeiro sublinhado "", *depois combine e e e tudo depois disso até o segundo ""*, e então pule tudo depois disso.

ZONA: Z_E2FHDBS01_E1NETAPP

- Nome do host:* E2FHDBS01

RegExp: .?(E.?).*?

Exemplo 3

Os parênteses "()" ao redor da última seção na expressão regular (abaixo) identificam qual parte é o nome do host. Se você quisesse que o VSAN3 fosse o nome do host, seria: [A-zA-Z0-9] ([a-zA-Z0-9]).*

ZONA: A_VSAN3_SR48KENT_A_CX2578_SPA0

- Nome do anfitrião:* SR48KENT

RegExp: [a-zA-Z0-9]_[a-zA-Z0-9] ([a-zA-Z0-9]).*

Exemplo 4 mostrando um padrão de nomenclatura mais complicado

Você pode criar uma expressão regular se tiver algo semelhante aos seguintes nomes de zona:

- myComputerName123-HBA1_Symm1_FA3
- myComputerName123-HBA2_Symm1_FA5
- myComputerName123-HBA3_Symm1_FA7

A expressão regular que você poderia usar para capturá-los seria:

```
([a-zA-Z0-9]*)_.*
```

A variável 1 conterá apenas `_myComputerName123_` depois de ser avaliada por esta expressão.

A expressão regular pode ser dividida em seus componentes:

- Os parênteses indicam que o padrão contido dentro será armazenado na variável 1.
- Os caracteres entre colchetes [a-zA-Z0-9] significam que qualquer letra (independentemente do caso) ou dígito corresponderá.

- O * (asterisco) que segue os colchetes indica que os caracteres entre colchetes ocorrem 0 ou mais vezes.
- O caractere _ (sublinhado) na expressão regular significa que o nome da zona deve ter um sublinhado imediatamente após a cadeia alfanumérica correspondente aos colchetes anteriores.
- O . (ponto) corresponde a qualquer caractere (um curinga).
- O * (asterisco) indica que o curinga do período anterior pode ocorrer 0 ou mais vezes.

Em outras palavras, a combinação .* indica qualquer caractere, qualquer número de vezes.

Exemplo 5 mostrando nomes de zona sem um padrão

Você pode criar uma expressão regular se tiver algo semelhante aos seguintes nomes de zona:

- myComputerName_HBA1_Symm1_FA1
- myComputerName123_HBA1_Symm1_FA1

A expressão regular que você poderia usar para capturá-los seria:

```
(.*?)_.*
```

A variável 1 conterá _MyComputerName_ (no exemplo do nome da primeira zona) ou _myComputerName123_ (no exemplo do nome da segunda zona). Esta expressão regular combinaria, assim, tudo antes do primeiro sublinhado.

A expressão regular pode ser dividida em seus componentes:

- Os parênteses indicam que o padrão contido dentro será armazenado na variável 1.
- O .* (asterisco de ponto) corresponde a qualquer caractere, qualquer número de vezes.
- O * (asterisco) que segue os colchetes indica que os caracteres entre colchetes ocorrem 0 ou mais vezes.
- O personagem ? faz o jogo não-ganancioso. Isso obriga-o a parar de combinar no primeiro sublinhado, em vez do último.
- Os caracteres _.* correspondem ao primeiro sublinhado encontrado e todos os caracteres que o seguem.

Exemplo 6 mostrando nomes de computadores com um padrão

Você pode criar uma expressão regular se tiver algo semelhante aos seguintes nomes de zona:

- Storage1_Switch1_myComputerName123A_A1_FC1
- Storage2_Switch2_myComputerName123B_A2_FC2
- Storage3_Switch3_myComputerName123T_A3_FC3

A expressão regular que você poderia usar para capturá-los seria:

```
.*?_.*?_([a-zA-Z0-9]*[ABT])_.*
```

Como a convenção de nomenclatura de zona tem mais de um padrão, podemos usar a expressão acima, que corresponderá a todas as instâncias de um nome de host (MyComputerName no exemplo) que termina com um A, um B ou um T, colocando esse nome de host na variável 1.

A expressão regular pode ser dividida em seus componentes:

- O `.` (asterisco de ponto) corresponde a qualquer caractere, qualquer número de vezes.
- O personagem `?` faz o jogo não-ganancioso. Isso obriga-o a parar de combinar no primeiro sublinhado, em vez do último.
- O caractere sublinhado corresponde ao primeiro sublinhado no nome da zona.
- Assim, a primeira combinação `.*_` corresponde aos caracteres `storage1_` no primeiro exemplo de nome de zona.
- A segunda combinação `.*_` comporta-se como a primeira, mas corresponde a `Switch1_` no exemplo do nome da primeira zona.
- Os parênteses indicam que o padrão contido dentro será armazenado na variável 1.
- Os caracteres entre colchetes `[a-zA-Z0-9]` significam que qualquer letra (independentemente do caso) ou dígito corresponderá.
- O `*` (asterisco) que segue os colchetes indica que os caracteres entre colchetes ocorrem 0 ou mais vezes.
- Os caracteres entre colchetes na expressão regular `[ABT]` correspondem a um único caractere no nome da zona que deve ser A, B ou T.
- O `_` (sublinhado) que segue os parênteses indica que a correspondência de caracteres `[ABT]` deve ser seguida de um sublinhado.
- O `.` (asterisco de ponto) corresponde a qualquer caractere, qualquer número de vezes.

O resultado disso faria com que a variável 1 contivesse qualquer cadeia alfanumérica que:

- foi precedido por algum número de caracteres alfanuméricos e dois sublinhados
- foi seguido por um sublinhado (e, em seguida, qualquer número de caracteres alfanuméricos)
- Teve um caráter final de A, B ou T, antes do terceiro sublinhado.

Exemplo 7

Zona: myComputerName123_HBA1_Symm1_FA1

- Nome do anfitrião:* myComputerName123

RegExp: ([a-zA-Z0-9])_.*

Exemplo 8

Este exemplo encontra tudo antes do primeiro `_`.

Zona: MyComputerName_HBA1_Symm1_FA1

MyComputerName123_HBA1_Symm1_FA1

Nome do host: MyComputerName

Regexp: (.?)_.

Exemplo 9

Este exemplo encontra tudo após o 1st _ e até o segundo _.

Zone: Z_MyComputerName_StorageName

Nome do host: MyComputerName

RegExp: .?(.?).*?

Exemplo 10

Este exemplo extrai "MyComputerName123" dos exemplos de zona.

Zona: storage1_Switch1_MyComputerName123A_A1_FC1

Storage2_Switch2_MyComputerName123B_A2_FC2

Storage3_Switch3_MyComputerName123T_A3_FC3

- Nome do anfitrião:* MyComputerName123

RegExp: .??.?([a-zA-Z0-9])[ABT]_.

Exemplo 11

Zona: storage1_Switch1_MyComputerName123A_A1_FC1

- Nome do anfitrião:* MyComputerName123A

RegExp: .??.?([a-zA-Z0-9]).*?

Exemplo 12

(Circumflex ou caret) **dentro de colchetes** nega a expressão, por exemplo, [FF] significa qualquer coisa, exceto F maiúscula ou minúscula, e [a-z] significa tudo, exceto a minúscula a z, e, no caso acima, qualquer coisa, exceto o _ . O comando format adiciona o "-" ao nome do host de saída.

Zona: mhs_apps44_d_A_10a0_0429

- Nome do host: * mhs-apps44-d

RegExp: ([/])([AB]). * Formato em dados de infraestrutura Insights: 1- 2 ([/])([/])([]). * Formato em Data Infrastructure Insights: 1- 2- 3

Exemplo 13

Neste exemplo, o alias de armazenamento é delimitado por "" e a expressão precisa usar "" para definir que realmente existem "" sendo usados na cadeia de caracteres, e que esses não são parte da própria expressão.

Alias de armazenamento: hosts E2DOC01C1/E2DOC01N1

Nome do host: E2DOC01N1

RegExp: .?.?(.*?)

Exemplo 14

Este exemplo extrai "PD-RV-W-AD-2" dos exemplos de zona.

ZONE: PD_D-PD-RV-W-AD-2_01

NOME DO HOST: PD-RV-W-AD-2

RegExp: [-

Exemplo 15

A configuração de formato, neste caso, adiciona o "US-BV-" ao nome do host.

ZONA: SRV_USBVM11_F1

NOME DO ANFITRIÃO: US-BV-M11

RegExp: SRV_USBV([A-ZA-Z0-9])_F[12]

Formato: US-BV- 1

Informações da página de ativos

Visão geral da página de ativos

As páginas de ativos resumem o status atual de um ativo e contêm links para informações adicionais sobre o ativo e seus ativos relacionados.

Tipos de páginas de ativos

O Data Infrastructure Insights fornece páginas de ativos para os seguintes ativos:

- Máquina virtual
- Máquina de Storage Virtual (SVM)
- Volume
- Volume interno
- Host (incluindo hipervisor)
- Pool de storage
- Armazenamento
- Armazenamento de dados
- Aplicação
- Nó de storage
- Qtree
- Disco

- VMDK
- Porta
- Interruptor
- Malha

Alterar o intervalo de tempo dos dados apresentados

Por padrão, uma página de ativo exibe as últimas 24 horas de dados; no entanto, você pode alterar o segmento de dados exibido selecionando outro intervalo de tempo fixo ou um intervalo de tempo personalizado para exibir menos ou mais dados.

Você pode alterar o segmento de tempo dos dados exibidos usando uma opção localizada em cada página de ativo, independentemente do tipo de ativo. Para alterar o intervalo de tempo, clique no intervalo de tempo exibido na barra superior e escolha entre os seguintes segmentos de tempo:

- Durar 15 minutos
- Durar 30 minutos
- Durar 60 minutos
- Últimas 2 horas
- Últimas 3 horas (este é o padrão)
- Últimas 6 horas
- Últimas 12 horas
- Últimas 24 horas
- Últimos 2 dias
- Últimos 3 dias
- Últimos 7 dias
- Últimos 30 dias
- Intervalo de tempo personalizado

O intervalo de tempo personalizado permite-lhe selecionar até 31 dias consecutivos. Também pode definir a hora de início e a hora de fim do dia para este intervalo. A hora de Início padrão é 12:00 AM no primeiro dia selecionado e a hora de término padrão é 11:59 PM no último dia selecionado. Clicar em aplicar aplicará o intervalo de tempo personalizado à página de ativos.

As informações em uma seção de resumo da página de ativos, bem como em quaisquer tabelas ou widgets personalizados na página, são atualizadas automaticamente com base no intervalo de tempo selecionado. A taxa de atualização atual é exibida no canto superior direito da seção Resumo, bem como em quaisquer tabelas ou widgets relevantes na página.

Adicionar widgets personalizados

Você pode adicionar seus próprios widgets a qualquer página de ativos. Os widgets que você adicionar aparecerão nas páginas de ativos para todos os objetos desse tipo. Por exemplo, adicionar um widget personalizado a uma página de ativos de armazenamento exibirá esse widget nas páginas de ativos para todos os ativos de armazenamento.

Filtragem de objetos em contexto

Ao configurar um widget na Landing page de um ativo, você pode definir filtros *in-context* para mostrar apenas objetos diretamente relacionados ao ativo atual. Por padrão, quando você adiciona um widget, *todos* objetos do tipo selecionado no seu locatário são exibidos. Os filtros de contexto permitem exibir apenas os dados relevantes para o seu ativo atual.

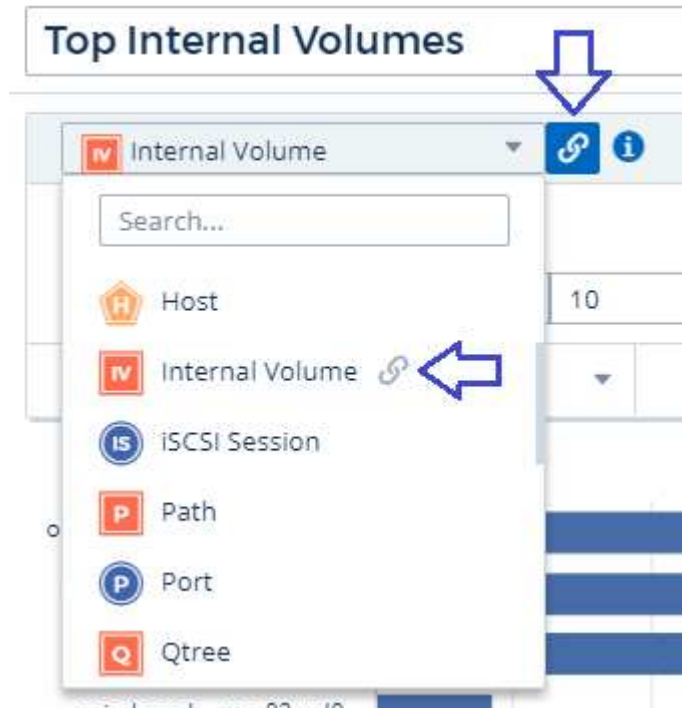
Na maioria das Landing pages de ativos, os widgets permitem filtrar objetos relacionados ao ativo atual. Em listas suspensas de filtros, os tipos de objetos que exibem um ícone de link podem ser filtrados em contexto para o ativo atual.

Por exemplo, em uma página de ativos de armazenamento, você pode adicionar um widget Gráfico de barras para mostrar as principais IOPS em volumes internos somente nesse armazenamento. Por padrão, quando você adiciona um widget, *all* volumes internos em seu locatário são exibidos.

Para mostrar apenas volumes internos no ativo de storage atual, faça o seguinte:

Passos

1. Abra uma página de ativos para qualquer ativo **Storage**.
2. Clique em **Editar** para abrir a página de ativos no modo Editar.
3. Clique em **Add Widget** e selecione *Bar Chart*.
4. Selecione **volume interno** para o tipo de objeto a ser exibido no gráfico de barras. Observe que o tipo de objeto de volume interno tem um ícone de link ao lado dele. O ícone "ligado" está ativado por predefinição.



5. Escolha *IOPS - Total* e defina quaisquer filtros adicionais que você goste.
6. Diminua o campo **Roll Up** clicando no [X] ao lado dele. O campo **Show** é exibido.
7. Escolha para mostrar Top 10.

8. Salve o widget.

O gráfico de barras mostra apenas os volumes internos que residem no ativo de storage atual.

O widget será exibido nas páginas de ativos para todos os objetos de armazenamento. Quando o link no contexto está ativado no widget, o gráfico de barras mostra dados para volumes internos relacionados apenas ao ativo de armazenamento atualmente exibido.

Para desvincular os dados do objeto, edite o widget e clique no ícone de link ao lado do tipo de objeto. O link fica desativado e o gráfico exibe dados para objetos *all* no locatário.

Você também pode usar **"* variáveis especiais em widgets*"** para exibir informações relacionadas a ativos em Landing pages.

Seção Resumo da página de ativos

A seção Resumo de uma página de ativo exibe informações gerais sobre um ativo, incluindo se alguma métrica ou políticas de desempenho são motivo de preocupação. As áreas problemáticas potenciais são indicadas por um círculo vermelho.

As informações na seção de resumo, bem como em quaisquer tabelas ou widgets personalizados na página de ativos, são atualizadas automaticamente com base no intervalo de tempo selecionado. Você pode ver a taxa de atualização atual no canto superior direito da seção Resumo, as tabelas e quaisquer widgets personalizados.

Virtual Machine Summary

5m

Power State:

On

Guest State:

Running

Datastore:

[i-00cc58b5c47a69271](#)

CPU Utilization - Total:

13.82 %

Memory Utilization - Total:

N/A

Memory:

32.0 GB

Capacity - Total:

200.0 GB

Capacity - Used:

N/A

Latency - Total:

6.35 ms

IOPS - Total:

 316.59 IO/s

Throughput - Total:

68.81 MB/s

DNS Name:

ip-10-30-23-12.ec2.internal

IP:

10.30.23.12

OS:

CentOS Linux 7 x86_64 HVM
EBS ENA 1901_01-b7ee8a69-
ee97-4a49-9e68-afaae216db2e-
ami-05713873c6794f575.4
x86_64

Processors:

8

Hypervisor Name:

us-east-1a

Hypervisor IP:

US-EAST-1A-052113251141

Hypervisor OS:

Amazon AWS EC2

Hypervisor FC Fabrics:

0

Hypervisor CPU Utilization:

N/A

Hypervisor Memory

Utilization:

N/A

Alert Monitors:

[High Latency VMs](#)

[Instance CPU Under-utilized](#)

[View Topology](#)

Observação: As informações exibidas na seção Resumo variam, dependendo do tipo de ativo que você está visualizando.

Você pode clicar em qualquer um dos links de ativos para exibir suas páginas de ativos. Por exemplo, se você estiver exibindo um nó de armazenamento, poderá clicar em um link para exibir a página de ativos do armazenamento ao qual está associado.

Você pode visualizar as métricas associadas ao ativo. Um círculo vermelho ao lado de uma métrica indica que você pode precisar diagnosticar e resolver possíveis problemas.



Você pode notar que a capacidade de volume pode mostrar mais de 100% em alguns ativos de storage. Isso se deve aos metadados relacionados à capacidade do volume fazer parte dos dados de capacidade consumida reportados pelo ativo.

Se aplicável, você pode clicar em um link de alerta para exibir o alerta e o monitor associados ao ativo.

Topologia

Em determinadas páginas de ativos, a seção de resumo contém um link para visualizar a topologia do ativo e suas conexões.

A topologia está disponível para os seguintes tipos de ativos:

- Aplicação
- Disco
- Malha
- Host
- Volume interno
- Porta
- Interruptor
- Máquina virtual
- VMDK
- Volume

The image shows a screenshot of a storage management interface. The top window, titled 'Internal Volume', displays the following details:

- Storage:** barbados1,barbados2
- Storage Pool:** barbados1:aggr1
- Status:** Online
- Type:** FlexVol
- UUID:**
- SVM/vFiler:** vfiler0
- Capacity - Total:** 1.0 GB
- Capacity - Used:** 0.0 GB
- Snapshot:** <0,1 GB
- Latency - Total:** 0.02 ms
- Storage Pool Utilization:** 0.68 %
- IOPS - Total:** 0.13 IO/s
- Datstore:**
- Deduplication Savings:** 0.0 %
- Thin Provisioned:** No
- Replication Source(s):**
- Performance Policies:** Find High Latency FlexVols

A 'View Topology' button is located at the bottom of the 'Internal Volume' window. An arrow points from this button to a 'Topology' window below it. The 'Topology' window displays a diagram showing the relationship between three components:

```

graph LR
    H[ocise-esx-1431...] --> NAS[NAS]
    NAS --> S[barbados1,bar...]
  
```

The diagram shows a host (H) connected to a Network Attached Storage (NAS) device, which is in turn connected to a storage volume (S). The 'Topology' window also includes a 'Close' button in the bottom right corner.

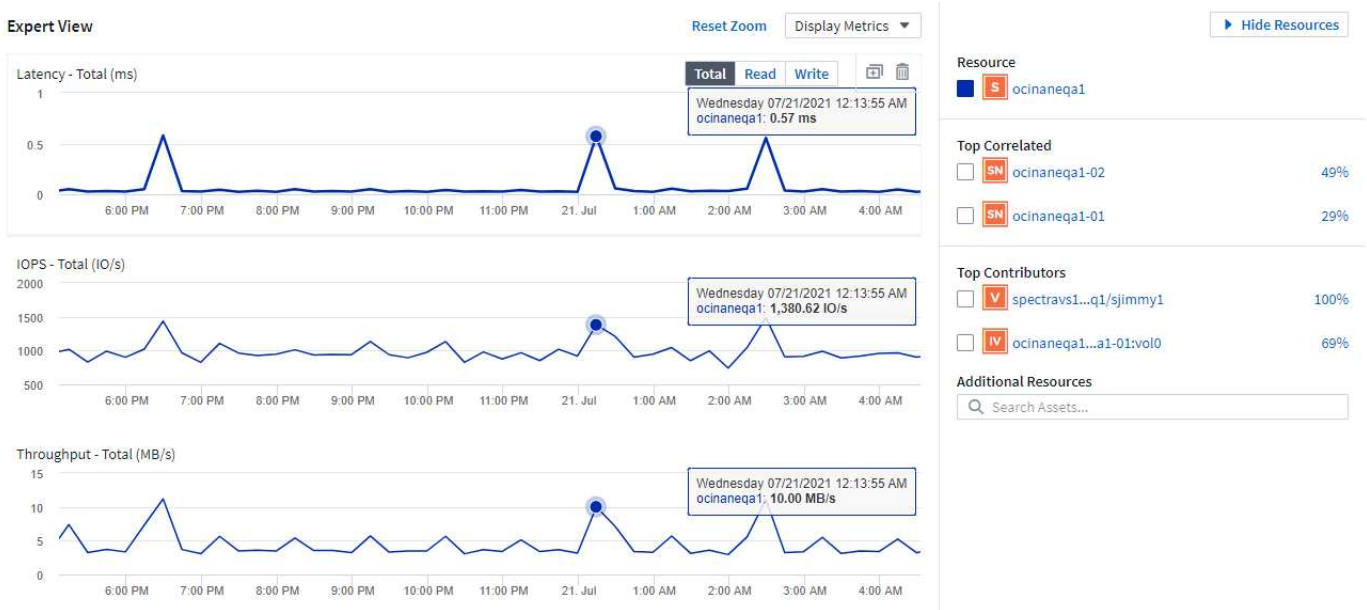
Visão do especialista

A seção Expert View de uma página de ativo permite que você visualize uma amostra de desempenho do ativo base com base em qualquer número de métricas aplicáveis no contexto de um período de tempo escolhido no gráfico de desempenho e quaisquer ativos relacionados a ele. Os dados nos gráficos são atualizados automaticamente à

medida que os coletores de dados pesquisam e os dados atualizados são adquiridos.

Usando a seção Expert View

Veja a seguir um exemplo da seção Expert View em uma página de ativos de armazenamento:



Você pode selecionar as métricas que deseja exibir no gráfico de desempenho para o período de tempo selecionado. Clique no menu suspenso *Display Metrics* e escolha entre as métricas listadas.

A seção **recursos** mostra o nome do ativo base e a cor que representa o ativo base no gráfico de desempenho. Se a seção **Top correlacionado** não contiver um ativo que você deseja visualizar no gráfico de desempenho, você poderá usar a caixa **pesquisar ativos** na seção **recursos adicionais** para localizar o ativo e adicioná-lo ao gráfico de desempenho. À medida que você adiciona recursos, eles aparecem na seção recursos adicionais.

Também são mostrados na seção recursos, quando aplicável, quaisquer ativos relacionados ao ativo base nas seguintes categorias:

- Topo correlacionado

Mostra os ativos que têm uma alta correlação (porcentagem) com uma ou mais métricas de performance para o ativo base.

- Principais colaboradores

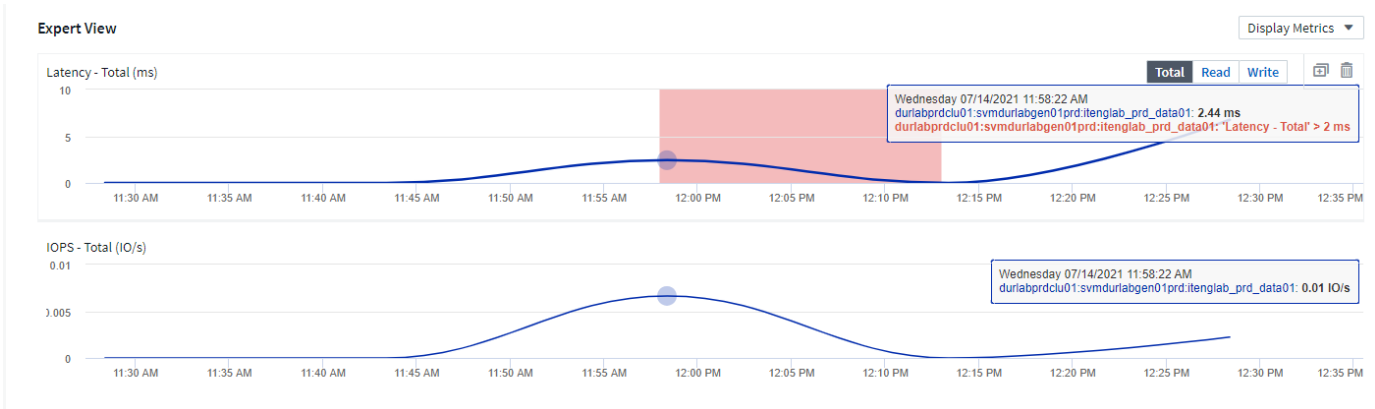
Mostra os ativos que contribuem (porcentagem) para o ativo base.

- Contenções da carga de trabalho

Mostra os ativos que impactam ou são afetados por outros recursos compartilhados, como hosts, redes e armazenamento. Estes são às vezes chamados de recursos *gananciosos* e *degradados*.

Alertas no Expert View

Os alertas também são exibidos na seção Expert View de uma página inicial de ativos, mostrando o tempo e a duração do alerta, bem como a condição do monitor que o acionou.



Definições de métricas do Expert View

A seção Expert View de uma página de ativo exibe várias métricas com base no período de tempo selecionado para o ativo. Cada métrica é exibida em seu próprio gráfico de desempenho. Você pode adicionar ou remover métricas e ativos relacionados dos gráficos, dependendo dos dados que deseja ver. As métricas que você pode escolher variam dependendo do tipo de ativo.

Métrica	Descrição
BB crédito zero Rx, TX	Número de vezes que a contagem de crédito de buffer para buffer de recepção/transmissão foi transferida para zero durante o período de amostragem. Esta métrica representa o número de vezes que a porta anexada teve que parar de transmitir porque esta porta estava fora de créditos para fornecer.
BB crédito zero duração TX	Tempo em milissegundos durante o qual o crédito BB de transmissão foi zero durante o intervalo de amostragem.
Taxa de acerto do cache (Total, leitura, escrita) %	Porcentagem de solicitações que resultam em acertos de cache. Quanto maior o número de acessos versus acessos ao volume, melhor é o desempenho. Esta coluna está vazia para matrizes de armazenamento que não recolhem informações de acerto de cache.
Utilização de cache (total) %	Porcentagem total de solicitações de cache que resultam em acertos de cache
Classe 3 descarta	Contagem de cartões de transporte de dados de classe 3 Fibre Channel.
Utilização de CPU (total) %	Quantidade de recursos de CPU usados ativamente, como uma porcentagem do total disponível (sobre todas as CPUs virtuais).
Erro CRC	Número de quadros com verificações de redundância cíclica (CRCs) inválidas detetadas pela porta durante o período de amostragem
Taxa de quadros	Taxa de quadros de transmissão em quadros por segundo (FPS)

Tamanho médio do fotograma (Rx, TX)	Relação entre o tráfego e o tamanho do quadro. Essa métrica permite identificar se há estruturas suspensas na malha.
Tamanho do quadro demasiado longo	Contagem de quadros de transmissão de dados Fibre Channel que são muito longos.
Tamanho do quadro demasiado curto	Contagem de quadros de transmissão de dados Fibre Channel que são muito curtos.
Densidade de e/S (total, leitura, gravação)	Número de IOPS dividido pela capacidade usada (conforme adquirido da pesquisa de inventário mais recente da fonte de dados) para o elemento volume, volume interno ou armazenamento. Medido em número de operações de e/S por segundo por TB.
IOPS (total, leitura, gravação)	Número de solicitações de serviço de e/S de leitura/gravação que passam pelo canal de e/S ou uma parte desse canal por unidade de tempo (medido em e/S por segundo)
Taxa de transferência IP (total, leitura, gravação)	Total: Taxa agregada à qual os dados IP foram transmitidos e recebidos em megabytes por segundo.
Leitura: Taxa de transferência IP (receber):	Taxa média na qual os dados IP foram recebidos em megabytes por segundo.
Escreva: Taxa de transferência IP (transmissão):	Taxa média na qual os dados IP foram transmitidos em megabytes por segundo.
Latência (total, leitura, gravação)	Latência (R&W): Taxa na qual os dados são lidos ou gravados nas máquinas virtuais em um período fixo de tempo. O valor é medido em megabytes por segundo.
Latência:	Tempo médio de resposta das máquinas virtuais em um armazenamento de dados.
Latência máxima:	O maior tempo de resposta das máquinas virtuais em um armazenamento de dados.
Falha na ligação	Número de falhas de link detetadas pela porta durante o período de amostragem.
Reposição da ligação Rx, TX	O número de redefinições da ligação de recepção ou de transmissão durante o período de amostragem. Essa métrica representa o número de redefinições de link que foram emitidas pela porta anexada a essa porta.
% De utilização da memória (total)	Limite para a memória usada pelo host.

% R/W parcial (total)	Número total de vezes que uma operação de leitura/gravação cruza um limite de distribuição em qualquer módulo de disco em um LUN RAID 5, RAID 1/0 ou RAID 0 geralmente, os cruzamentos de faixa não são benéficos, porque cada um requer uma e/S adicional. Uma porcentagem baixa indica um tamanho eficiente do elemento de distribuição e é uma indicação de alinhamento inadequado de um volume (ou um LUN NetApp). Para CLARiiON, esse valor é o número de cruzamentos de faixa divididos pelo número total de IOPS.
Erros de porta	Relatório de erros de porta durante o período de amostragem/período de tempo determinado.
Contagem de perda de sinal	Número de erros de perda de sinal. Se ocorrer um erro de perda de sinal, não existe uma ligação elétrica e existe um problema físico.
Taxa de swap (taxa total, em taxa, fora taxa)	Taxa na qual a memória é trocada dentro, fora ou ambos do disco para a memória ativa durante o período de amostragem. Este contador aplica-se a máquinas virtuais.
Contagem de perdas de sincronização	Número de erros de perda de sincronização. Se ocorrer um erro de perda de sincronização, o hardware não poderá fazer sentido do tráfego ou bloquear nele. Todo o equipamento pode não estar usando a mesma taxa de dados, ou a ótica ou as conexões físicas podem ser de baixa qualidade. A porta deve resincronizar após cada erro, o que afeta o desempenho do sistema. Medido em KB/seg
Taxa de transferência (total, leitura, gravação)	Taxa na qual os dados estão sendo transmitidos, recebidos ou ambos em um período fixo de tempo em resposta a solicitações de serviço de e/S (medido em MB por segundo).
Limites de eliminação de tempo limite - TX	Contagem de quadros de transmissão descartados causada por tempo limite.
Taxa de tráfego (total, leitura, gravação)	Tráfego transmitido, recebido ou ambos recebidos durante o período de amostragem, em mebibytes por segundo.
Utilização de tráfego (Total, leitura, escrita)	Relação de tráfego recebido/transmitido/total para receber/transmitir/capacidade total, durante o período de amostragem.
Utilização (Total, leitura, escrita) %	Porcentagem da largura de banda disponível utilizada para transmissão (TX) e recepção (Rx).
Escrever pendente (total)	Número de solicitações de serviço de e/S de gravação pendentes.

Usando a seção Expert View

A seção visualização de especialistas permite que você visualize gráficos de desempenho de um ativo com base em qualquer número de métricas aplicáveis durante um período de tempo escolhido e adicione ativos relacionados para comparar e contrastar o desempenho do ativo e do ativo relacionado em diferentes períodos de tempo.

Passos

1. Localize uma página de ativo fazendo uma das seguintes opções:

- PESQUISE e selecione um ativo específico.
- Selecione um ativo de um widget de painel.
- Consulte um conjunto de ativos e selecione um na lista de resultados.

A página de ativos é exibida. Por padrão, o gráfico de desempenho mostra duas métricas para o período de tempo selecionado para a página de ativo. Por exemplo, para um storage, o gráfico de desempenho mostra a latência e o total de IOPS por padrão. A seção recursos exibe o nome do recurso e uma seção recursos adicionais, que permite pesquisar ativos. Dependendo do ativo, você também pode ver os ativos nas seções Top Correlated, Top Colaborador, ganancioso e degradado. Se não houver ativos relevantes para essas seções, elas não serão exibidas.

2. Você pode adicionar um gráfico de desempenho para uma métrica clicando em **Display Metrics** e selecionando as métricas que deseja exibir.

Um gráfico separado é exibido para cada métrica selecionada. O gráfico exibe os dados do período de tempo selecionado. Você pode alterar o período de tempo clicando em outro período de tempo no canto superior direito da página de ativos ou ampliando o zoom em qualquer gráfico.

Clique em **Display Metrics** para desmarcar qualquer gráfico. O gráfico de desempenho da métrica é removido do Expert View.

3. Você pode posicionar o cursor sobre o gráfico e alterar os dados de métrica exibidos para esse gráfico clicando em qualquer uma das opções a seguir, dependendo do ativo:

- Leitura, escrita ou Total
- TX, Rx ou Total

Total é o padrão.

Você pode arrastar o cursor sobre os pontos de dados no gráfico para ver como o valor da métrica muda ao longo do período de tempo selecionado.

4. Na seção recursos, você pode adicionar quaisquer ativos relacionados aos gráficos de desempenho:

- Você pode selecionar um ativo relacionado nas seções **Top correlacionado**, **Top Contribuidores**, **ganancioso** e **degradado** para adicionar dados desse ativo ao gráfico de desempenho para cada métrica selecionada.

Depois de selecionar o ativo, um bloco de cores aparece ao lado do ativo para indicar a cor de seus pontos de dados no gráfico.

5. Clique em **Ocultar recursos** para ocultar o painel recursos adicionais. Clique em **Resources** para mostrar o painel.

- Para qualquer ativo mostrado, você pode clicar no nome do ativo para exibir sua página de ativo, ou

você pode clicar na porcentagem que o ativo correlaciona ou contribui para o ativo base para ver mais informações sobre a relação do ativo com o ativo base.

Por exemplo, clicar na porcentagem vinculada ao lado de um ativo correlacionado superior exibe uma mensagem informativa comparando o tipo de correlação que o ativo tem com o ativo base.

- Se a seção superior correlacionada não contiver um ativo que você deseja exibir em um gráfico de desempenho para fins de comparação, você poderá usar a caixa pesquisar ativos na seção recursos adicionais para localizar outros ativos.

Depois de selecionar um ativo, ele é exibido na seção recursos adicionais. Quando você não quiser mais exibir informações sobre o ativo, clique no ícone de lixeira para excluir.

Seção de dados do usuário

A seção dados do usuário de uma página de ativo exibe e permite que você altere quaisquer dados definidos pelo usuário, como aplicativos e anotações.

Usando a seção dados do usuário para atribuir ou modificar aplicativos

É possível atribuir aplicativos em execução no locatário a determinados ativos (host, máquinas virtuais, volumes, volumes internos, qtrees e hipervisores). A seção dados do usuário permite adicionar, alterar ou remover os aplicativos atribuídos a um ativo. Para todos esses tipos de ativos, exceto volumes, você pode atribuir mais de um aplicativo.

Passos

1. Localize uma página de ativo fazendo qualquer um dos seguintes procedimentos:
 - a. Consulte uma lista de ativos e, em seguida, selecione um da lista.
 - b. Em um Dashboard, localize um nome de ativo e clique nele.
 - c. Faça uma pesquisa e escolha um ativo dos resultados.

A página de ativos é exibida. A seção dados do utilizador da página apresenta aplicações ou anotações atualmente atribuídas.

Para alterar o aplicativo atribuído ou atribuir um aplicativo ou aplicativos adicionais, solte a lista **aplicativo** e selecione o(s) aplicativo(s) que deseja atribuir ao ativo. Você pode digitar para pesquisar um aplicativo ou selecionar um na lista.

Para remover uma aplicação, desça a lista de aplicações e desmarque a aplicação.

Utilizar a seção dados do utilizador para atribuir ou modificar anotações

Ao personalizar o Data Infrastructure Insights para rastrear dados para seus requisitos corporativos, você pode definir notas especializadas chamadas anotações e atribuí-las aos seus ativos. A seção dados do usuário de uma página de ativo exibe anotações atribuídas a um ativo e também permite que você altere as anotações atribuídas a esse ativo.

Passos

1. Para adicionar uma anotação ao ativo, na seção dados do usuário da página de ativo, clique em **Annotation***.
2. Selecione uma anotação na lista.

3. Clique em valor e efetue uma das seguintes ações, dependendo do tipo de anotação selecionado:
 - a. Se o tipo de anotação for lista, data ou Booleano, selecione um valor na lista.
 - b. Se o tipo de anotação for texto, introduza um valor.
4. Clique em Guardar.

A anotação é atribuída ao ativo. Você pode filtrar ativos posteriormente por anotação usando uma consulta.

Se pretender alterar o valor da anotação depois de a atribuir, largue a lista de anotações e introduza um valor diferente.

Se a anotação for do tipo de lista para o qual a opção *Add new values on the fly* está selecionada, você pode digitar para adicionar um novo valor além de selecionar um valor existente.

Seção Alertas relacionados à Página de ativos

Você pode usar a seção Alertas relacionados de uma página de ativo para ver quaisquer alertas que ocorram no seu localário como resultado de um monitor atribuído a um ativo. Os monitores geram alertas com base nas condições definidas e permitem identificar a implicação e analisar o impacto e a causa raiz do problema de uma forma que permita uma correção rápida e eficaz.

O exemplo a seguir mostra uma seção típica de Alertas relacionados que é exibida em uma página de ativos:

Related Alerts ⋮

16 items found

Alert ID	Active Status	Triggered Time ↓	Top Severity	Monitor	Triggered On	Status
AL-146777	Resolved	5 minutes ago Jul 28, 2021 4:01 PM	Warning	Workload IOPS	workload_volume_name: podAuVol-wid12074	New
AL-146748	Resolved	11 minutes ago Jul 28, 2021 3:55 PM	Warning	Workload IOPS	workload_volume_name: podAuVol-wid12074	New
AL-146711	Resolved	23 minutes ago Jul 28, 2021 3:43 PM	Critical	Workload IOPS	workload_volume_name: podAuVol-wid12074	New
AL-146704	Resolved	25 minutes ago	Warning	Workload IOPS	workload_volume_name: podAuVol-wid12074	New

A seção Alertas relacionados permite visualizar e gerenciar os alertas que ocorrem em sua rede como resultado das condições de monitoramento atribuídas a um ativo.

Passos

- Localize uma página de ativo fazendo qualquer um dos seguintes procedimentos:
 - Digite o nome do ativo na área pesquisar e, em seguida, selecione o ativo na lista.
 - Em um widget de painel, clique no nome de um ativo.
 - Consulte um conjunto de ativos e selecione ligado na lista de resultados.

A página de ativos é exibida. A seção Alertas relacionados exibe a hora em que o alerta foi acionado, bem como o status atual do alerta e do monitor que o acionou. Você pode clicar no ID de alerta para abrir a página de destino do alerta para mais investigação.

Virtualização de storage

O Data Infrastructure Insights pode diferenciar um storage array com storage local ou virtualização de outros storage arrays. Isso possibilita relacionar os custos e diferenciar a

performance do front-end todo o caminho até o back-end da sua infraestrutura.

Virtualização em um widget de tabela

Uma das maneiras mais fáceis de começar a olhar para a virtualização de armazenamento é criar um widget de tabela de painel mostrando o tipo virtualizado. Ao criar a consulta para o widget, basta adicionar "virtualizedType" ao seu agrupamento ou filtro.

Storage X ▾

Display Last 3 Hours (Dashboard Time) ▾ Override Dashboard Time

Filter by Attribute +

Filter by Metric +

Group by virtualizedType X ▾

O widget de tabela resultante mostra os armazenamentos *Standard*, *backend* e *Virtual* no seu locatário.

Storage by virtualizedType

50 items found in 4 groups

virtualizedType ↑	Storage
Backend (5)	--
Backend	Sym-Perf
Backend	Sym-000050074300343
Backend	CX600_26_CK00351029326
Backend	VNX8000_46_CK00351029346
Backend	Sym-000050074300324
Standard (36)	--
Virtual (8)	--

As páginas iniciais mostram informações virtualizadas

Em uma página inicial de armazenamento, volume, volume interno ou disco, você pode ver informações relevantes de virtualização. Por exemplo, olhando para a página inicial de armazenamento abaixo, você pode ver que este é um armazenamento virtual e que sistema de armazenamento de back-end se aplica. Quaisquer tabelas relevantes em páginas de destino também mostrarão informações de virtualização, conforme aplicável.

Storage Summary

Model:
V-Series

Vendor:
NetApp

Family:
V-Series

Serial Number:
1306894

IP:
192.168.7.41

Virtualized Type:
Virtual

Backend Storage:
Sym-000050074300343

Microcode Version:
8.0.2 7-Mode

Raw Capacity:
0.0 GiB

Latency - Total:
N/A

IOPS - Total:
N/A

Throughput - Total:
N/A

Management:

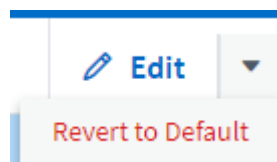
FC Fabrics Connected:
7

Alert Monitors:

Landing pages e dashboards existentes

Esteja ciente de que, se você tiver páginas de destino ou painéis personalizados no seu locatário, elas não mostrarão automaticamente todas as informações de virtualização por padrão. No entanto, você pode *reverter para o padrão* qualquer painel personalizado ou página de destino (você terá que reimplementar suas personalizações) ou modificar os widgets relevantes para incluir os atributos ou métricas de virtualização desejados.

Revert to Default está disponível no canto superior direito de um painel personalizado ou tela de página inicial.



Dicas e dicas para pesquisar ativos e alertas

Várias técnicas de pesquisa podem ser usadas para pesquisar dados ou objetos em seu ambiente monitorado.

- * Pesquisa de curinga*

Você pode realizar a pesquisa de caracteres curinga múltiplos usando o caractere *. Por exemplo, *applic*n* retornaria *application*.

- Frases usadas na busca

Uma frase é um grupo de palavras cercado por aspas duplas; por exemplo, "VNX LUN 5". Você pode usar aspas duplas para procurar documentos que contenham espaços em seus nomes ou atributos.

- Operadores booleanos

Usando operadores booleanos OU, E, e NÃO, você pode combinar vários termos para formar uma consulta mais complexa.

OU

O OPERADOR OU é o operador de conjunção predefinido.

Se não houver um operador booleano entre dois termos, o OPERADOR OR será usado.

O OPERADOR OR vincula dois termos e encontra um documento correspondente se algum dos termos existir em um documento.

Por exemplo, *storage OU NetApp* procura documentos que contenham *storage* ou *NetApp*.

Pontuações altas são dadas a documentos que correspondem à maioria dos termos.

E

Pode utilizar o operador E para localizar documentos nos quais existem ambos os termos de pesquisa num único documento. Por exemplo, *storage E NetApp* procura documentos que contenham *storage* e *NetApp*.

Pode utilizar o símbolo **&&** em vez da palavra e.

NÃO

Quando você usa o operador NOT, todos os documentos que contêm o termo depois DE NÃO são excluídos dos resultados da pesquisa. Por exemplo, *storage NOT NetApp* procura documentos que contenham apenas *storage* e não *NetApp*.

Você pode usar o símbolo ! em vez da palavra NÃO.

A pesquisa é insensível a maiúsculas e minúsculas.

Pesquisar usando termos indexados

Pesquisas que correspondem a mais dos termos indexados resultam em pontuações mais altas.

A cadeia de pesquisa é dividida em termos de pesquisa separados por espaço. Por exemplo, a cadeia de pesquisa "storage aurora NetApp" é dividida em três palavras-chave: "Storage", "aurora" e "NetApp". A pesquisa é realizada usando todos os três termos. Os documentos que correspondem à maioria destes termos terão a pontuação mais alta. Quanto mais informações você fornecer, melhores são os resultados da pesquisa. Por exemplo, você pode procurar um armazenamento pelo nome e modelo.

A IU exibe os resultados da pesquisa entre categorias, com os três melhores resultados por categoria. Se você não encontrou um objeto que estava esperando, você pode incluir mais termos na cadeia de caracteres de pesquisa para melhorar os resultados da pesquisa.

A tabela a seguir fornece uma lista de termos indexados que podem ser adicionados à cadeia de caracteres de pesquisa.

Categoria	Termos indexados
Armazenamento	modelo de fornecedor de nomes "storage"
StoragePool	Nome "storagepool" dos endereços IP de armazenamento do número de série de armazenamento dos nomes de modelo de armazenamento de dados do fornecedor de armazenamento para todos os nomes de volumes internos associados para todos os discos associados

Categoria	Termos indexados
Volume interno	Nome "internalvolume" dos endereços IP de armazenamento do número de série de armazenamento do nome do modelo de armazenamento do fornecedor de armazenamento dos nomes do conjunto de armazenamento de todos os nomes de partilha associados de todas as aplicações associadas
Volume	Nomes de etiquetas de nome "volume" de todos os volumes internos nome do conjunto de armazenamento nome dos endereços IP de armazenamento do número de série de armazenamento do modelo de armazenamento de dados do fornecedor de armazenamento
Nó de storage	Nome "storagenode" dos endereços IP de armazenamento do número de série de armazenamento do modelo de armazenamento do fornecedor de armazenamento
Host	Nomes de endereços IP de nome "host" de todos os aplicativos associados
Armazenamento de dados	Nome "datastore" nomes IP do centro virtual de todos os nomes de volumes de todos os volumes internos
Máquinas virtuais	Nome "virtualmachine" Nome DNS endereços IP nome dos endereços IP do host dos nomes de host de todos os nomes de datastores de todos os aplicativos associados
Interrutores (regular e NPV)	Endereço IP "switch" Nome wwn nome de série modelo nome de domínio ID nome da estrutura wwn da estrutura
Aplicação	linha de inquilino de nome "aplicação" do projeto de unidade de negócio
Fita	Fornecedor do número de série do nome do endereço IP "TAPE"
Porta	nome wwn "port"
Malha	nome wwn "tecido"
Máquina de Storage Virtual (SVM)	Nome "storagevirtualmachine" UUID

Relatórios

Visão geral do Relatório de Insights da infraestrutura de dados

Os relatórios do Data Infrastructure Insights são uma ferramenta de business intelligence que permite visualizar relatórios predefinidos ou criar relatórios personalizados.



O recurso relatórios está disponível no Data Infrastructure Insights ["Edição Premium"](#).

Com os relatórios do Data Infrastructure Insights, você pode executar as seguintes tarefas:

- Execute um relatório predefinido
- Crie um relatório personalizado
- Personalizar o formato e o método de entrega de um relatório
- Programe relatórios para serem executados automaticamente
- Relatórios por e-mail
- Use cores para representar limites nos dados

O Data Infrastructure Insights Reporting pode gerar relatórios personalizados para áreas como chargeback, análise de consumo e previsão, e pode ajudar a responder a perguntas como:

- Que inventário tenho?
- Onde está o meu inventário?
- Quem está usando nossos ativos?
- Qual é o chargeback para storage alocado para uma unidade de negócios?
- Por quanto tempo até que eu precise adquirir capacidade de armazenamento adicional?
- As unidades de negócios estão alinhadas ao longo das camadas de storage adequadas?
- Como a alocação de storage muda ao longo de um mês, trimestre ou ano?

Acessando o Data Infrastructure Insights Reporting

Você pode acessar o Data Infrastructure Insights Reporting clicando no link **relatórios** no menu.

Você será levado para a interface de relatórios. O Data Infrastructure Insights usa o IBM Cognos Analytics para seu mecanismo de relatórios.

O que é ETL?

Ao trabalhar com relatórios, você ouvirá os termos "Data Warehouse" e "ETL". ETL significa "Extract, Transform and Load" (extrair, transformar e carregar). O processo ETL recupera os dados coletados no Data Infrastructure Insights e transforma os dados em um formato para uso no Reporting. "Armazém de dados" refere-se aos dados recolhidos disponíveis para relatórios.

O processo ETL inclui estes processos individuais:

- **Extract:** Obtém dados do Data Infrastructure Insights.
- **Transform:** Aplica regras ou funções de lógica de negócios aos dados à medida que são extraídos do Data Infrastructure Insights.
- **Load:** Salva os dados transformados no data warehouse para uso no Reporting.

Funções de usuário do Data Infrastructure Insights Reporting

Se você tiver o Data Infrastructure Insights Premium Edition com relatórios, todos os usuários do Data Infrastructure Insights no seu local também terão um login único (SSO) no aplicativo relatórios (ou seja, Cognos). Basta clicar no link **relatórios** no menu e você será automaticamente conectado ao Reporting.

Sua função de usuário no Data Infrastructure Insights determina sua função de usuário de relatórios:

Função Data Infrastructure Insights	Função de relatório	Permissões de relatórios
Convidado	Consumidor	Pode visualizar, programar e executar relatórios e definir preferências pessoais, como as de idiomas e fusos horários. Os consumidores não podem criar relatórios ou executar tarefas administrativas.
Utilizador	Autor	Pode executar todas as funções de consumidor, bem como criar e gerenciar relatórios e painéis.
Administrador	Administrador	Pode executar todas as funções do autor, bem como todas as tarefas administrativas, tais como a configuração de relatórios e o encerramento e reinício das tarefas de relatório.

A tabela a seguir mostra as funções disponíveis para cada função de relatório.

Recurso	Consumidor	Autor	Administrador
Exibir relatórios na guia conteúdo da equipe	Sim	Sim	Sim
Execute relatórios	Sim	Sim	Sim
Agendar relatórios	Sim	Sim	Sim
Carregar ficheiros externos	Não	Sim	Sim
Criar trabalhos	Não	Sim	Sim
Crie histórias	Não	Sim	Sim
Crie relatórios	Não	Sim	Sim
Crie Pacotes e módulos de dados	Não	Sim	Sim
Executar tarefas administrativas	Não	Não	Sim
Adicionar/Editar item HTML	Não	Não	Sim
Executar relatório com item HTML	Sim	Sim	Sim
Adicionar/editar SQL personalizado	Não	Não	Sim
Execute relatórios com SQL personalizado	Sim	Sim	Sim

Configurando preferências de e-mail do Cognos (relatórios)

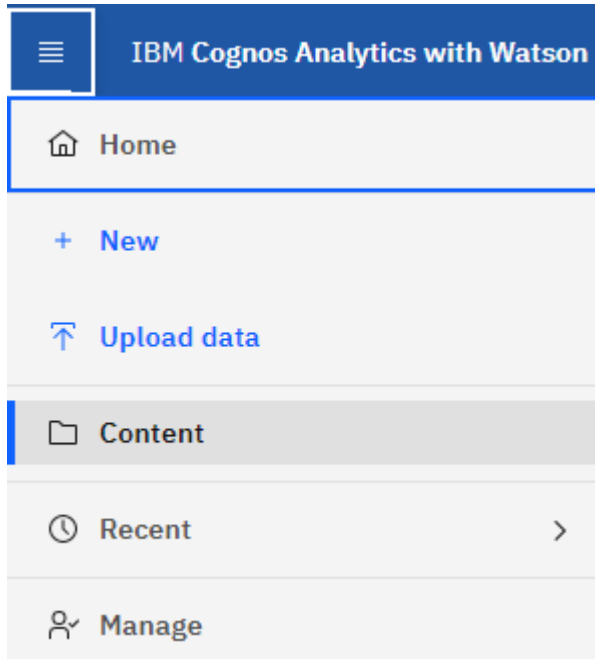


Se você alterar suas preferências de e-mail de usuário no Data Infrastructure Insights Reporting (ou seja, o aplicativo Cognos), essas preferências estarão ativas *somente para a sessão atual*. Fazer logout do Cognos e voltar a entrar irá redefinir as suas preferências de e-mail.

Que passos devo tomar para preparar o meu ambiente existente para ativar o SSO?

Para garantir que seus relatórios sejam mantidos, migre todos os relatórios de *meu conteúdo* para *conteúdo de equipe* usando as etapas a seguir. Você deve fazer isso antes de ativar o SSO no seu locatário:

1. Navegue até **Menu > conteúdo**



1. Crie uma nova pasta em **Team Content**
 - a. Se vários usuários tiverem sido criados, crie uma pasta separada para cada usuário para evitar a substituição de relatórios com nomes duplicados
2. Navegue até *meu conteúdo*
3. Selecione todos os relatórios que deseja manter.
4. No canto superior direito do menu, selecione "Copiar ou mover"
5. Navegue até a pasta recém-criada em *conteúdo da equipe*
6. Cole os relatórios na pasta recém-criada usando os botões "Copiar para" ou "mover para"
7. Quando o SSO estiver habilitado para o Cognos, faça login no Data Infrastructure Insights com o endereço de e-mail usado para criar sua conta.
8. Navegue até a pasta *conteúdo da equipe* dentro do Cognos e copie ou mova os relatórios salvos anteriormente de volta para *meu conteúdo*.

Relatórios predefinidos facilitados

O Data Infrastructure Insights Reporting inclui relatórios predefinidos que atendem a vários requisitos comuns de relatórios, fornecendo insights críticos de que as partes

interessadas precisam para tomar decisões informadas sobre sua infraestrutura de storage.



O recurso relatórios está disponível no Data Infrastructure Insights "Edição Premium".

Você pode gerar relatórios predefinidos a partir do Data Infrastructure Insights Reporting Portal, enviá-los por e-mail para outros usuários e até modificá-los. Vários relatórios permitem que você filtre por dispositivo, entidade de negócios ou nível. As ferramentas de relatórios usam o IBM Cognos como base e oferecem muitas opções de apresentação de dados.

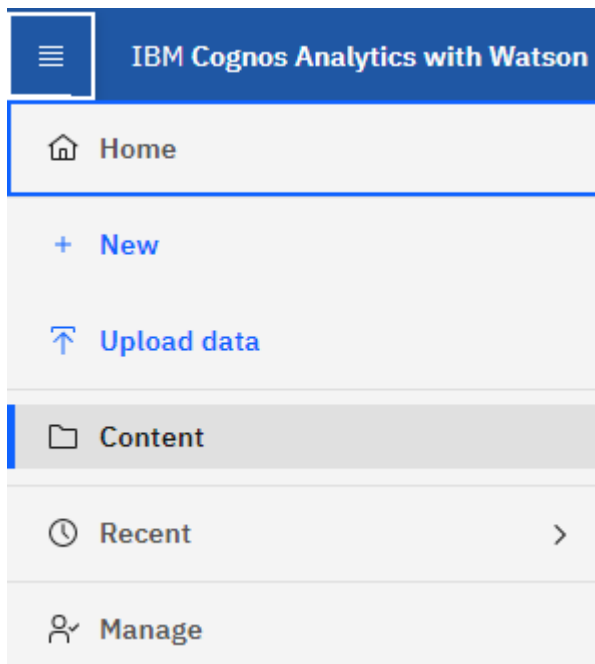
Os relatórios predefinidos mostram seus dados de inventário, capacidade de storage, chargeback, performance, eficiência de storage e custos de nuvem. Você pode modificar esses relatórios predefinidos e salvar suas modificações.

Você pode gerar relatórios em vários formatos, incluindo HTML, PDF, CSV, XML e Excel.

Navegar para relatórios predefinidos

Quando você abre o Portal de relatórios, a pasta *conteúdo da equipe* é o ponto de partida para selecionar o tipo de informação que você precisa nos relatórios Insights da infraestrutura de dados.

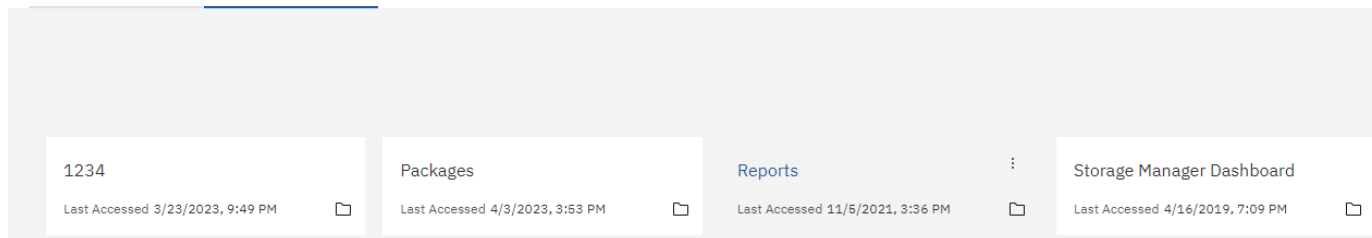
1. No painel de navegação à esquerda, selecione **Content > Team Content**.
2. Selecione **relatórios** para acessar os relatórios predefinidos.



Content

My content

Team content



Usando relatórios predefinidos para responder perguntas comuns

Os seguintes relatórios predefinidos estão disponíveis em **conteúdo da equipe > relatórios**.

Capacidade e desempenho do nível de serviço de aplicações

O relatório capacidade e desempenho do nível de Serviço do aplicativo fornece uma visão geral de alto nível de seus aplicativos. Você pode usar essas informações para Planejamento de capacidade ou para um plano de migração.

Chargeback

O relatório Chargeback fornece informações de chargeback de capacidade de storage e responsabilidade por hosts, aplicações e entidades empresariais, além de incluir dados atuais e históricos.

Para evitar a contagem dupla não inclua servidores ESX, monitore apenas as VMs.

Fontes de dados

O relatório fontes de dados mostra todas as fontes de dados que estão instaladas no seu site, o status da fonte de dados (sucesso/falha) e as mensagens de status. O relatório fornece informações sobre onde começar a solucionar problemas de fontes de dados. As fontes de dados falhadas afetam a precisão do relatório e a usabilidade geral do produto.

Desempenho do ESX vs VM

O relatório de desempenho do ESX vs VM fornece uma comparação entre servidores ESX e VMs, mostrando IOPs médios e de pico, taxa de transferência e latência e utilizações para servidores e VMs ESX. Para evitar a contagem dupla, exclua os servidores ESX; inclua somente as VMs. Uma versão atualizada deste relatório está disponível no repositório de automação do storage da NetApp.

Resumo da malha

O relatório Resumo da malha identifica informações de switches e switches, incluindo contagens de portas, versões de firmware e status da licença. O relatório não inclui portas de comutação NPV.

HBAs de host

O relatório HBAs do host fornece uma visão geral dos hosts no ambiente e fornece a versão do fornecedor, modelo e firmware dos HBAs e o nível de firmware dos switches aos quais estão conectados. Este relatório pode ser usado para analisar a compatibilidade do firmware ao Planejar uma atualização de firmware para um switch ou HBA.

Capacidade e desempenho do nível de serviço de host

O relatório capacidade e desempenho de nível de serviço do host fornece uma visão geral da utilização do storage por host para aplicativos somente de bloco.

Resumo do host

O relatório Resumo do host fornece uma visão geral da utilização do storage por cada host selecionado com informações para hosts Fibre Channel e iSCSI. O relatório permite comparar portas e caminhos, a capacidade de Fibre Channel e iSCSI e contagens de violações.

Detalhes da licença

O relatório Detalhes da licença mostra a quantidade de recursos para os quais você está licenciado em todos os sites com licenças ativas. O relatório também mostra uma soma da quantidade real em todos os sites com licenças ativas. A soma pode incluir sobreposições de matrizes de armazenamento geridas por vários servidores.

Volumes mapeados, mas não mascarados

O relatório volumes mapeados, mas não mascarados, lista os volumes cujo número de unidade lógica (LUN) foi mapeado para uso por um host específico, mas não está mascarado para esse host. Em alguns casos, esses LUNs podem ser desativados que foram desmascarados. Volumes desmascarados podem ser acessados por qualquer host, tornando-os vulneráveis à corrupção de dados.

Capacidade e performance do NetApp

O relatório capacidade e desempenho do NetApp fornece dados globais para capacidade alocada, utilizada e comprometida com dados de tendências e desempenho para a capacidade do NetApp.

Cartão de pontuação

O relatório do Scorecard fornece um resumo e o status geral de todos os ativos adquiridos pelo Data Infrastructure Insights. O estado é indicado com sinalizadores verde, amarelo e vermelho:

- Verde indica a condição normal
- Amarelo indica um problema potencial no ambiente
- Vermelho indica um problema que requer atenção

Todos os campos do relatório são descritos no Dicionário de dados fornecido com o relatório.

Resumo de armazenamento

O relatório Resumo do storage fornece um resumo global dos dados de capacidade usados e não utilizados para volumes e pools de storage brutos, alocados. Este relatório fornece uma visão geral de todo o armazenamento descoberto.

Capacidade e performance de VM

Descreve o ambiente de máquina virtual (VM) e seu uso de capacidade. As ferramentas de VM devem estar habilitadas para visualizar alguns dados, como quando as VMs foram desativadas.

Caminhos de VM

O relatório de caminhos de VM fornece dados de capacidade de armazenamento de dados e métricas de desempenho para as quais a máquina virtual está sendo executada em qual host, quais hosts estão acessando quais volumes compartilhados, qual é o caminho de acesso ativo e o que compreende alocação e uso de capacidade.

Capacidade do HDS por thin Pool

O relatório capacidade do HDS por thin Pool mostra a quantidade de capacidade utilizável em um pool de storage que é thin Provisioning.

Capacidade de NetApp por agregado

O relatório capacidade por agregado do NetApp mostra o total bruto, total, usado, disponível e comprometido dos agregados.

Symmetrix capacidade por thick Array

O relatório Symmetrix Capacity by Thick Array mostra capacidade bruta, capacidade utilizável, capacidade livre, mapeada, mascarada e capacidade livre total.

Symmetrix capacidade por Thin Pool

O relatório Symmetrix Capacity by Thin Pool mostra a capacidade bruta, a capacidade utilizável, a capacidade usada, a capacidade livre, a porcentagem usada, a capacidade subscrita e a taxa de assinatura.

XIV capacidade por Array

O relatório XIV Capacity by Array mostra a capacidade usada e não utilizada para o array.

XIV capacidade por Piscina

O relatório XIV capacidade por pool mostra a capacidade usada e não utilizada para pools de armazenamento.

Dashboard do Storage Manager

O Storage Manager Dashboard fornece uma visualização centralizada que permite comparar e contrastar o uso de recursos ao longo do tempo com os intervalos aceitáveis e os dias anteriores de atividade. Mostrando apenas as principais métricas de performance dos seus serviços de storage, você pode tomar decisões sobre como manter seus data centers.



O recurso relatórios está disponível no Data Infrastructure Insights ["Edição Premium"](#).

Resumo

Selecionar **Storage Manager Dashboard** no Team Content fornece vários relatórios que fornecem informações sobre o seu tráfego e armazenamento.

Storage Manager Dashboard

My content | **Team content**

Team content / Storage Manager Dashboard

Data Center Traffic Details

Last Accessed: 4/17/2019, 6:47 PM

Orphaned Storage Details

Last Accessed: 5/2/2019, 8:30 PM

[Storage Manager Report](#)

Last Accessed: 12/17/2019, 9:44 PM

Storage Pools Capacity and Performance Details

Last Accessed: 4/17/2019, 6:47 PM

Para uma visualização rápida, o **Storage Manager Report** inclui sete componentes que contêm informações contextuais sobre muitos aspectos do seu ambiente de armazenamento. Você pode detalhar os aspectos de seus serviços de storage para realizar uma análise aprofundada de uma seção que mais lhe interessa.

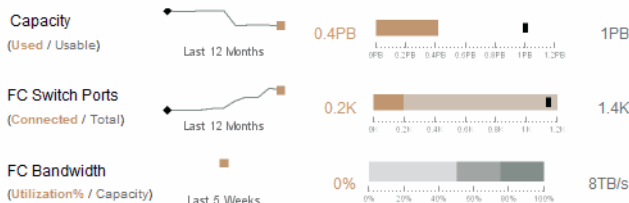
Public Folders | My Folders | **Storage Manager Dashboard**

NetApp Storage Manager Dashboard

(Data as of Jan 28, 2016)

Summary

History (Target, Actual, Forecast, Low, Mid, High)



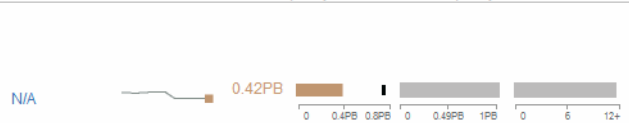
Data Centers Time to Full

(<3 months, 3-6 months, >6 months)



Storage Tiers Capacity

Last 12 Months Used Capacity Total Capacity Months to Full



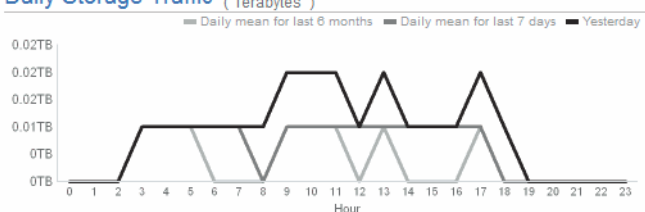
Top 10 Applications

Last 12 Months Used Allocated Response Time (Acceptable)

Application	Last 12 Months	Used	Allocated	Response Time
Hadoop	■	11.7TB	■	1ms
Applicatio..	—	0.2TB	■	0ms
Applicatio..	■	0TB	■	3ms
Applicatio..	■	0TB	■	2ms
JUICE	—	0TB	■	2ms
Saprox4	■	0TB	■	1ms
Twilight	—	0TB	■	1ms

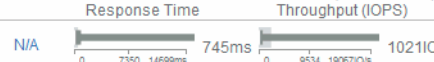
Daily Storage Traffic

(Terabytes) Daily mean for last 6 months, Daily mean for last 7 days, Yesterday



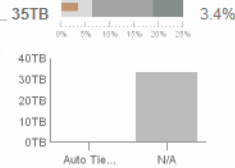
Storage Tiers Daily Performance

(Acceptable) Response Time Throughput (IOPS)



Orphaned Capacity

35TB 3.4%



Esse componente mostra a capacidade de storage usada versus a capacidade utilizável, o total de portas do switch versus o número de portas do switch conectadas e a utilização total de portas do switch conectadas versus a largura de banda total e como cada uma dessas tendências ao longo do tempo. Você pode visualizar a utilização real em comparação com as faixas baixa, média e alta, o que permite comparar e contrastar o uso

entre projeções e as ações desejadas, com base em um alvo. Para portas de capacidade e switch, você pode configurar esse destino. A previsão é baseada em uma extrapolação da taxa de crescimento atual e da data definida. Quando a capacidade usada prevista, que é baseada na data de projeção de uso futuro, excede o alvo, um alerta (círculo vermelho sólido) aparece ao lado da capacidade.

Capacidade das camadas de storage

Esse componente mostra a capacidade do nível usada em comparação com a capacidade alocada ao nível, o que indica como a capacidade usada aumenta ou diminui em um período de 12 meses e quantos meses restam para a capacidade total. O uso da capacidade é exibido com os valores fornecidos para o uso real, a previsão de uso e um destino para a capacidade, que você pode configurar. Quando a capacidade usada prevista, que é baseada na data de projeção de uso futuro, excede a capacidade alvo, um alerta (círculo vermelho sólido) aparece ao lado de um nível.

Você pode clicar em qualquer camada para exibir o relatório Detalhes de desempenho e capacidade dos pools de storage, que mostra as capacidades gratuitas versus as usadas, o número de dias completos e os detalhes de desempenho (IOPS e tempo de resposta) de todos os pools na camada selecionada. Você também pode clicar em qualquer nome de conjunto de armazenamento ou armazenamento neste relatório para exibir a página de ativos resumindo o estado atual desse recurso.

Tráfego de armazenamento diário

Esse componente mostra como o ambiente está se saindo, se houver algum grande crescimento, mudanças ou problemas potenciais em comparação com os seis meses anteriores. Também mostra o tráfego médio versus o tráfego nos sete dias anteriores e no dia anterior. Você pode visualizar quaisquer anormalidades na performance da infraestrutura porque ela fornece informações que destacam variações cíclicas (sete dias anteriores) e sazonais (seis meses anteriores).

Pode clicar no título (tráfego de armazenamento diário) para apresentar o relatório Detalhes de tráfego de armazenamento, que mostra o mapa de calor do tráfego de armazenamento por hora para o dia anterior para cada sistema de armazenamento. Clique em qualquer nome de armazenamento neste relatório para exibir a página de ativos resumindo o estado atual desse recurso.

Data centers Time to Full

Esse componente mostra todos os data centers em vez de todas as categorias e quanta capacidade resta em cada data center para cada camada de storage com base em taxas de crescimento previstas. O nível de capacidade de nível é mostrado em azul; quanto mais escura a cor, menor o tempo que o nível no local deixou antes de estar cheio.

Você pode clicar em uma seção de um nível para exibir o relatório dias a detalhes completos dos pools de storage, que mostra a capacidade total, a capacidade livre e o número de dias a serem preenchidos para todos os pools na camada selecionada e no data center. Clique em qualquer nome de conjunto de armazenamento ou armazenamento neste relatório para exibir a página de ativos resumindo o estado atual desse recurso.

Top 10 aplicações

Este componente mostra as 10 principais aplicações com base na capacidade utilizada. Independentemente de como o nível organiza os dados, essa área exibe a capacidade usada atual e o compartilhamento da infraestrutura. Você pode visualizar o intervalo de experiência do usuário para os sete dias anteriores para ver se os consumidores experimentam tempos de resposta aceitáveis (ou, mais importante, inaceitáveis).

Essa área também mostra tendências, o que indica se os aplicativos atendem aos seus objetivos de nível de serviço (SLO) de desempenho. Você pode visualizar o tempo mínimo de resposta da semana anterior, o

primeiro quartil, o terceiro quartil e o tempo máximo de resposta, com uma mediana mostrada contra um SLO aceitável, que você pode configurar. Quando o tempo de resposta médio para qualquer aplicação está fora do intervalo de SLO aceitável, um alerta (círculo vermelho sólido) aparece ao lado da aplicação. Você pode clicar em um aplicativo para exibir a página de ativo resumindo o estado atual desse recurso.

Desempenho diário das camadas de armazenamento

Este componente mostra um resumo do desempenho da categoria para o tempo de resposta e IOPS nos sete dias anteriores. Essa performance é comparada a um SLO que você pode configurar. Assim, você pode ver se há oportunidade de consolidar camadas, realinhar workloads nessas camadas ou identificar problemas em categorias específicas. Quando o tempo de resposta mediano ou o IOPS mediano estão fora do intervalo de SLO aceitável, um alerta (círculo vermelho sólido) aparece ao lado de um nível.

Você pode clicar no nome de um nível para exibir o relatório Detalhes de desempenho e capacidade dos pools de storage, que mostra as capacidades livres versus as usadas, o número de dias completos e os detalhes de performance (IOPS e tempo de resposta) de todos os pools no nível selecionado. Clique em qualquer conjunto de armazenamento ou armazenamento neste relatório para exibir a página de ativos resumindo o estado atual desse recurso.

Capacidade órfã

Esse componente mostra a capacidade órfã total e a capacidade órfã por nível, comparando-a com faixas aceitáveis para a capacidade utilizável total e mostrando a capacidade real órfã. A capacidade órfã é definida pela configuração e pelo desempenho. O storage órfão pela configuração descreve uma situação em que há armazenamento alocado a um host. No entanto, a configuração não foi executada corretamente e o host não pode acessar o armazenamento. Órfão pelo desempenho é quando o armazenamento está configurado corretamente para ser acessado por um host. No entanto, não houve tráfego de armazenamento.

A barra horizontal empilhada mostra os intervalos aceitáveis. Quanto mais escuro o cinza, mais inaceitável é a situação. A situação real é mostrada com a barra de bronze estreita que mostra a capacidade real que é órfã.

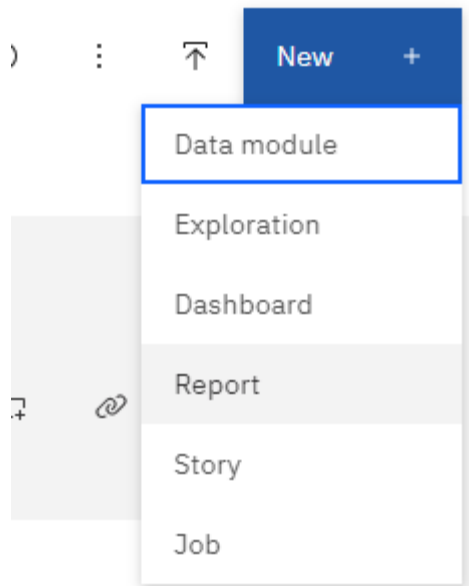
Você pode clicar em um nível para exibir o relatório Detalhes do armazenamento órfão, que mostra todos os volumes identificados como órfãos pela configuração e desempenho do nível selecionado. Clique em qualquer armazenamento, pool de armazenamento ou volume neste relatório para exibir a página de ativos resumindo o estado atual desse recurso.

Criando um relatório (exemplo)

Siga as etapas neste exemplo para gerar um relatório simples sobre a capacidade física de pools de armazenamento e armazenamento em vários data centers.

Passos

1. Navegue até **Menu > conteúdo > conteúdo da equipe > relatórios**
2. No canto superior direito do ecrã, selecione **[novo]**
3. Selecione **Relatório**



4. Na guia **Templates**, selecione *blank*

As guias fonte e dados são exibidas

5. Abrir **Selecione uma fonte**

6. Em **conteúdo da equipe**, abra **Pacotes**

É apresentada uma lista de pacotes disponíveis.

7. Escolha **capacidade do pool de armazenamento e armazenamento**

The screenshot shows a 'Select a source' dialog on the left with a 'Select a source +' button. On the right, the 'Open' window displays 'Team content' / Packages. Below is a table of available packages:

Name	Type	Last Accessed
Host Volume Hourly Performance	Package	6/25/2021, 9:36 PM
Internal Volume Capacity	Package	11/4/2021, 4:23 PM
Internal Volume Daily Performance	Package	1/7/2022, 4:23 PM
Internal Volume Hourly Performance	Package	1/6/2022, 11:41 PM
Inventory	Package	12/17/2019, 9:22 PM
Port Capacity	Package	11/20/2019, 4:13 PM
Qtree Capacity	Package	11/4/2021, 6:07 PM
Qtree Performance	Package	11/4/2021, 11:07 PM
Storage and Storage Pool Capacity	Package	12/17/2019, 5:58 PM
Storage Efficiency	Package	12/17/2019, 9:17 PM
Storage Node Capacity	Package	1/13/2023, 4:09 PM
Storage Node Performance	Package	1/13/2023, 6:11 PM

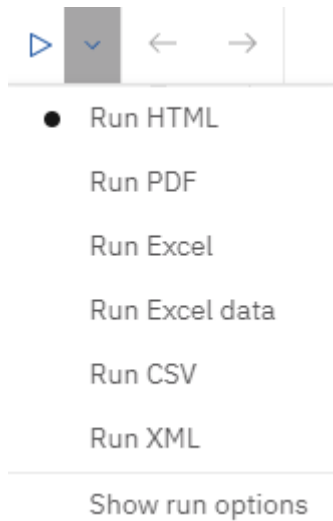
8. Selecione **Open**

Os estilos disponíveis para o seu relatório são exibidos.

9. Selecione **Lista**

Adicione nomes apropriados para Lista e consulta

10. Selecione **OK**
11. Expanda *capacidade física*
12. Expanda para o nível mais baixo de *Data Center*
13. Arraste *Data Center* para o Palato de relatórios.
14. Expanda *capacidade (MB)*
15. Arraste *capacidade (MB)* para o Palato de relatórios.
16. Arraste *Used Capacity (MB)* para o Palato de relatórios.
17. Execute o relatório selecionando um tipo de saída no menu **Run**.



Resultado

É criado um relatório semelhante ao seguinte:

	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

Top
 Page up
 Page down
 Bottom

Gerenciando relatórios

Você pode personalizar o formato de saída e a entrega de um relatório, definir propriedades ou horários do relatório e relatórios de e-mail.



O recurso relatórios está disponível no Data Infrastructure Insights "Edição Premium".

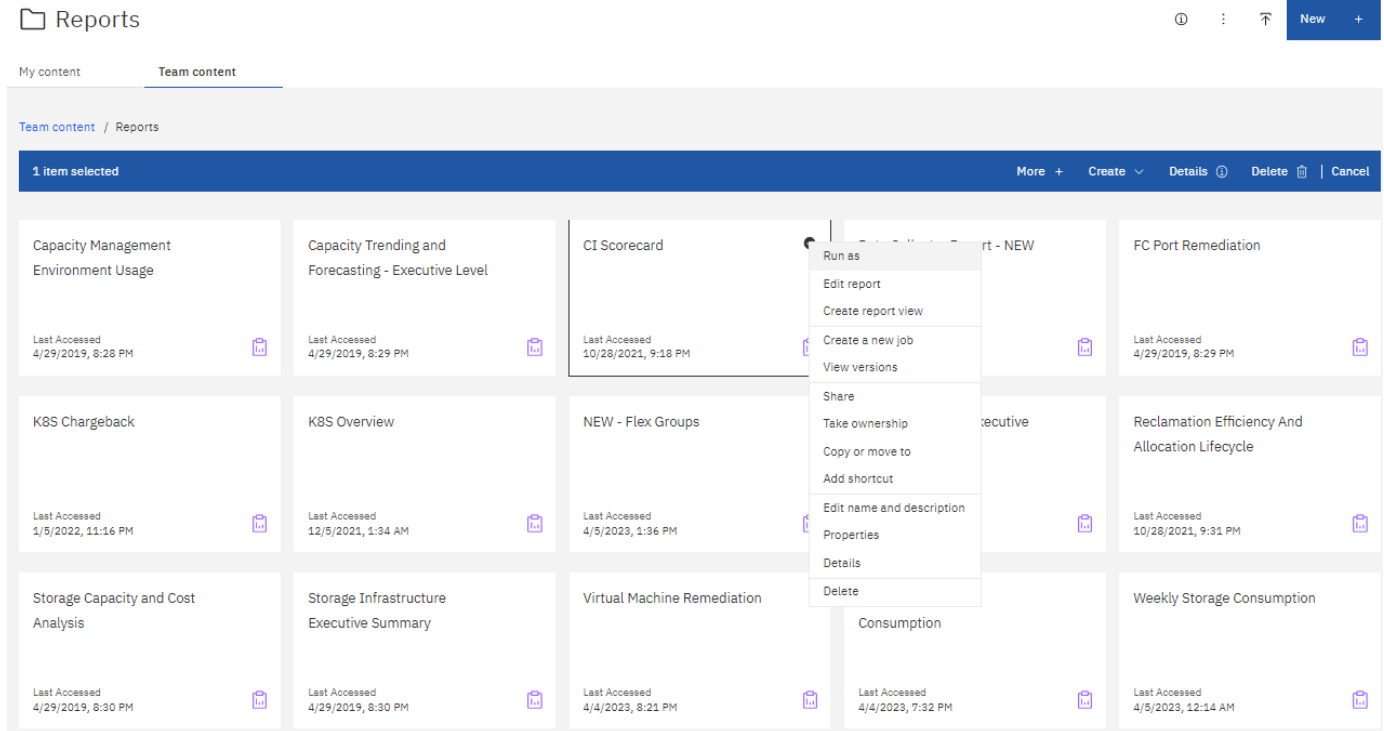


Antes de fazer alterações nas permissões de relatórios ou na segurança, você deve copiar os relatórios "meu conteúdo" para a pasta "conteúdo da equipe" para garantir que os relatórios sejam salvos.

Personalizar o formato de saída e a entrega de um relatório

Você pode personalizar o formato e o método de entrega dos relatórios.

1. No Portal de relatórios do Data Infrastructure Insights, vá para **Menu > conteúdo > meu conteúdo/conteúdo da equipe**. Passe o Mouse sobre o relatório que você deseja personalizar e abra o menu "três pontos".

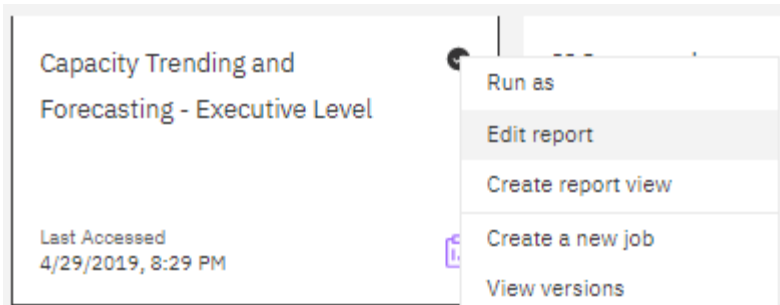


1. Clique em **Propriedades > Programação**
2. Pode definir as seguintes opções:
 - **Agendar** quando quiser que os relatórios sejam executados.
 - Escolha **Opções** para o formato e entrega do relatório (Salvar, Imprimir, e-mail) e idiomas para o relatório.
3. Clique em **Salvar** para produzir o relatório usando as seleções feitas.

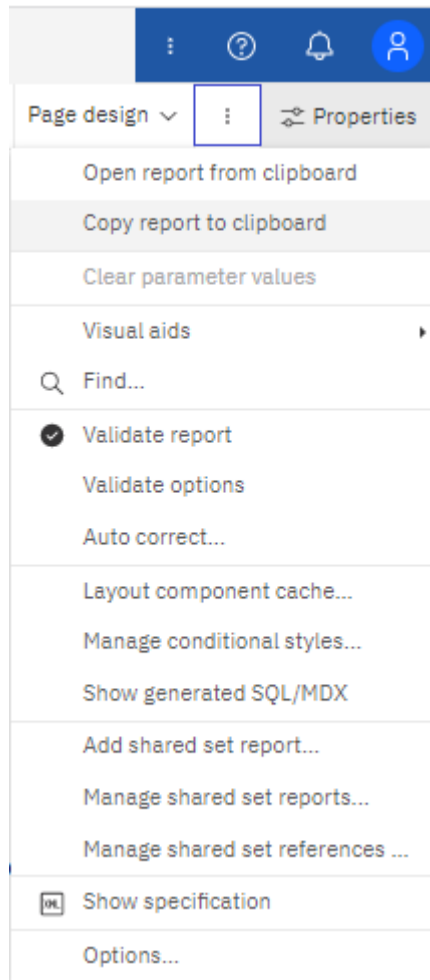
Copiar um relatório para a área de transferência

Use este processo para copiar um relatório para a área de transferência.

1. Selecione um relatório para copiar de (**Menu > conteúdo > meu conteúdo ou conteúdo da equipe**)
2. Escolha *Editar relatório* no menu suspenso do relatório



3. No canto superior direito da tela, abra o menu "três pontos" ao lado de "Propriedades".
4. Selecione **Copiar relatório para a área de transferência**.

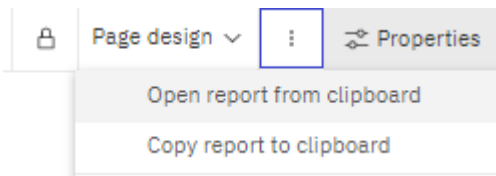


Abrindo relatórios da área de transferência

Você pode abrir uma especificação de relatório que foi copiada anteriormente para a área de transferência.

Sobre esta tarefa Comece criando um novo relatório ou abrindo um relatório existente que você deseja substituir pelo relatório copiado. As etapas abaixo são para um novo relatório.

1. Selecione **Menu > novo > Relatório** e crie um relatório em branco.
2. No canto superior direito da tela, abra o menu "três pontos" ao lado de "Propriedades".
3. Selecione **Open Report from Clipboard** (abrir relatório da área de transferência).



1. Cole o código copiado na janela e selecione **OK**.
2. Selecione o ícone de disquete para salvar o relatório.
3. Escolha onde salvar o relatório (*My Content*, *Team Content*, ou crie uma nova pasta).
4. Dê ao novo relatório um nome significativo e selecione **Salvar**.

Editar um relatório existente

Esteja ciente de que a edição de arquivos em seu local padrão corre o risco de esses relatórios serem substituídos na próxima atualização do catálogo de relatórios. Recomenda-se salvar o relatório editado com um novo nome ou armazená-lo em um local não padrão.

Solução de problemas

Aqui você encontrará sugestões para solucionar problemas com relatórios.

Problema:	Tente isto:
Ao agendar um relatório para ser enviado por e-mail, o nome do usuário conectado é preenchido previamente para o campo "para" do e-mail. No entanto, o nome está na forma de "nome próprio lastname" (nome próprio, espaço, sobrenome). Como esse não é um endereço de e-mail válido, o e-mail não será enviado quando o relatório programado for executado.	Ao agendar o relatório para ser enviado por e-mail, limpe o nome pré-preenchido e insira um endereço de e-mail válido e formatado corretamente no campo "para".

Criando relatórios personalizados

Você pode usar as ferramentas de criação de relatórios para criar relatórios personalizados. Depois de criar relatórios, você pode salvá-los e executá-los em um horário regular. Os resultados dos relatórios podem ser enviados automaticamente por e-mail para você e para os outros.



O recurso relatórios está disponível no Data Infrastructure Insights ["Edição Premium"](#).

Os exemplos nesta seção mostram o seguinte processo, que pode ser usado para qualquer um dos modelos de dados de relatórios de Insights de infraestrutura de dados:

- Identificar uma pergunta a ser respondida com um relatório
- Determinando os dados necessários para dar suporte aos resultados
- Selecionar elementos de dados para o relatório

Antes de projetar seu relatório personalizado, você precisa concluir algumas tarefas pré-requisitos. Se você não concluir estes, os relatórios podem estar imprecisos ou incompletos.

Por exemplo, se você não terminar o processo de identificação do dispositivo, seus relatórios de capacidade não serão precisos. Ou, se você não terminar de definir anotações (como camadas, unidades de negócios e data centers), seus relatórios personalizados podem não relatar dados com precisão em todo o domínio ou podem mostrar "N/A" para alguns pontos de dados.

Antes de criar seus relatórios, execute as seguintes tarefas:

- Configure tudo "[coletores de dados](#)" corretamente.
- Insira anotações (como camadas, data centers e unidades de negócios) em dispositivos e recursos do locatário. É benéfico ter anotações estáveis antes de gerar relatórios, porque o Data Infrastructure Insights Reporting coleta informações históricas.

Processo de criação de relatórios

O processo de criação de relatórios personalizados (também chamados de "ad hoc") envolve várias tarefas:

- Planeje os resultados do seu relatório.
- Identifique dados para apoiar seus resultados.
- Selecione o modelo de dados (por exemplo, modelo de dados de Chargeback, modelo de dados de inventário, etc.) que contenha os dados.
- Selecione elementos de dados para o relatório.
- Opcionalmente, formate, ordene e filtre os resultados do relatório.

Planejando os resultados do seu Relatório Personalizado

Antes de abrir as ferramentas de criação de relatórios, talvez você queira Planejar os resultados desejados no relatório. Com as ferramentas de criação de relatórios, você pode criar relatórios facilmente e pode não precisar de muito Planejamento; no entanto, é uma boa ideia ter uma ideia do solicitante do relatório sobre os requisitos do relatório.

- Identifique a pergunta exata que você deseja responder. Por exemplo:
 - Quanta capacidade tenho deixado?
 - Quais são os custos de estorno por unidade de negócios?
 - Qual é a capacidade por camada para garantir que as unidades de negócios estejam alinhadas ao nível adequado de storage?
 - Como posso prever requisitos de energia e refrigeração? (Adicione metadados personalizados adicionando anotações aos recursos.)
- Identifique os elementos de dados que você precisa para dar suporte à resposta.
- Identifique as relações entre os dados que você deseja ver na resposta. Não inclua relacionamentos ilógicos em sua pergunta, por exemplo, "Eu quero ver as portas que se relacionam com a capacidade".
- Identifique os cálculos necessários nos dados.
- Determine quais tipos de filtragem são necessários para limitar os resultados.
- Determine se você precisa usar dados atuais ou históricos.
- Determine se você precisa definir o Access Privileges em relatórios para limitar os dados a públicos específicos.
- Identificar como o relatório será distribuído. Por exemplo, ele deve ser enviado por e-mail em um cronograma definido ou incluído na área de pasta conteúdo da equipe?

- Determine quem manterá o relatório. Isso pode afetar a complexidade do design.
- Crie um modelo do relatório.

Dicas para projetar relatórios

Várias dicas podem ser úteis quando você está projetando relatórios.

- Determine se você precisa usar dados atuais ou históricos.

A maioria dos relatórios só precisa informar sobre os dados mais recentes disponíveis no Data Infrastructure Insights.

- O Data Infrastructure Insights Reporting fornece informações históricas sobre a capacidade e o desempenho, mas não sobre o inventário.
- Todo mundo vê todos os dados; no entanto, você pode precisar limitar os dados a públicos específicos.

Para segmentar as informações para diferentes usuários, você pode criar relatórios e definir permissões de acesso neles.

Modelos de dados de relatórios

O Data Infrastructure Insights inclui vários modelos de dados a partir dos quais você pode selecionar relatórios predefinidos ou criar seu próprio relatório personalizado.

Cada modelo de dados contém um data mart simples e um data mart avançado:

- O simples data mart fornece acesso rápido aos elementos de dados mais comumente usados e inclui apenas o último snapshot dos dados do Data Warehouse; ele não inclui dados históricos.
- O avançado data mart fornece todos os valores e detalhes disponíveis a partir do simples data mart e inclui acesso a valores históricos de dados.

Modelos de dados de capacidade

Permite que você responda a perguntas sobre capacidade de storage, utilização do sistema de arquivos, capacidade de volume interno, capacidade da porta, capacidade de qtree e capacidade de máquina virtual (VM). O modelo de dados de capacidade é um contêiner para vários modelos de dados de capacidade. Você pode criar relatórios respondendo a vários tipos de perguntas usando este modelo de dados:

Modelo de dados de capacidade de pool de storage e storage

Permite que você responda a perguntas sobre o Planejamento de recursos de capacidade de storage, incluindo pools de storage e storage, além de incluir dados de pool de storage físico e virtual. Esse modelo de dados simples pode ajudar você a responder a perguntas relacionadas à capacidade física e ao uso da capacidade de pools de storage por camada e data center ao longo do tempo. Se você é novo no relatório de capacidade, deve começar com esse modelo de dados porque é um modelo de dados mais simples e direcionado. Você pode responder perguntas semelhantes às seguintes usando este modelo de dados:

- Qual é a data projetada para atingir o limite de capacidade de 80% do meu storage físico?
- Qual é a capacidade de storage físico em um array para uma determinada camada?
- Qual é a minha capacidade de armazenamento por fabricante e família, bem como por data center?
- Qual é a tendência de utilização do storage em um array para todas as camadas?

- Quais são os meus 10 principais sistemas de storage com maior utilização?
- Qual é a tendência de utilização do storage dos pools de storage?
- Quanta capacidade já está alocada?
- Que capacidade está disponível para alocação?

Modelo de dados de utilização do sistema de arquivos

Esse modelo de dados fornece visibilidade sobre a utilização de capacidade por hosts no nível do sistema de arquivos. Os administradores podem determinar a capacidade alocada e usada por sistema de arquivos, determinar o tipo de sistema de arquivos e identificar estatísticas de tendências por tipo de sistema de arquivos. Você pode responder às seguintes perguntas usando este modelo de dados:

- Qual é o tamanho do sistema de arquivos?
- Onde os dados são mantidos e como eles são acessados, por exemplo, local ou SAN?
- Quais são as tendências históricas para a capacidade do sistema de arquivos? Então, com base nisso, o que podemos prever para as necessidades futuras?

Modelo de dados de capacidade de volume interno

Permite que você responda a perguntas sobre o volume interno usado, a capacidade alocada e o uso da capacidade ao longo do tempo:

- Que volumes internos têm uma utilização superior a um limite predefinido?
- Que volumes internos correm o risco de ficar sem capacidade com base numa tendência? Qual é a capacidade usada versus a capacidade alocada em nossos volumes internos?

Modelo de dados de capacidade da porta

Permite que você responda perguntas sobre conectividade da porta do switch, status da porta e velocidade da porta ao longo do tempo. Você pode responder perguntas semelhantes às seguintes para ajudá-lo a planejar a compra de novos switches: Como posso criar uma previsão de consumo de porta que preveja a disponibilidade de recursos (portas) (de acordo com o data center, fornecedor de switch e velocidade da porta)?

- Quais portas provavelmente ficarão sem capacidade, fornecendo velocidade de dados, data center, fornecedor e número de portas de host e storage?
- Quais são as tendências de capacidade da porta do switch ao longo do tempo?
- Quais são as velocidades da porta?
- Que tipo de capacidade de porta é necessária e que organização está prestes a ficar sem um determinado tipo de porta ou fornecedor?
- Qual é o momento ideal para comprar essa capacidade e disponibilizá-la?

Modelo de dados de capacidade Qtree

Permite que você reduza a utilização de qtree (com dados como a capacidade usada versus a capacidade alocada) ao longo do tempo. Você pode exibir as informações por dimensões diferentes, por exemplo, por entidade de negócios, aplicativo, nível e nível de serviço. Você pode responder às seguintes perguntas usando este modelo de dados:

- Qual é a capacidade usada para qtrees versus os limites definidos por aplicativo ou entidade de negócios?

- Quais são as tendências da nossa capacidade usada e livre para que possamos fazer o Planejamento de capacidade?
- Quais entidades de negócios estão usando mais capacidade?
- Quais aplicações consomem mais capacidade?

Modelo de dados de capacidade da VM

Permite que você comunique seu ambiente virtual e seu uso de capacidade. Esse modelo de dados permite gerar relatórios sobre alterações no uso da capacidade ao longo do tempo para VMs e armazenamentos de dados. O modelo de dados também fornece thin Provisioning e dados de chargeback da máquina virtual.

- Como posso determinar o chargeback de capacidade com base na capacidade provisionada para VMs e armazenamentos de dados?
- Que capacidade não é usada pelas VMs e que parte do não utilizado é livre, órfão ou outra?
- O que precisamos comprar com base nas tendências de consumo?
- Quais são as minhas economias em eficiência de storage obtidas com o uso de tecnologias de thin Provisioning e deduplicação de storage?

As capacidades no modelo de dados de capacidade da VM são retiradas de discos virtuais (VMDKs). Isso significa que o tamanho provisionado de uma VM usando o modelo de dados de capacidade da VM é o tamanho de seus discos virtuais. Isso é diferente da capacidade provisionada na visualização máquinas virtuais no Data Infrastructure Insights, que mostra o tamanho provisionado para a própria VM.

Modelo de dados de capacidade de volume

Permite analisar todos os aspectos dos volumes no locatário e organizar os dados por fornecedor, modelo, categoria, nível de serviço e data center.

Você pode visualizar a capacidade relacionada a volumes órfãos, volumes não utilizados e volumes de proteção (usados para replicação). Você também pode ver diferentes tecnologias de volume (iSCSI ou FC) e comparar volumes virtuais com volumes não virtuais para problemas de virtualização de storage.

Você pode responder perguntas semelhantes às seguintes com este modelo de dados:

- Que volumes têm uma utilização superior a um limite predefinido?
- Qual é a tendência no meu data center para capacidade de volume órfã?
- Quanto da capacidade do meu data center é virtualizada ou thin Provisioning?
- Quanto da capacidade do meu data center deve ser reservada para replicação?

Modelo de dados de chargeback

Permite que você responda perguntas sobre a capacidade usada e a capacidade alocada em recursos de armazenamento (volumes, volumes internos e qtrees). Esse modelo de dados fornece informações de chargeback de capacidade de storage e responsabilidade por hosts, aplicações e entidades de negócios, além de incluir dados atuais e históricos. Os dados do relatório podem ser categorizados por nível de serviço e camada de storage.

Você pode usar esse modelo de dados para gerar relatórios de chargeback encontrando a quantidade de capacidade usada por uma entidade de negócios. Esse modelo de dados permite criar relatórios unificados de vários protocolos (incluindo nas, SAN, FC e iSCSI).

- Para storage sem volumes internos, os relatórios de chargeback mostram chargeback por volumes.
- Para armazenamento com volumes internos:
 - Se as entidades empresariais forem atribuídas a volumes, os relatórios de chargeback mostrarão chargeback por volumes.
 - Se as entidades de negócios não forem atribuídas a volumes, mas atribuídas a qtrees, os relatórios de chargeback mostram chargeback por qtrees.
 - Se as entidades de negócios não forem atribuídas a volumes e não forem atribuídas a qtrees, os relatórios de chargeback mostrarão o volume interno.
 - A decisão de mostrar o chargeback por volume, qtree ou volume interno é tomada por cada volume interno, portanto, é possível que diferentes volumes internos no mesmo pool de storage mostrem o chargeback em diferentes níveis.

Os factos da capacidade são eliminados após um intervalo de tempo predefinido. Para obter detalhes, consulte processos de Data Warehouse.

Os relatórios que usam o modelo de dados Chargeback podem exibir valores diferentes dos relatórios que usam o modelo de dados de capacidade de armazenamento.

- Para storage arrays que não são sistemas de storage NetApp, os dados de ambos os modelos de dados são os mesmos.
- Para sistemas de armazenamento NetApp e Celerra, o modelo de dados de chargeback usa uma única camada (de volumes, volumes internos ou qtrees) para basear suas cobranças, enquanto o modelo de dados de capacidade de armazenamento usa várias camadas (de volumes e volumes internos) para basear suas cobranças.

Modelo de dados de inventário

Permite que você responda perguntas sobre recursos de inventário, incluindo hosts, sistemas de armazenamento, switches, discos, fitas, qtrees, cotas, máquinas e servidores virtuais e dispositivos genéricos. O modelo de dados de inventário inclui vários sub-marts que permitem visualizar informações sobre replicações, caminhos FC, caminhos iSCSI, caminhos NFS e violações. O modelo de dados de inventário não inclui dados históricos. Perguntas que você pode responder com esses dados

- Que ativos tenho e onde estão?
- Quem está usando os ativos?
- Que tipos de dispositivos tenho e quais são os componentes desses dispositivos?
- Quantos hosts por SO tenho e quantas portas existem nesses hosts?
- Quais arrays de storage por fornecedor existem em cada data center?
- Quantos switches por fornecedor tenho em cada data center?
- Quantas portas não são licenciadas?
- Quais fitas de fornecedores estamos usando e quantas portas existem em cada fita?re todos os dispositivos genéricos identificados antes de começarmos a trabalhar em relatórios?
- Quais são os caminhos entre hosts e volumes ou fitas de armazenamento?
- Quais são os caminhos entre dispositivos genéricos e volumes ou fitas de armazenamento?
- Quantas violações de cada tipo tenho por data center?
- Para cada volume replicado, quais são os volumes de origem e destino?

- Tenho alguma incompatibilidade de firmware ou incompatibilidade de velocidade de porta entre HBAs de host Fibre Channel e switches?

Modelo de dados de desempenho

Permite responder a perguntas sobre a performance de volumes, volumes de aplicações, volumes internos, switches, aplicações, VMs, VMDKs, ESX versus VM, hosts e nós de aplicações. Muitos desses reportam dados *Hourly*, *Daily* ou ambos. Usando esse modelo de dados, você pode criar relatórios que respondem a vários tipos de perguntas de gerenciamento de desempenho:

- Que volumes ou volumes internos não foram usados ou acessados durante um período específico?
- Podemos identificar qualquer potencial configuração incorreta para armazenamento de um aplicativo (não utilizado)?
- Qual foi o padrão geral de comportamento de acesso para um aplicativo?
- Os volumes em camadas são atribuídos apropriadamente para um determinado aplicativo?
- Poderíamos usar um storage mais barato para uma aplicação atualmente em execução sem afetar a performance da aplicação?
- Quais são os aplicativos que estão produzindo mais acessos ao armazenamento configurado atualmente?

Quando você usa as tabelas de desempenho do switch, você pode obter as seguintes informações:

- O tráfego do meu host por meio de portas conectadas é equilibrado?
- Quais switches ou portas estão exibindo um grande número de erros?
- Quais são os switches mais usados com base no desempenho da porta?
- Quais são os switches subutilizados com base no desempenho da porta?
- Qual é a taxa de transferência de tendências do host com base no desempenho da porta?
- Qual é a utilização de performance dos últimos X dias para um host, sistema de storage, fita ou switch especificados?
- Quais dispositivos estão produzindo tráfego em um switch específico (por exemplo, quais dispositivos são responsáveis pelo uso de um switch altamente utilizado)?
- Qual é a taxa de transferência para uma unidade de negócios específica em nosso ambiente?

Ao usar as tabelas de desempenho do disco, você pode obter as seguintes informações:

- Qual é a taxa de transferência para um pool de storage especificado com base em dados de desempenho de disco?
- Qual é o pool de storage mais usado?
- Qual é a utilização média de disco para um storage específico?
- Qual é a tendência de uso para um sistema de storage ou pool de storage com base em dados de desempenho de disco?
- Qual é a tendência de uso do disco para um pool de storage específico?

Ao usar tabelas de desempenho VM e VMDK, você pode obter as seguintes informações:

- O meu ambiente virtual está a funcionar de forma ideal?
- Quais VMDKs relatam as cargas de trabalho mais altas?

- Como posso usar o desempenho relatado de VMDs mapeados para diferentes datastores para tomar decisões sobre a redistribuição em camadas.

O modelo de dados de performance inclui informações que ajudam a determinar a adequação das camadas, configurações incorretas de storage das aplicações e últimos tempos de acesso de volumes e volumes internos. Esse modelo de dados fornece dados como tempos de resposta, IOPs, taxa de transferência, número de gravações pendentes e status acessado.

Modelo de dados de eficiência de storage

Permite controlar a pontuação e o potencial de eficiência de storage ao longo do tempo. Este modelo de dados armazena medições não apenas da capacidade provisionada, mas também da quantidade que é usada ou consumida (a medição física). Por exemplo, quando o thin Provisioning é ativado, o Data Infrastructure Insights indica a quantidade de capacidade obtida do dispositivo. Você também pode usar esse modelo para determinar a eficiência quando a deduplicação está ativada. Você pode responder a várias perguntas usando o data mart de eficiência de storage:

- Quais são nossas economias em eficiência de storage como resultado da implementação de tecnologias de thin Provisioning e deduplicação?
- Quais são as economias de storage nos data centers?
- Com base nas tendências históricas de capacidade, quando precisamos adquirir armazenamento adicional?
- Qual seria o ganho de capacidade se habilitássemos tecnologias como thin Provisioning e deduplicação?
- Quanto à capacidade de armazenamento, estou em risco agora?

Tabelas de fato e dimensões do modelo de dados

Cada modelo de dados inclui tabelas de fato e dimensão.

- Tabelas de fatos: Contêm dados medidos, por exemplo, quantidade, capacidade bruta e utilizável. Contém chaves estrangeiras para tabelas de dimensões.
- Tabelas dimensionais: Contêm informações descritivas sobre fatos, por exemplo, data center e unidades de negócios. Uma dimensão é uma estrutura, muitas vezes composta de hierarquias, que categoriza os dados. Atributos dimensionais ajudam a descrever os valores dimensionais.

Usando atributos de dimensão diferentes ou múltiplos (vistos como colunas nos relatórios), você constrói relatórios que acessam dados para cada dimensão descrita no modelo de dados.

Cores usadas em elementos de modelo de dados

As cores dos elementos do modelo de dados têm indicações diferentes.

- Ativos amarelos: Representam medições.
- Ativos não amarelos: Representam atributos. Esses valores não agregam.

Usando vários modelos de dados em um relatório

Normalmente, você usa um modelo de dados por relatório. No entanto, você pode escrever um relatório que combine dados de vários modelos de dados.

Para escrever um relatório que combine dados de vários modelos de dados, escolha um dos modelos de dados a utilizar como base e, em seguida, escreva consultas SQL para aceder aos dados a partir dos marts

de dados adicionais. Você pode usar o recurso junção SQL para combinar os dados das diferentes consultas em uma única consulta que você pode usar para escrever o relatório.

Por exemplo, digamos que você deseja a capacidade atual para cada storage array e deseja capturar anotações personalizadas nos arrays. Você pode criar o relatório usando o modelo de dados de capacidade de armazenamento. Você pode usar os elementos das tabelas de capacidade e dimensão atuais e adicionar uma consulta SQL separada para acessar as informações de anotações no modelo de dados de inventário. Finalmente, você pode combinar os dados vinculando os dados de armazenamento de inventário à tabela dimensão de armazenamento usando o nome de armazenamento e os critérios de associação.

Acesse o banco de dados de relatórios via API

A poderosa API do Data Infrastructure Insights permite que os usuários consultem diretamente o banco de dados de relatórios do Data Infrastructure Insights, sem passar pelo ambiente do Cognos Reporting.



Esta documentação refere-se ao recurso Relatório de Insights de infraestrutura de dados, que está disponível no Data Infrastructure Insights Premium Edition.

OData

A API Data Infrastructure Insights Reporting segue o "OData v4" padrão (Open Data Protocol) para consulta do banco de dados Reporting. Para mais informações ou para saber mais, consulte ["este tutorial"](#) OData.

Todas as solicitações começarão com o url *URL do Insights de infraestrutura do* `https://<Data>/REST/v1/dwh-management/odata`

Gerando uma APIKey

Leia mais sobre ["APIs do Data Infrastructure Insights"](#).

Para gerar uma chave de API, faça o seguinte:

- Inicie sessão no ambiente Data Infrastructure Insights e selecione **Admin > API Access**.
- Clique em "API Access Token".
- Introduza um nome e uma descrição.
- Para o tipo, escolha *Data Warehouse*.
- Definir permissões como leitura/gravação.
- Defina uma data de expiração de desejos.
- Clique em "Salvar", depois * copie a chave e salve-a* em algum lugar seguro. Você não poderá acessar a chave completa mais tarde.

APIkeys são bons para [Sync](#) ou [Async](#).

Consulta direta de tabelas

Com a chave API em vigor, as consultas diretas do banco de dados de relatórios agora são possíveis. URLs longos podem ser simplificados para o `https://.../odata/` para fins de exibição, em vez do URL completo do Insights de infraestrutura da `https://<Data>/REST/v1/dwh-management/odata/`

Tente consultas simples como

- URL >/REST/v1/dwh-Management/odata/dwh_custom https://<Data>
- URL >/REST/v1/dwh-Management/odata/dwh_inventory https://<Data>
- URL >/REST/v1/dwh-Management/odata/dwh_inventory/storage https://<Data>
- URL >/REST/v1/dwh-Management/odata/dwh_inventory/Disk https://<Data>
- https://.../odata/dwh_custom/custom_queries

Exemplos de API REST

O URL para todas as chamadas é *URL do Insights da infraestrutura da https://<Data>/REST/v1/dwh-management/odata*.

- GET /** - recupera dados do Banco de dados de relatórios.

Formato: *URL do Insights da infraestrutura da https://<Data>/REST/v1/dwh-Management/odata/<schema_name>/<query>*

Exemplo:

```
https://<domain>/rest/v1/dwh-  
management/odata/dwh_inventory/fabric?$count=true&$orderby=name  
Resultado:
```

```

{
  "@odata.context": "$metadata#fabric",
  "@odata.count": 2,
  "value": [
    {
      "id": 851,
      "identifiier": "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,
      "identifiier": "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"
    }
  ]
}

```

Dicas úteis

Tenha em mente o seguinte ao trabalhar com consultas de API de relatórios.

- O payload da consulta deve ser uma string JSON válida
- A carga útil da consulta deve estar contida em uma única linha
- Aspas duplas devem ser escapadas, ou seja, ""
- Os separadores são suportados como t
- Evite comentários
- Nomes de tabelas minúsculas são suportados

Além disso:

- São necessários colhedores 2:
 - Nome "X-CloudInsights-ApiKey"
 - Valor de atributo "<apikey>"

Sua chave de API será específica do seu ambiente Data Infrastructure Insights.

Síncrono ou assíncrono?

Por padrão, um comando API operará no modo *synchronous*, o que significa que você envia a solicitação e a resposta é retornada imediatamente. No entanto, às vezes uma consulta pode levar muito tempo para ser executada, o que pode levar ao tempo limite da solicitação. Para contornar isso, você pode executar uma solicitação *assincronamente*. No modo assíncrono, a solicitação retornará um URL através do qual a execução pode ser monitorada. O URL retornará o resultado quando estiver pronto.

Para executar uma consulta no modo assíncrono, adicione o cabeçalho **Prefer: respond-async** à solicitação. Após a execução bem-sucedida, a resposta conterá os seguintes cabeçalhos:

```
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>
```

Consultar o URL de localização retornará os mesmos cabeçalhos se a resposta ainda não estiver pronta, ou retornará com o status 200 se a resposta estiver pronta. O conteúdo da resposta será do tipo texto e contém o status http da consulta original e alguns metadados, seguidos pelos resultados da consulta original.

```
HTTP/1.1 200 OK
OData-Version: 4.0
Content-Type: application/json;odata.metadata=minimal
odataResponseSizeCounted: true

{ <JSON_RESPONSE> }
```

Para ver uma lista de todas as consultas assíncronas e quais delas estão prontas, use o seguinte comando:

```
GET https://<Data Infrastructure Insights URL>/rest/v1/dwh-
management/odata/dwh_custom/asyncList
A resposta tem o seguinte formato:
```

```

{
  "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
    }
  ]
}

```

Como os dados históricos são retidos para relatórios

O Data Infrastructure Insights retém os dados históricos para uso no relatório com base nos marts de dados e na granularidade dos dados, como mostrado na tabela a seguir.

Data mart	Objeto medido	Granularidade	Período de retenção
Desempenho marts	Volumes e volumes internos	Por hora	14 dias
Desempenho marts	Volumes e volumes internos	Diariamente	13 meses
Desempenho marts	Aplicação	Por hora	13 meses
Desempenho marts	Host	Por hora	13 meses
Desempenho marts	Desempenho do switch para a porta	Por hora	35 dias
Desempenho marts	Alterne o desempenho para host, armazenamento e fita	Por hora	13 meses
Desempenho marts	Nó de storage	Por hora	14 dias
Desempenho marts	Nó de storage	Diariamente	13 meses
Desempenho marts	Desempenho da VM	Por hora	14 dias
Desempenho marts	Desempenho da VM	Diariamente	13 meses
Desempenho marts	Desempenho de hipervisor	Por hora	35 dias
Desempenho marts	Desempenho de hipervisor	Diariamente	13 meses
Desempenho marts	Desempenho da VMDK	Por hora	35 dias
Desempenho marts	Desempenho da VMDK	Diariamente	13 meses

Desempenho marts	Desempenho de disco	Por hora	14 dias
Desempenho marts	Desempenho de disco	Diariamente	13 meses
Capacidade marts	Todos (exceto volumes individuais)	Diariamente	13 meses
Capacidade marts	Todos (exceto volumes individuais)	Representante mensal	14 meses e mais além
Marts de inventário	Volumes individuais	Estado atual	1 dia (ou até o próximo ETL)

Diagramas de esquema de relatórios do Insights da infraestrutura de dados

Este documento fornece os diagramas de esquema para o Banco de dados de relatórios. Também pode transferir um ficheiro que contenha o "tabelas de esquema".

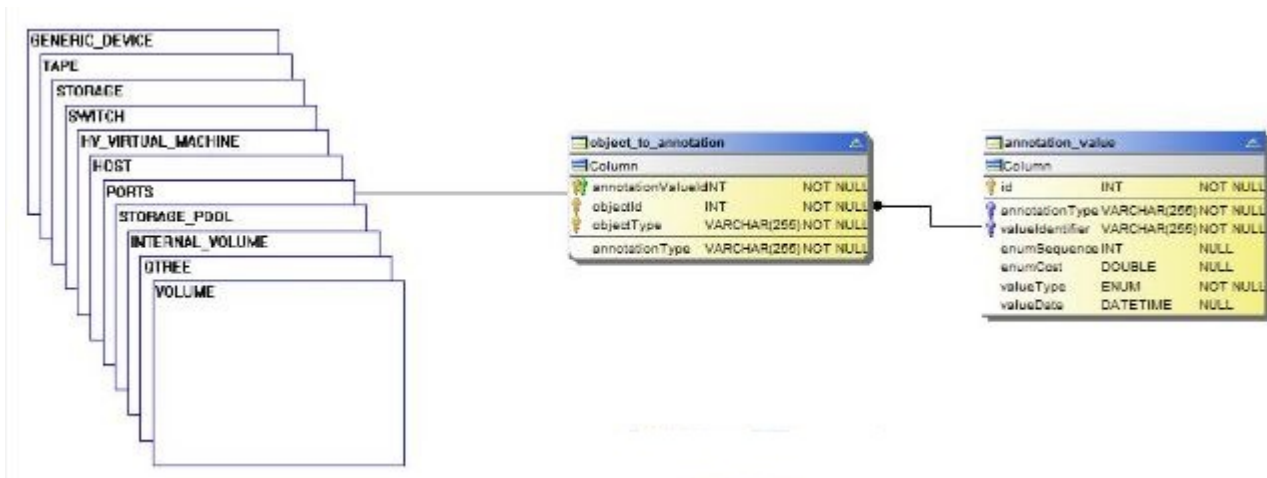


O recurso relatórios está disponível no Data Infrastructure Insights "Edição Premium".

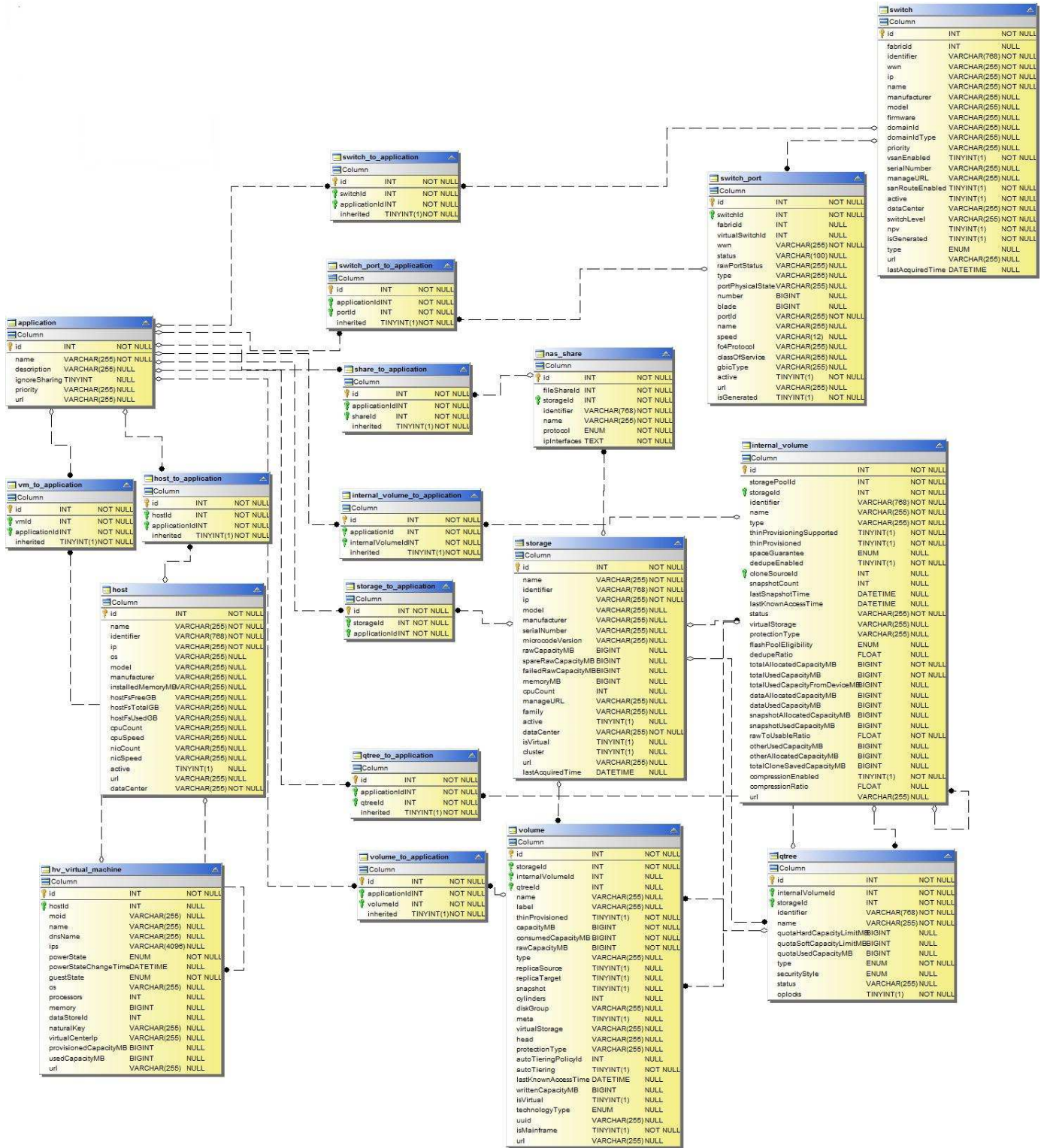
DataMart. Inventário

As imagens a seguir descrevem o datamart de inventário.

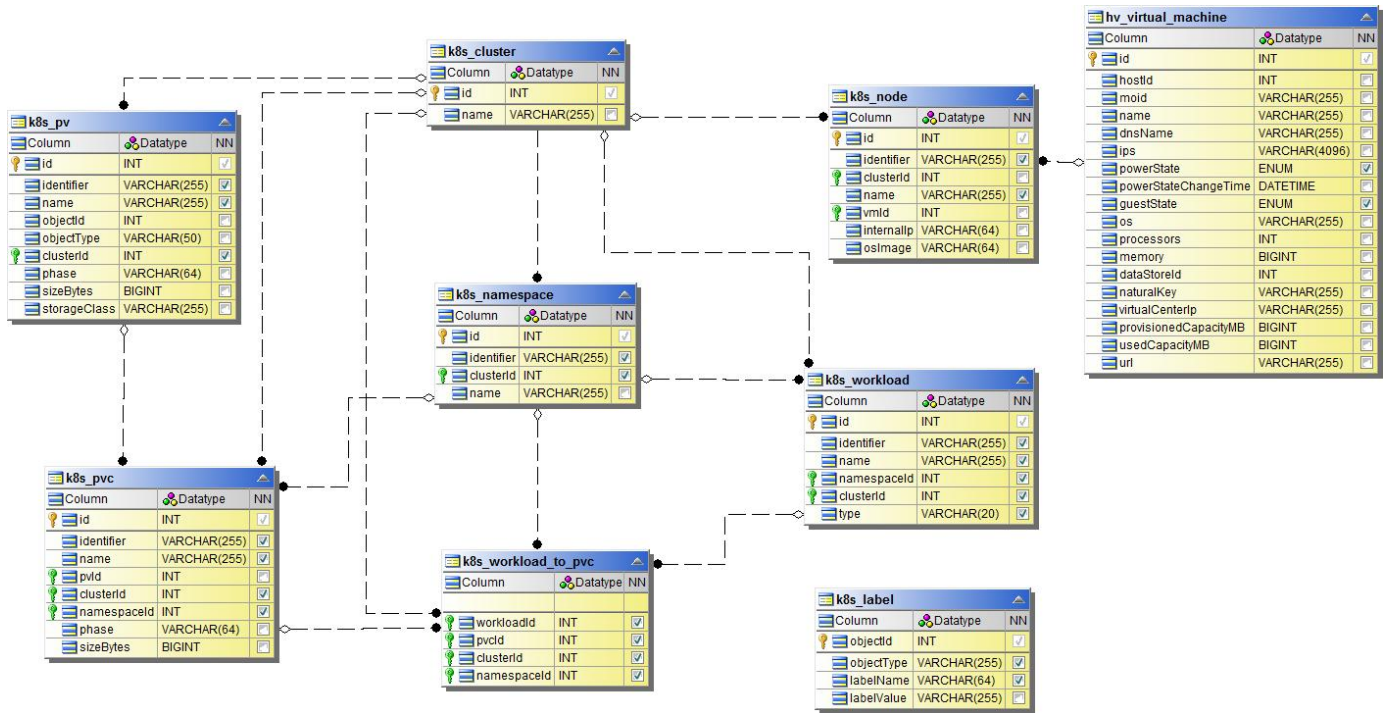
Anotações



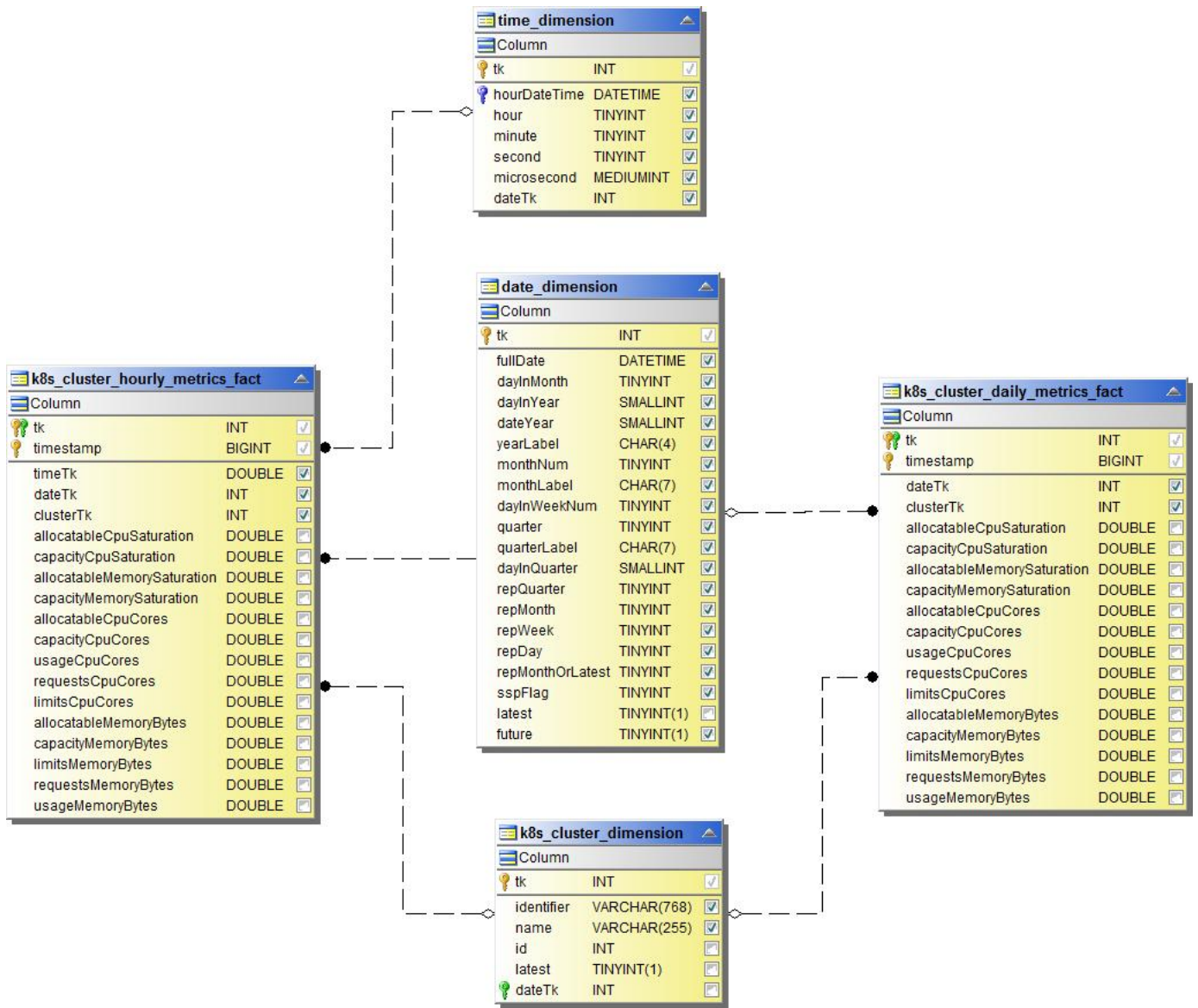
Aplicações



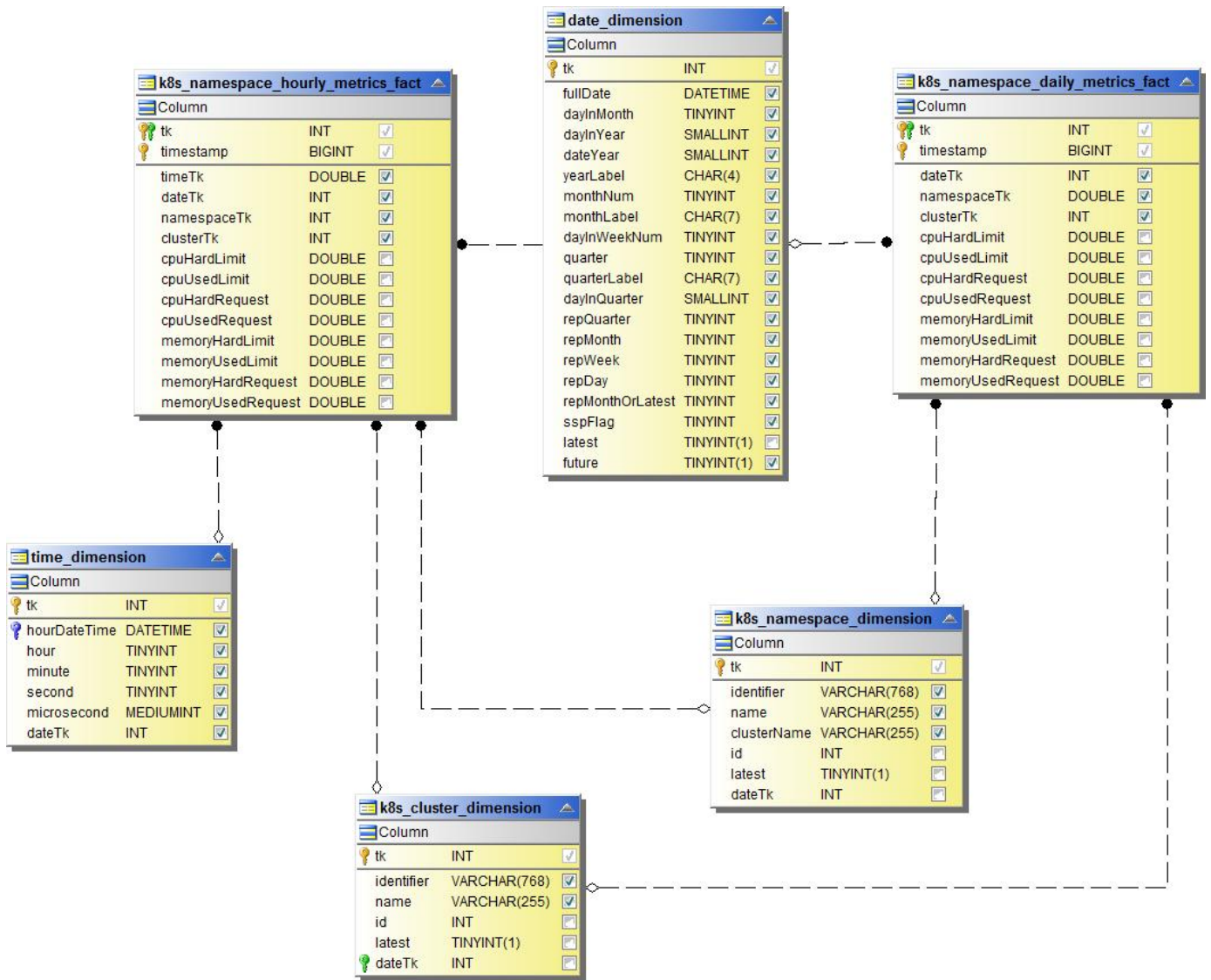
Métricas do Kubernetes



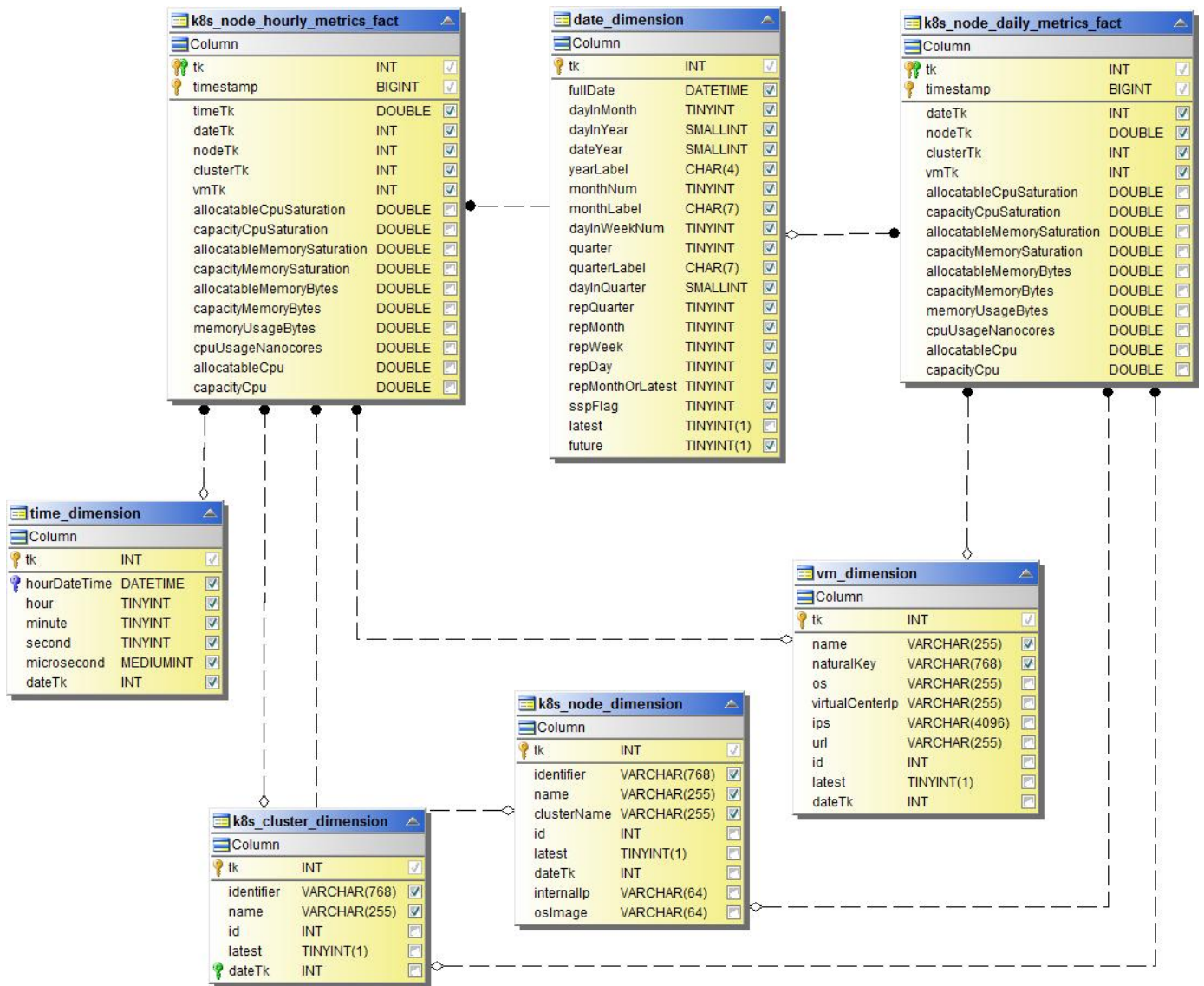
Fato das métricas de cluster do Kubernetes



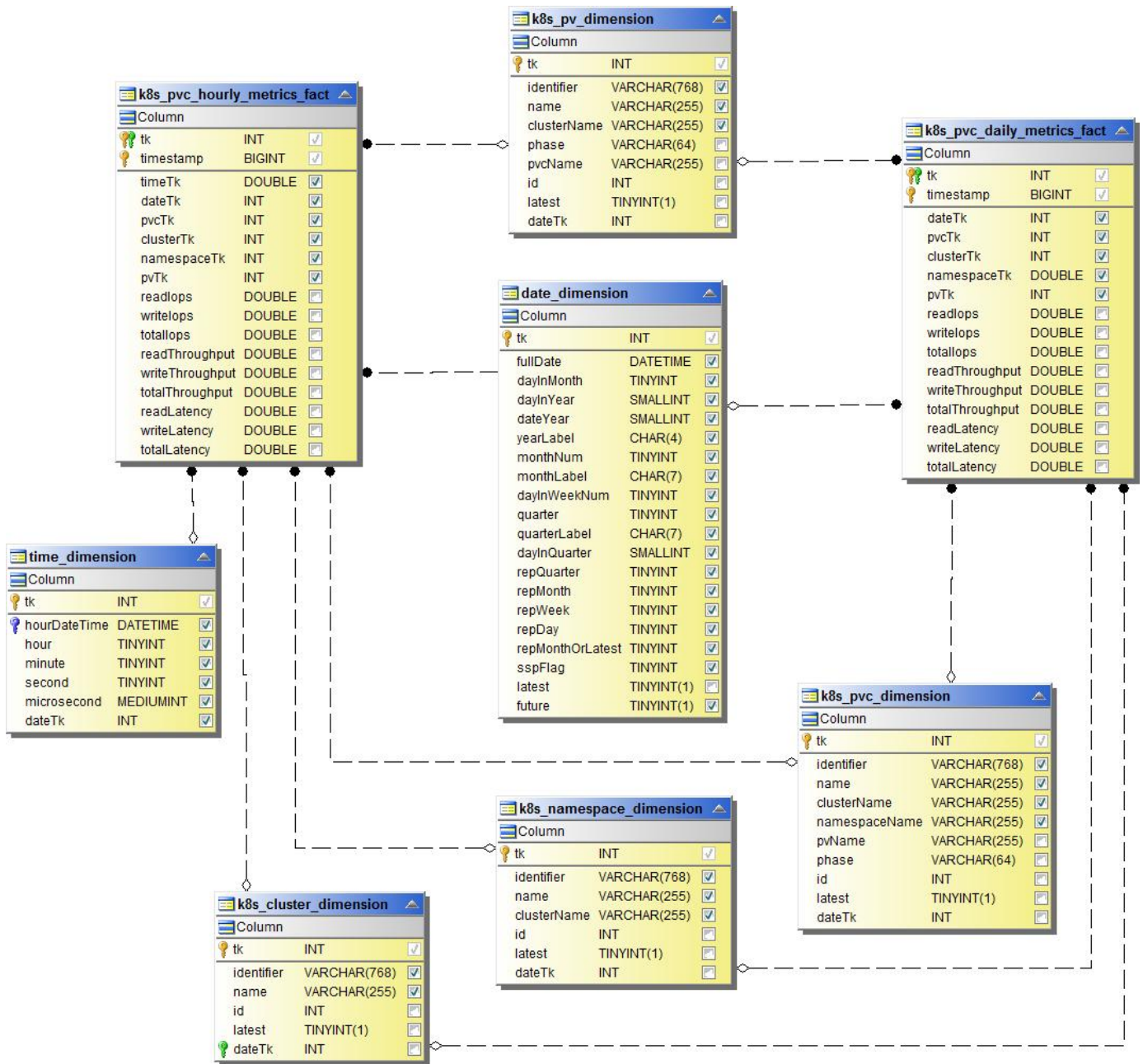
Fato da métrica do namespace do Kubernetes



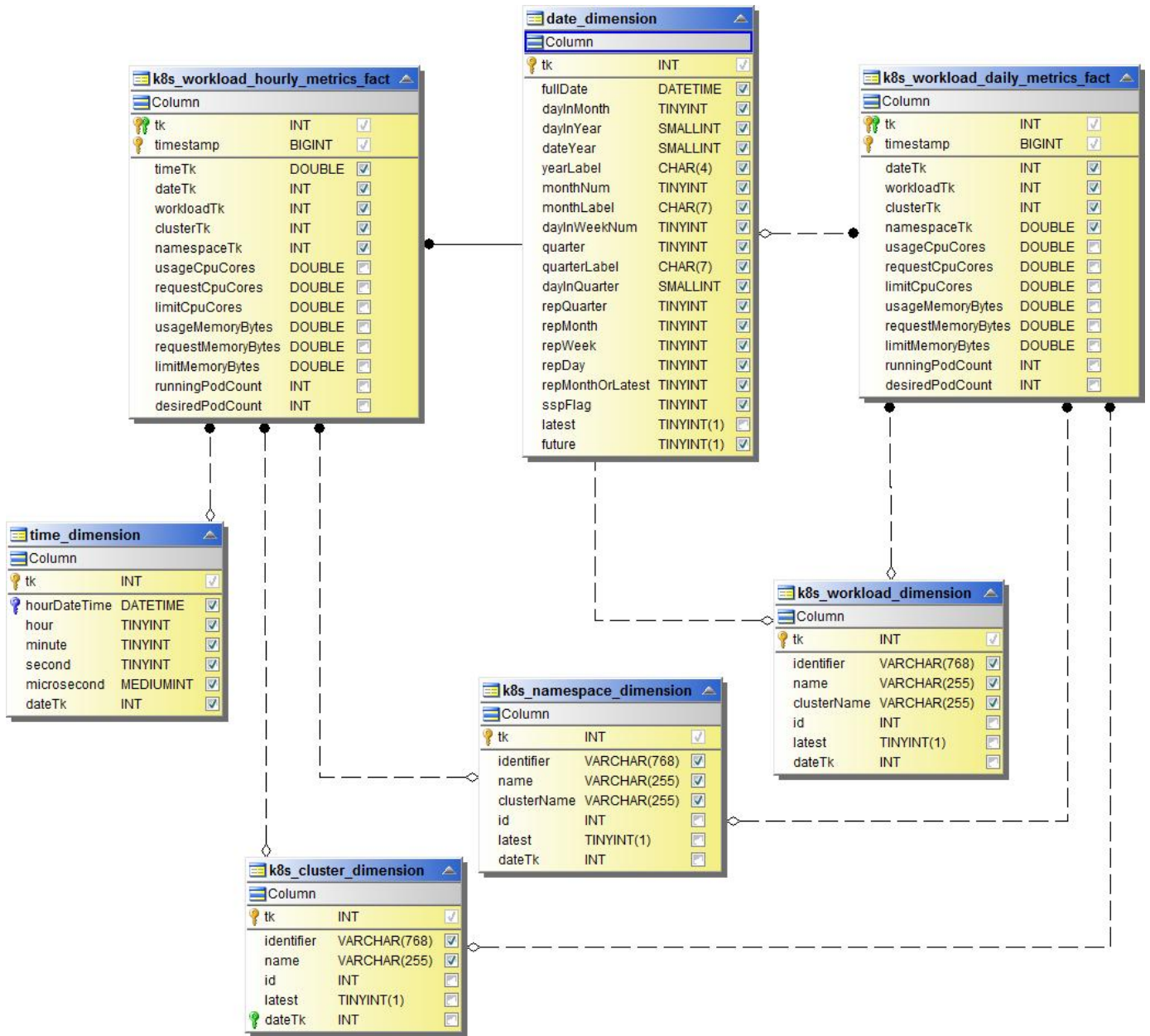
Fato das métricas do nó do Kubernetes



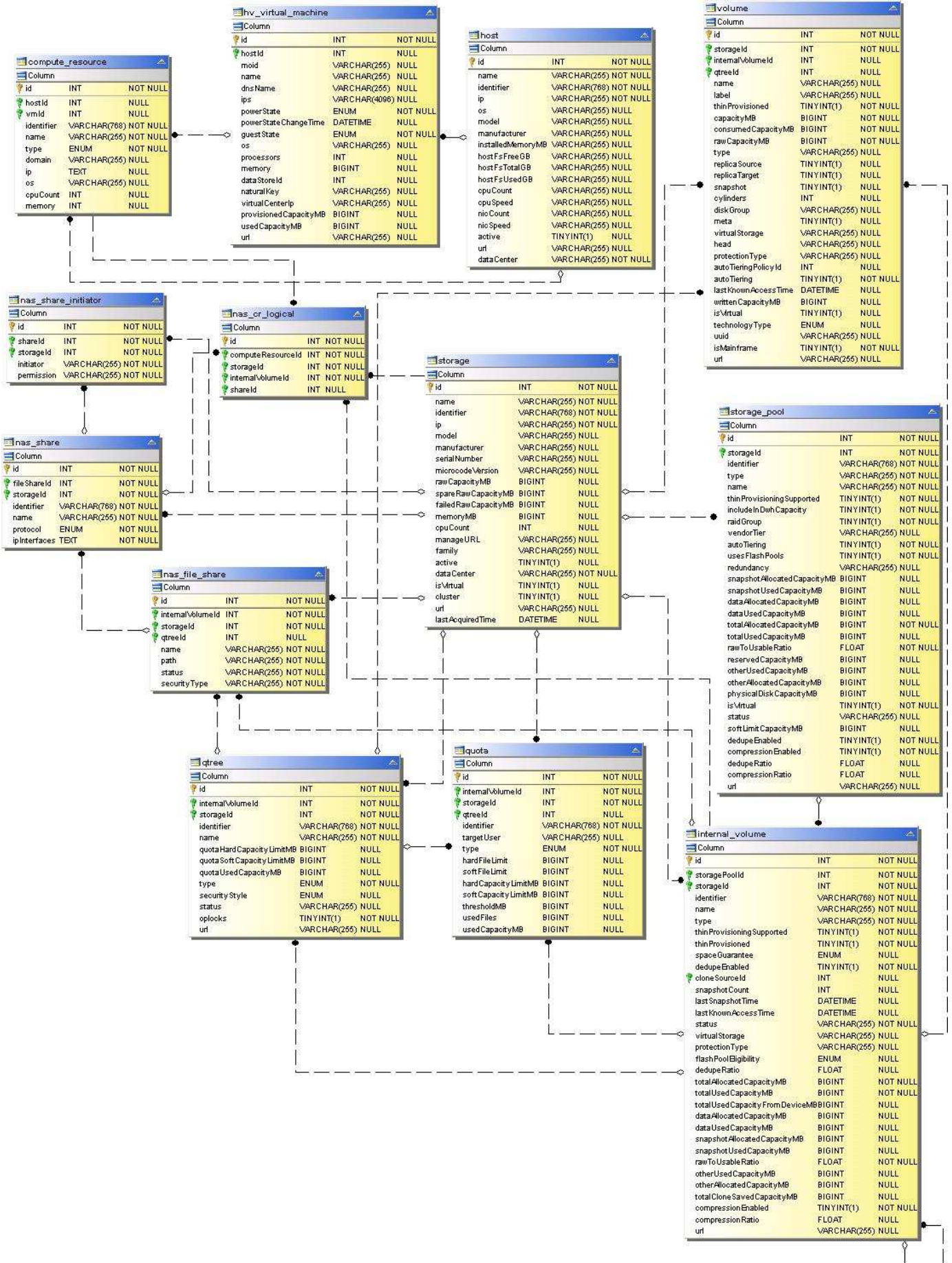
Fato das métricas de PVC do Kubernetes



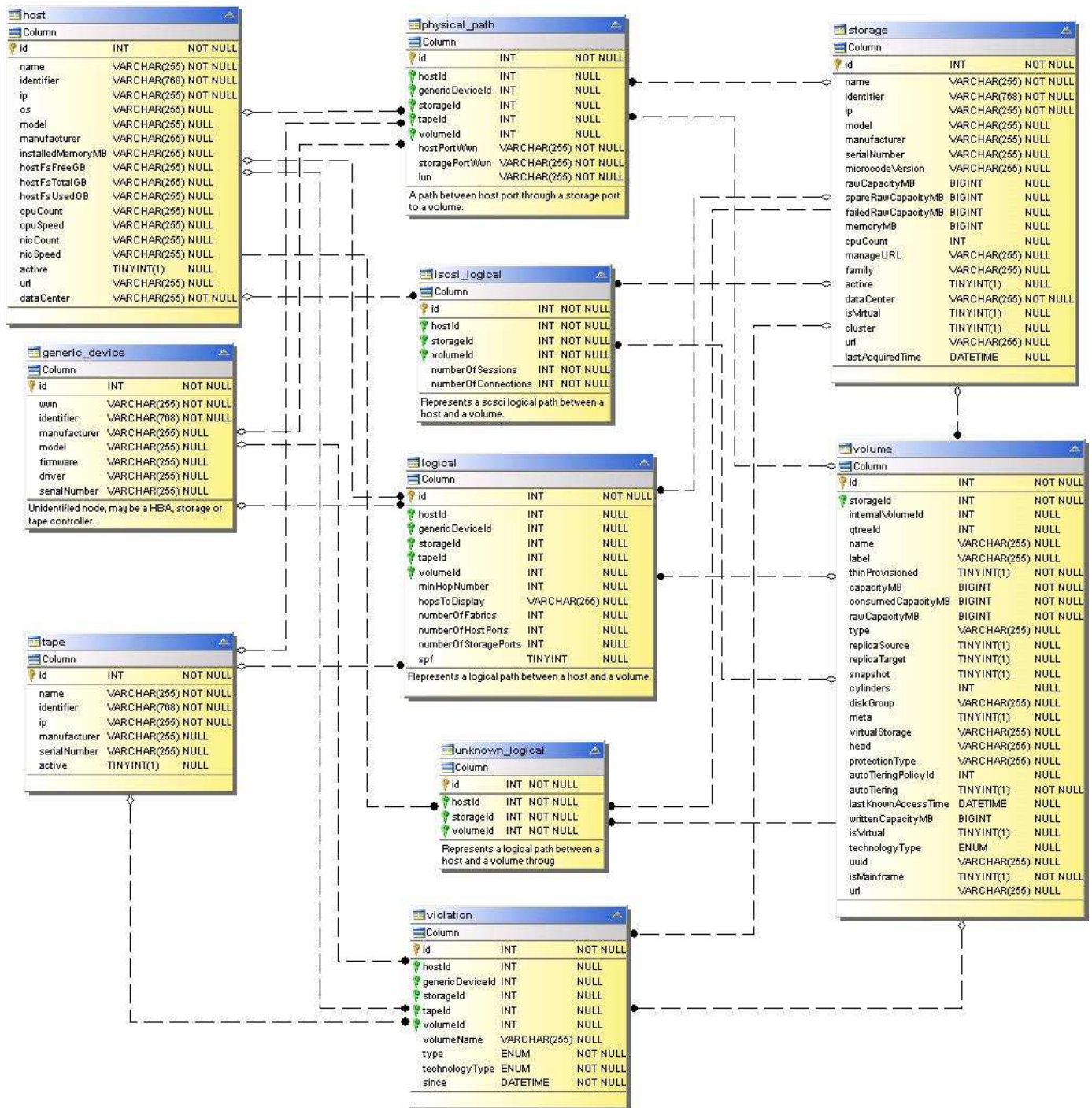
Fato das métricas de workload do Kubernetes



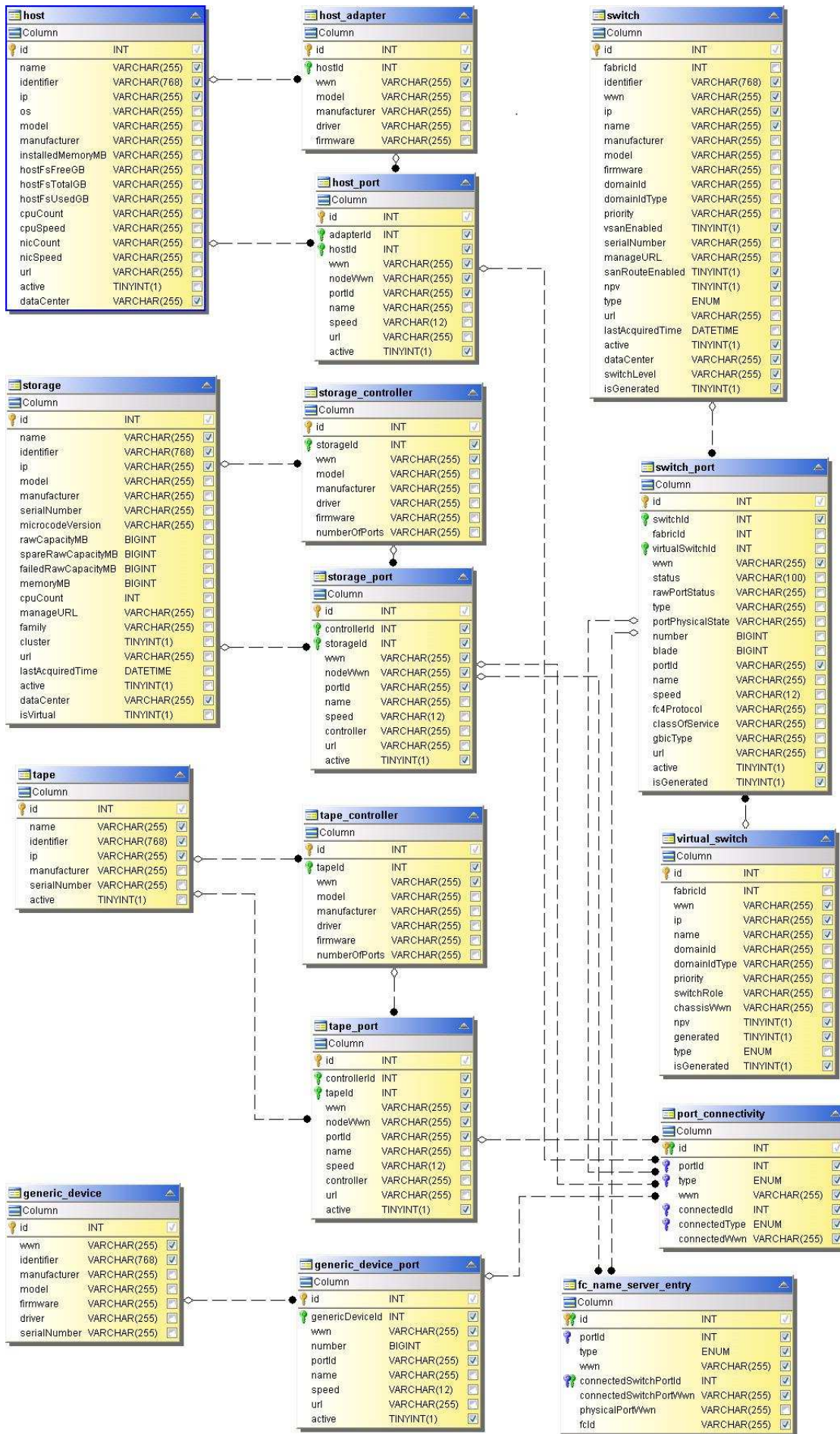
NAS



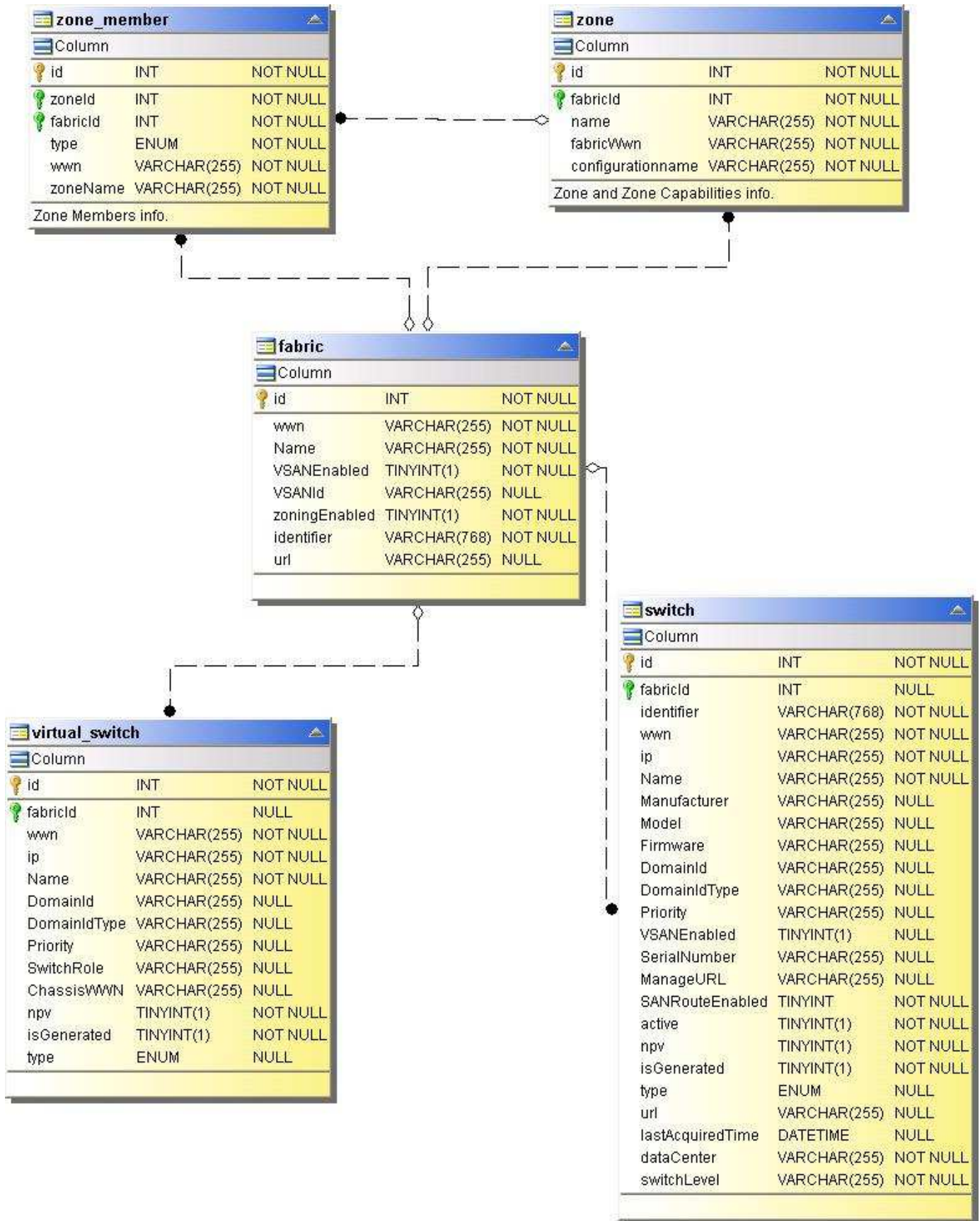
Caminhos e violações



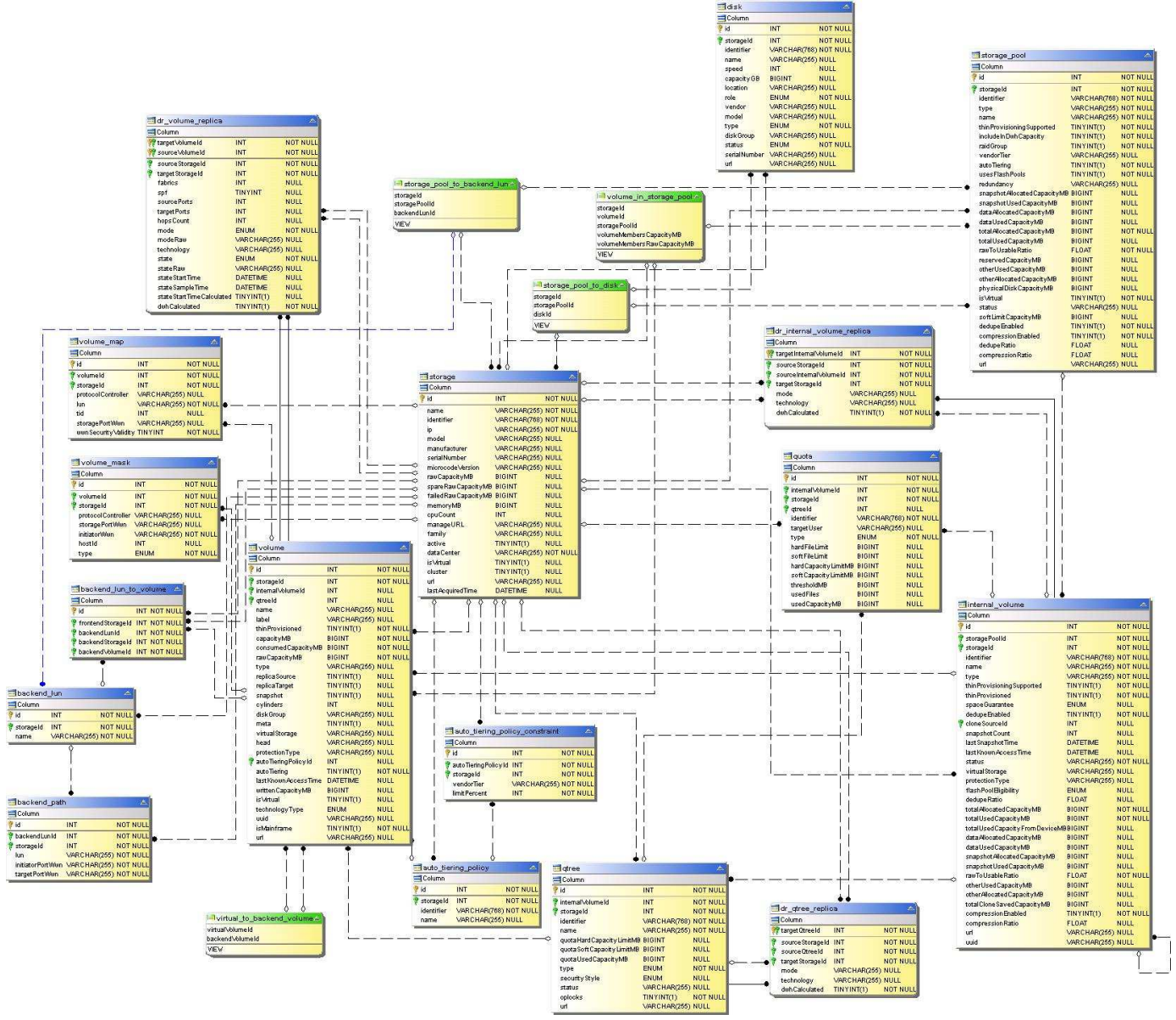
Conetividade da porta



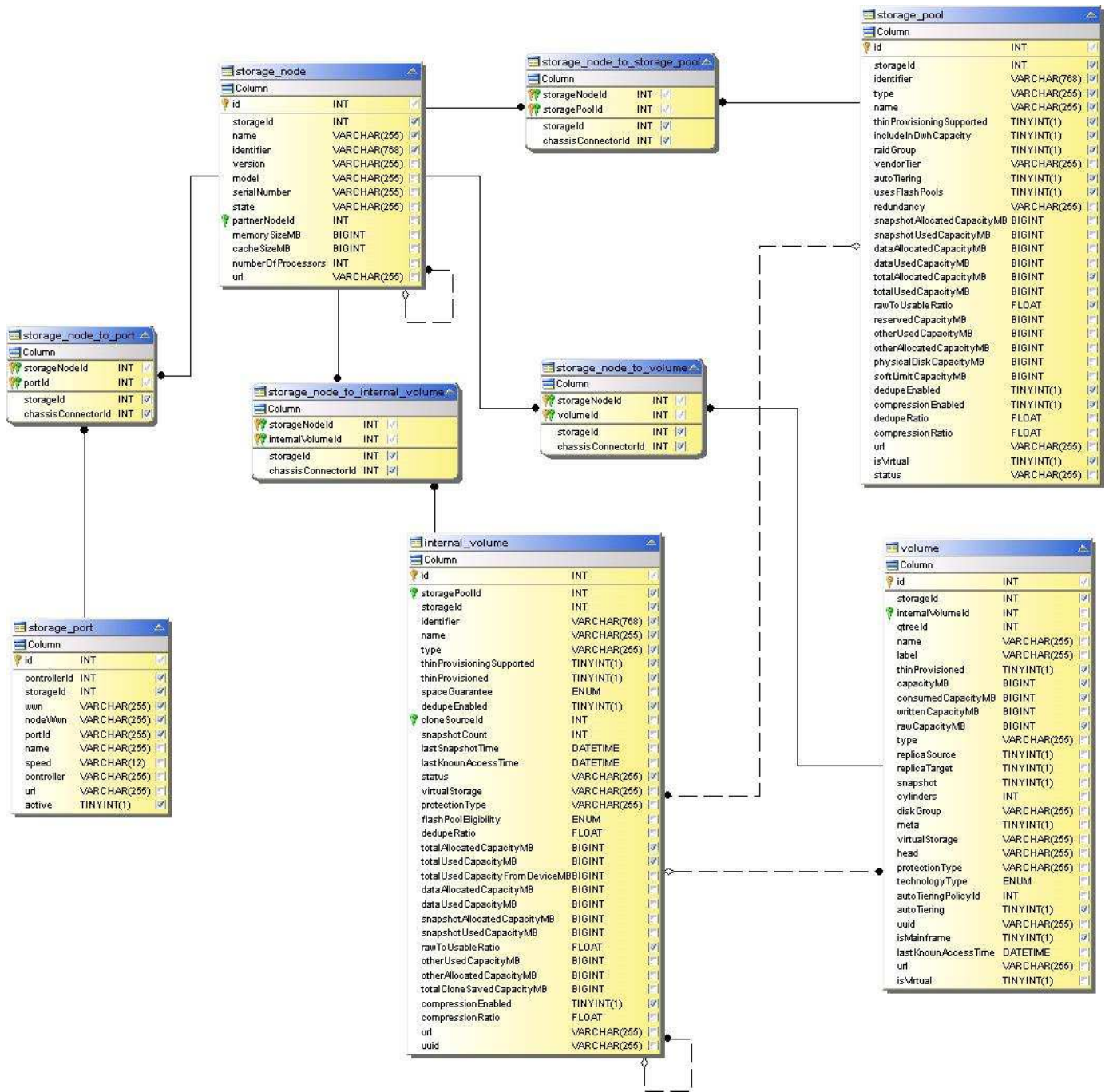
Tecido SAN



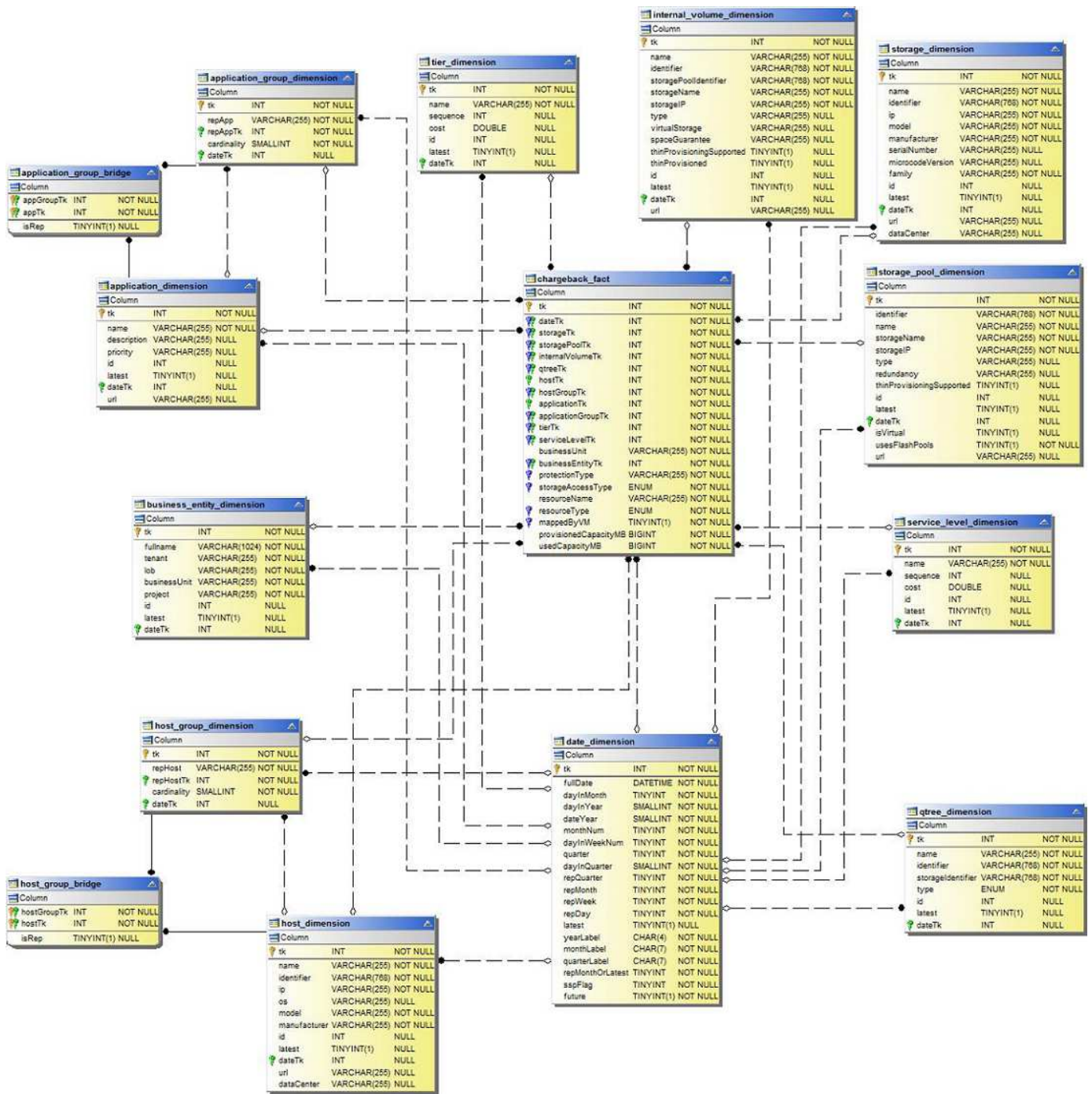
Armazenamento



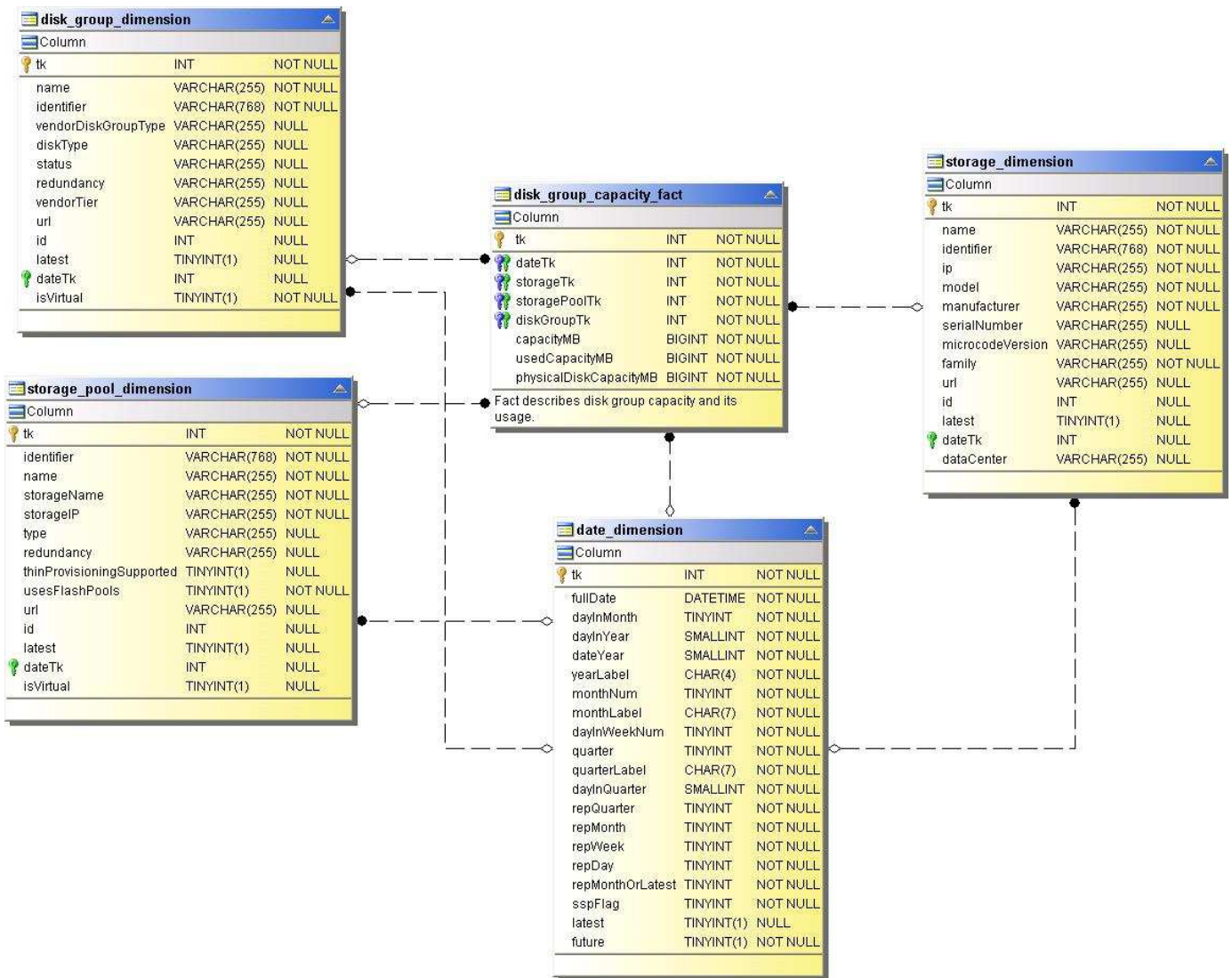
Nó de storage



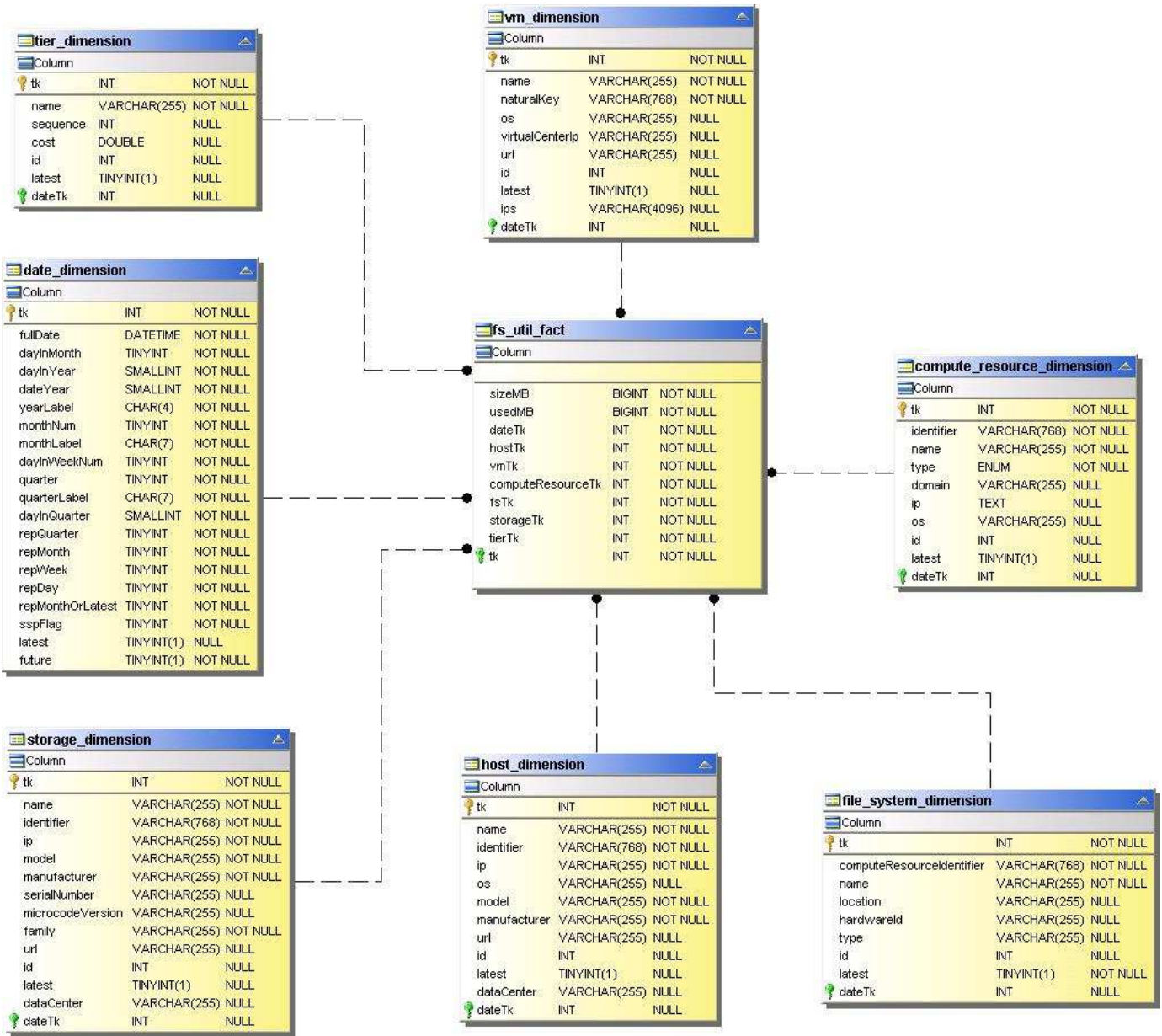
VM



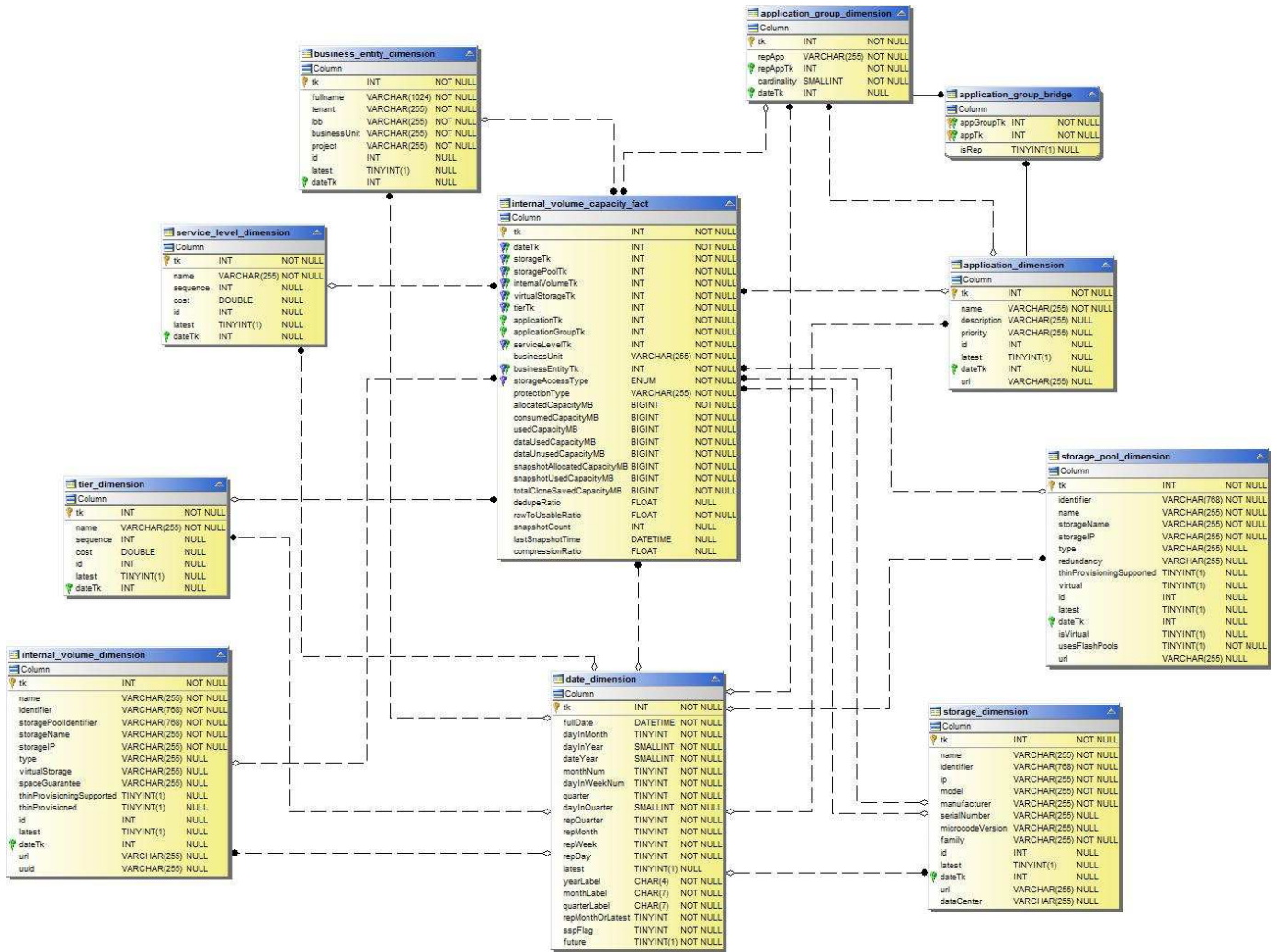
Capacidade do Grupo de discos



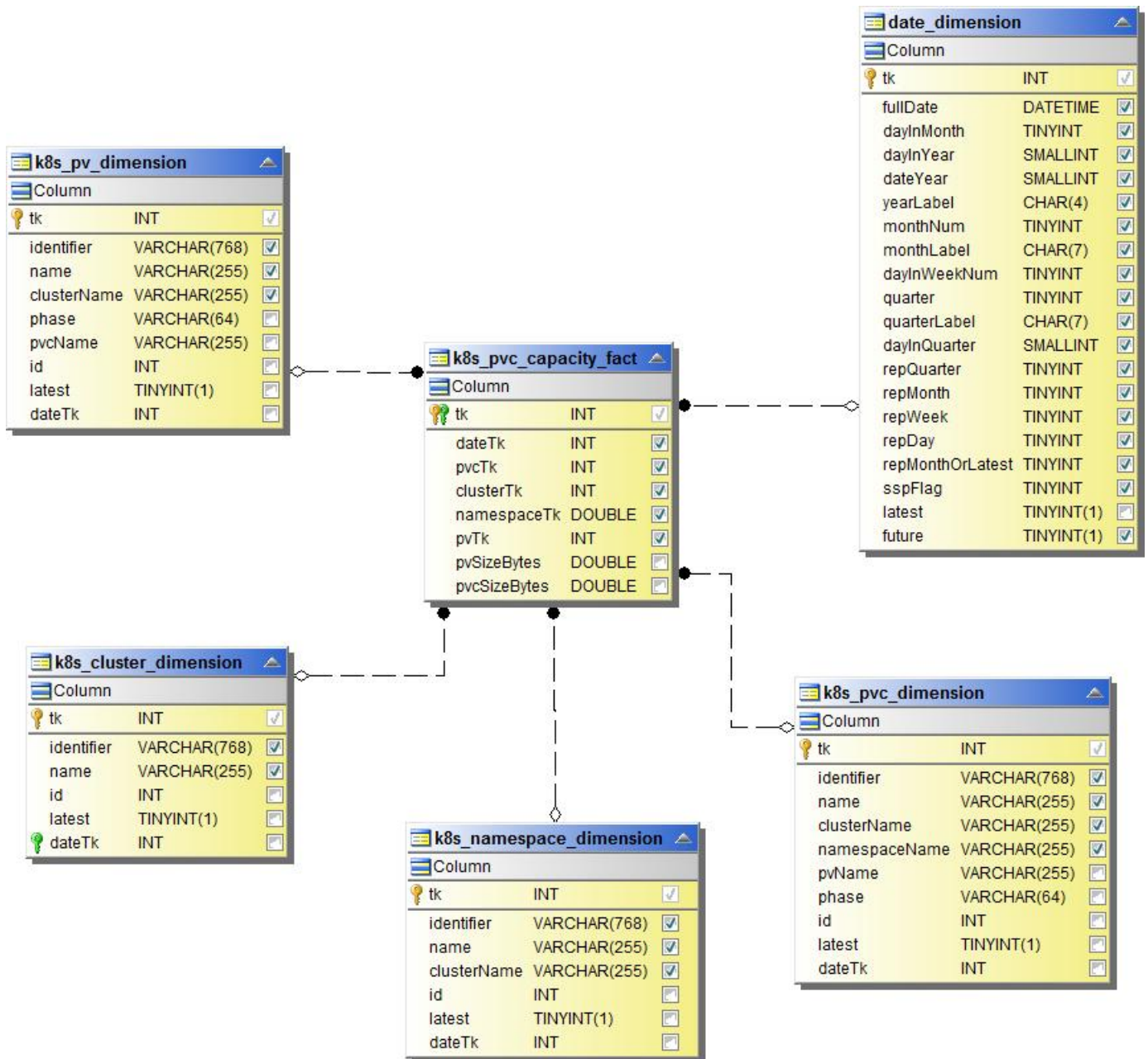
Utilização do sistema de arquivos



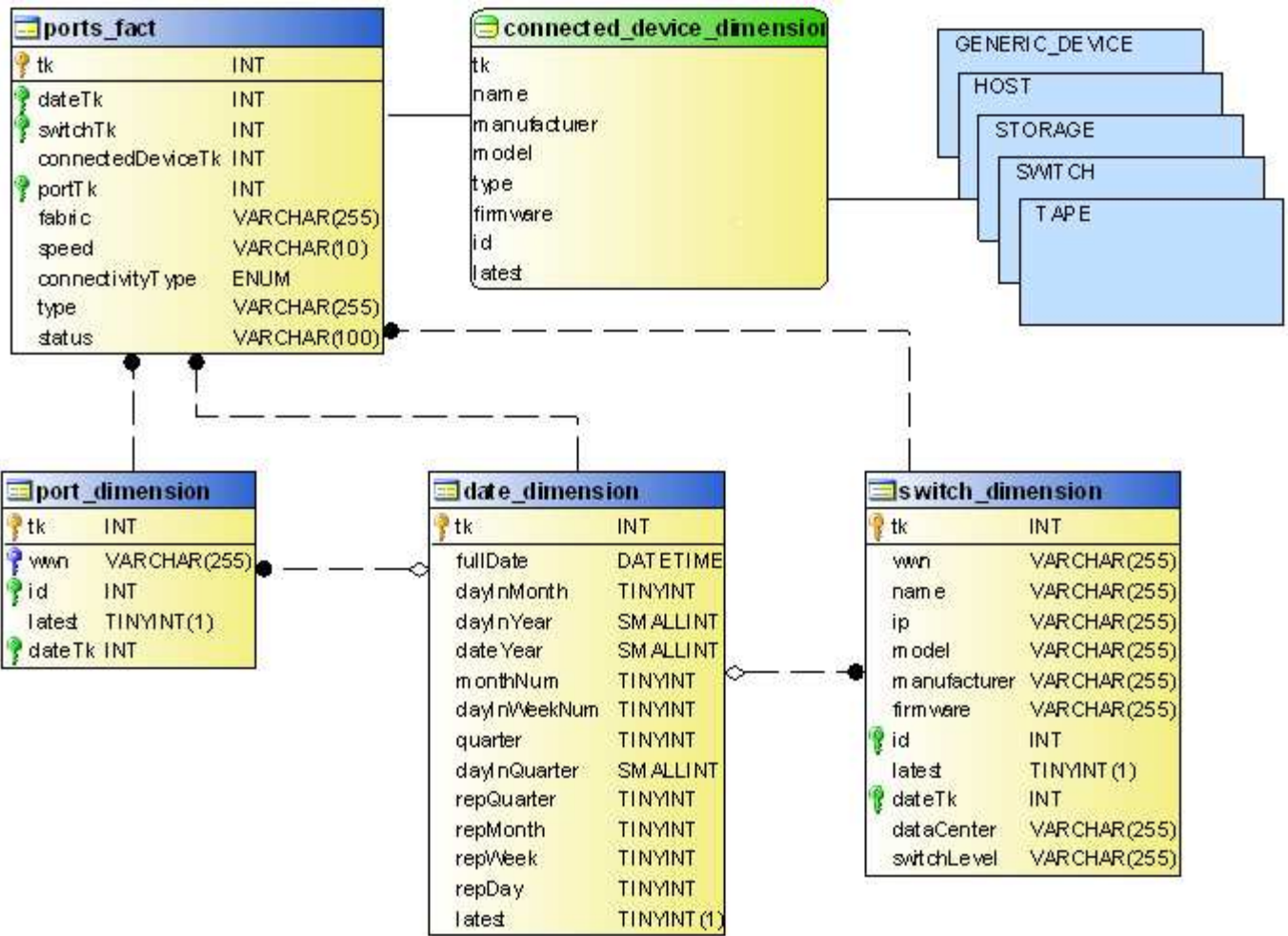
Capacidade de volume interno



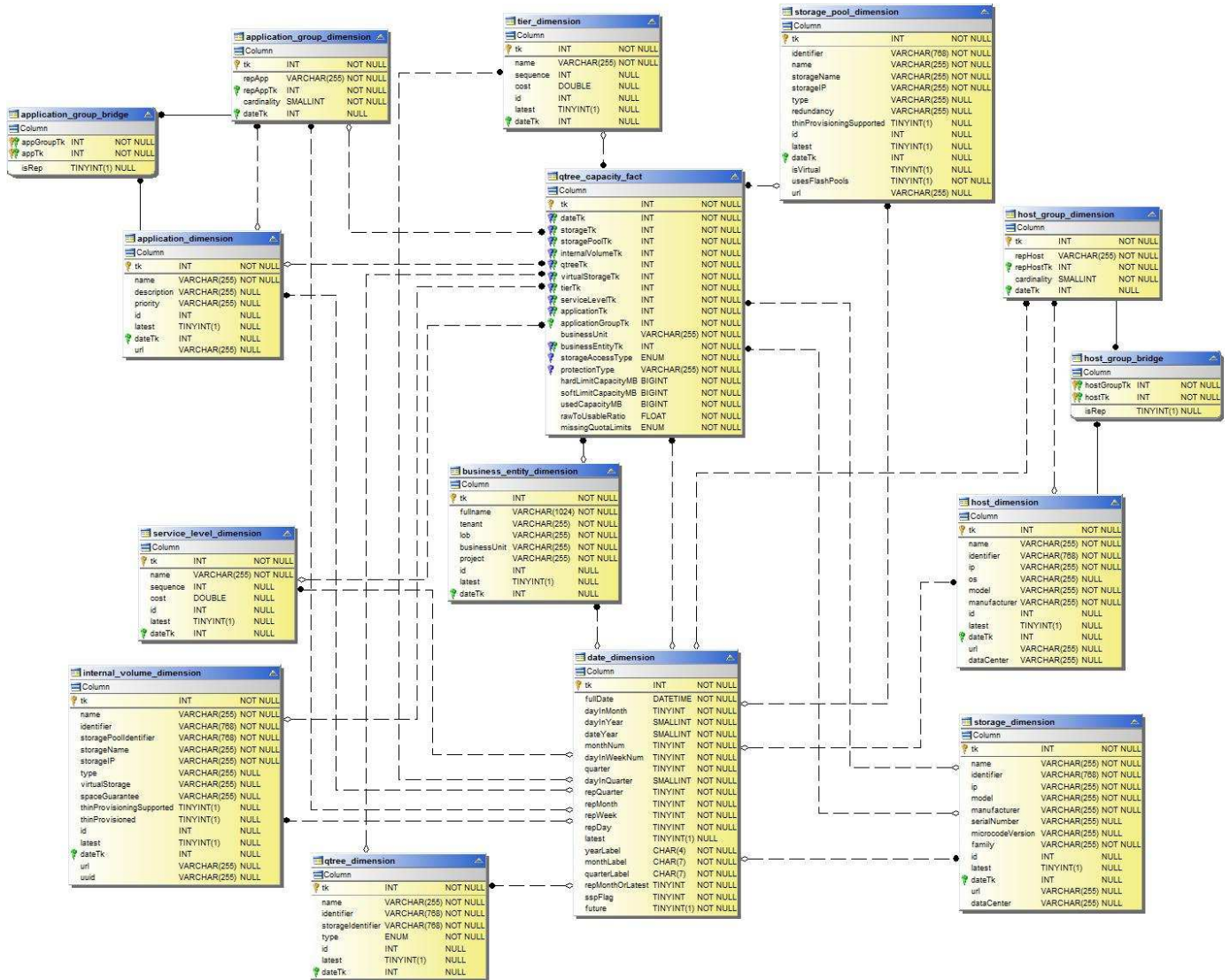
Capacidade fotovoltaica do Kubernetes



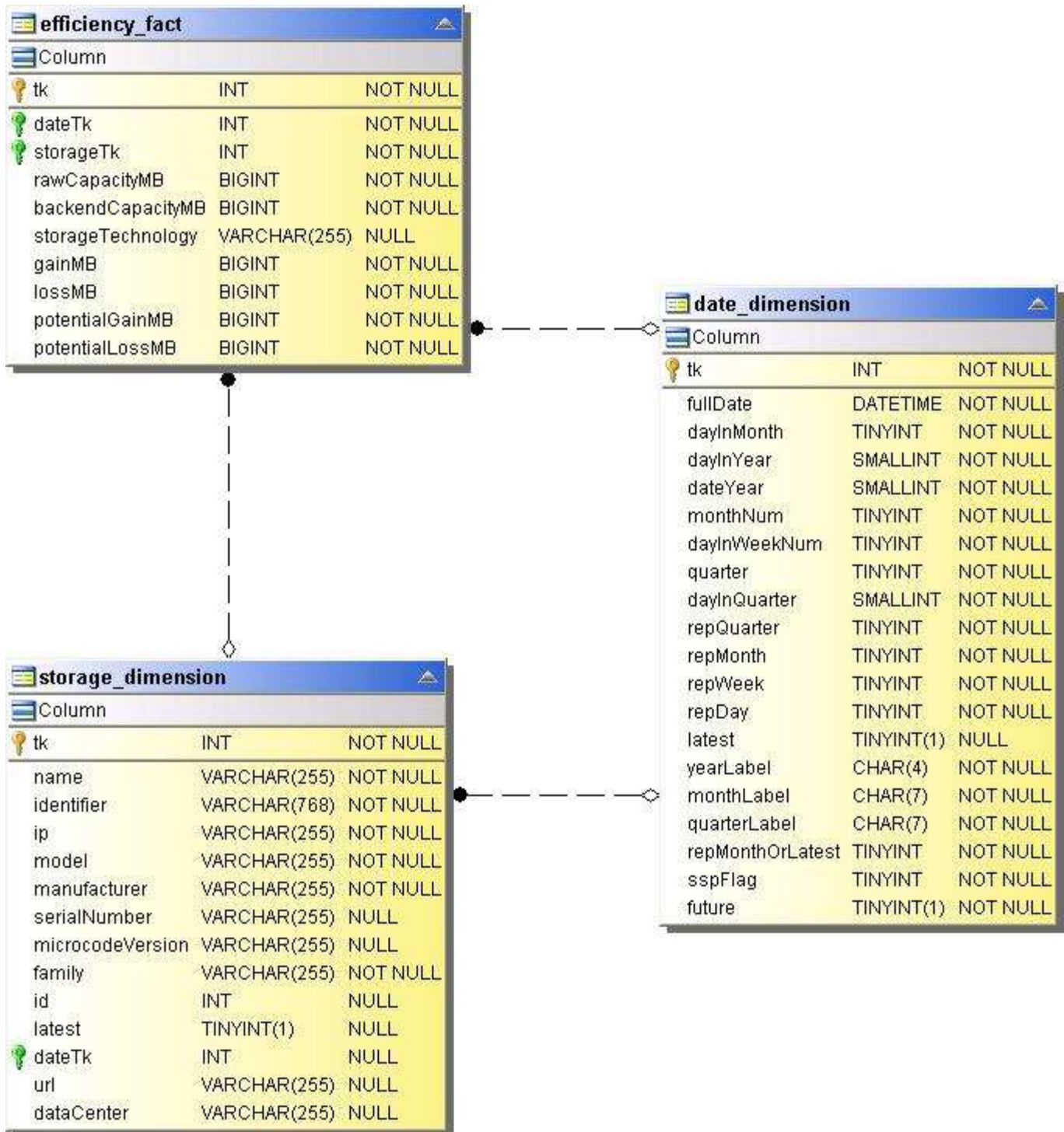
Capacidade da porta



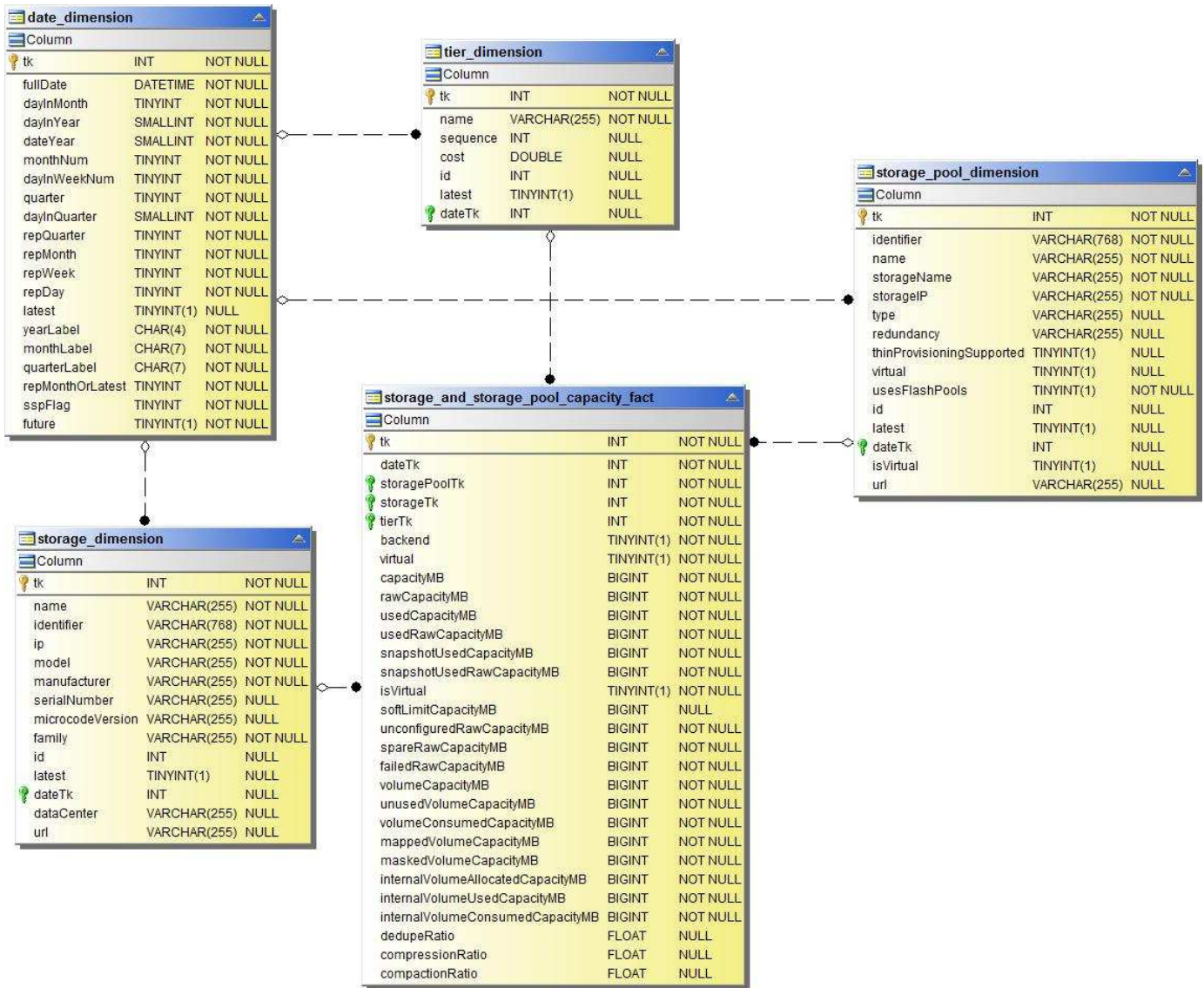
Qtree capacidade



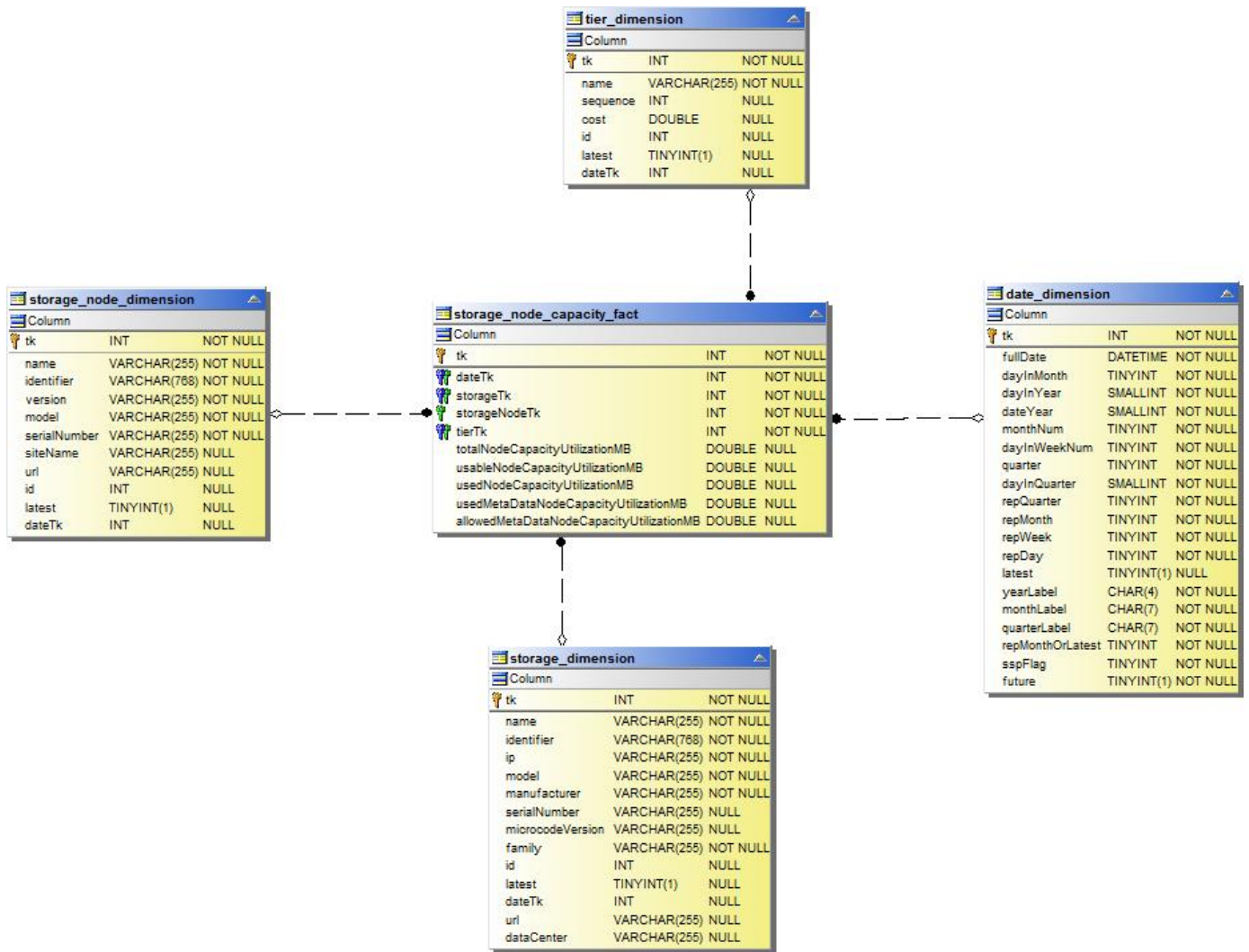
Eficiência de capacidade de storage



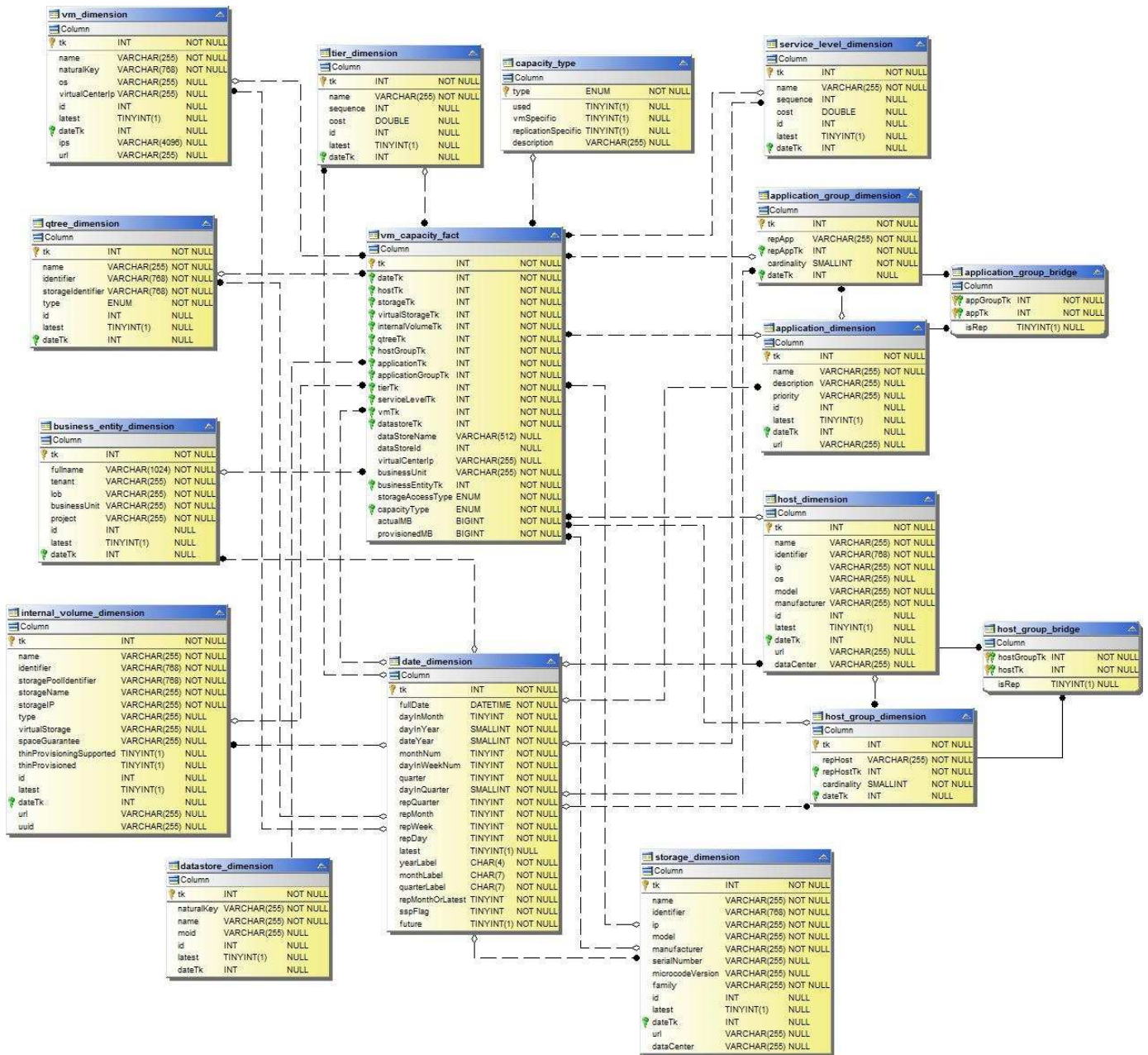
Capacidade do pool de armazenamento e armazenamento



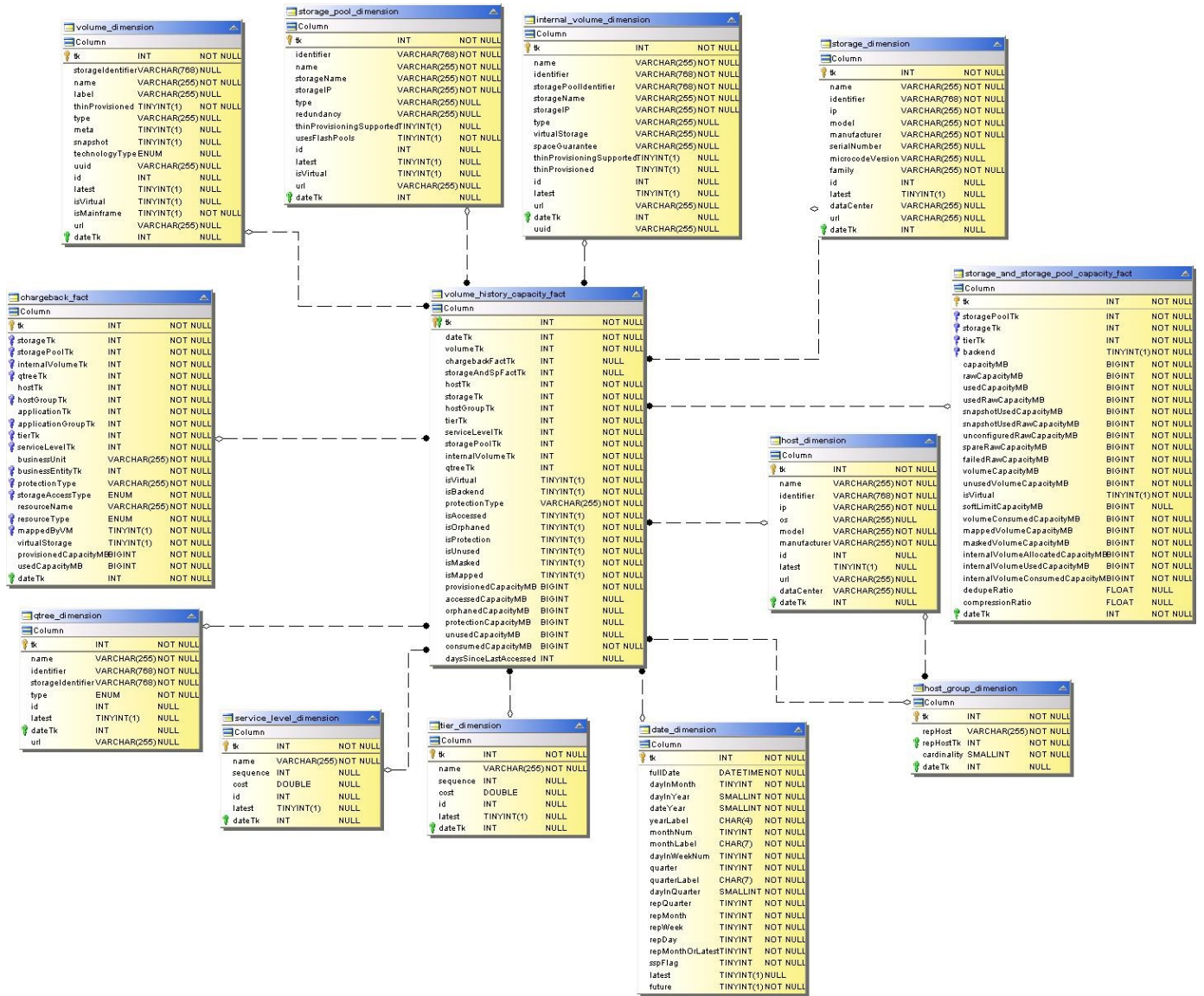
Capacidade do nó de storage



Capacidade da VM



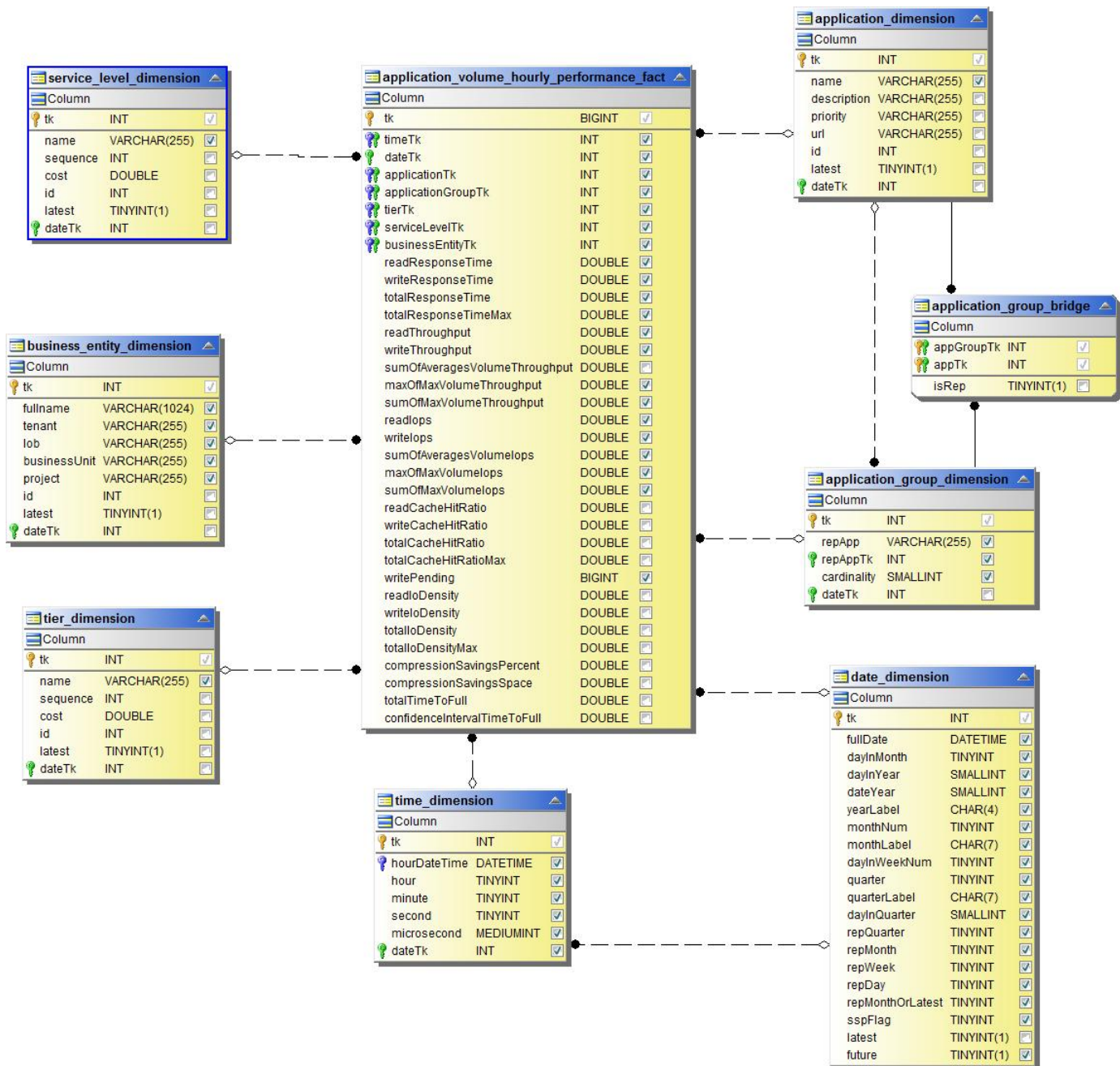
Capacidade de volume



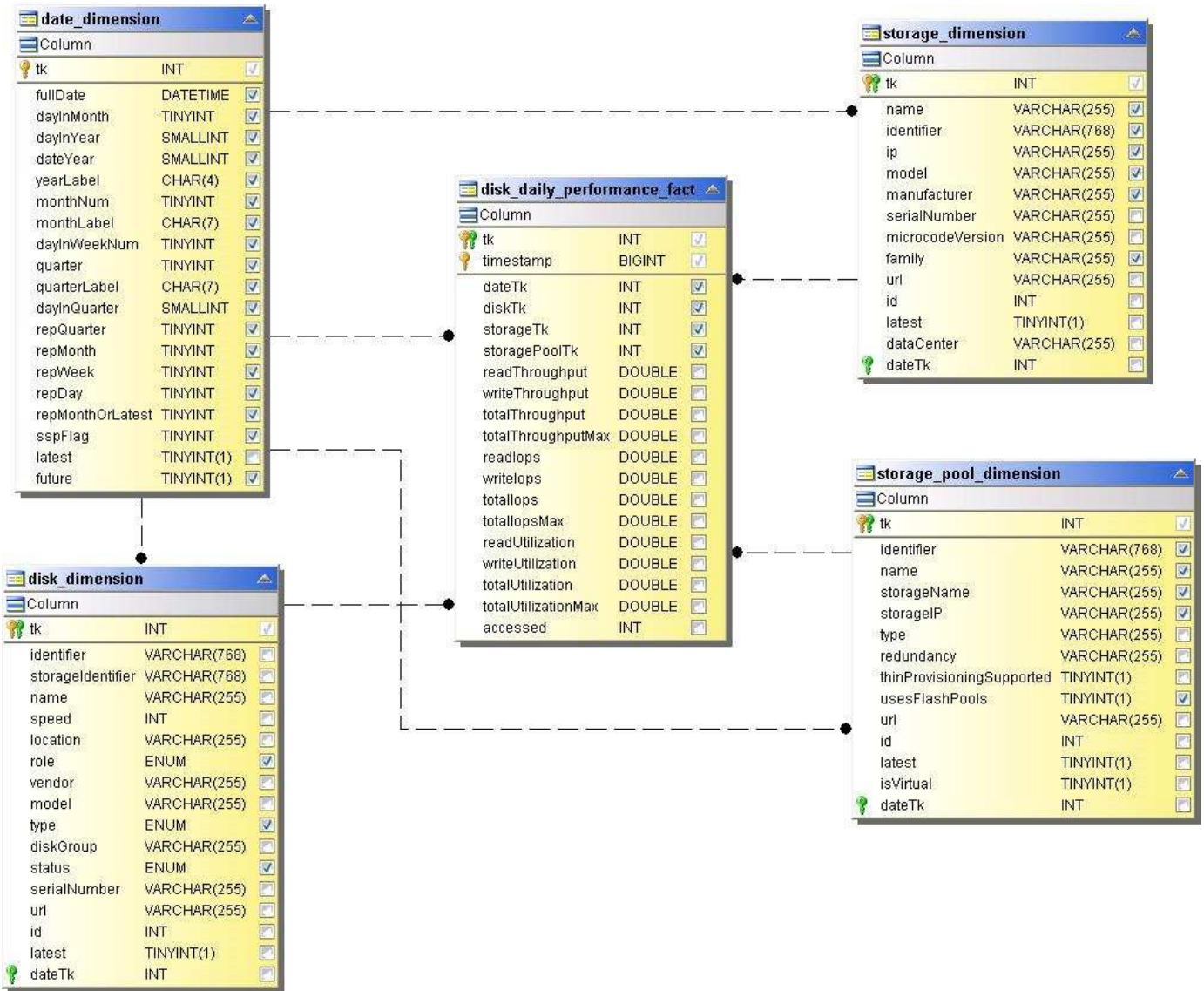
DataMart de desempenho

As imagens a seguir descrevem o datamart de desempenho.

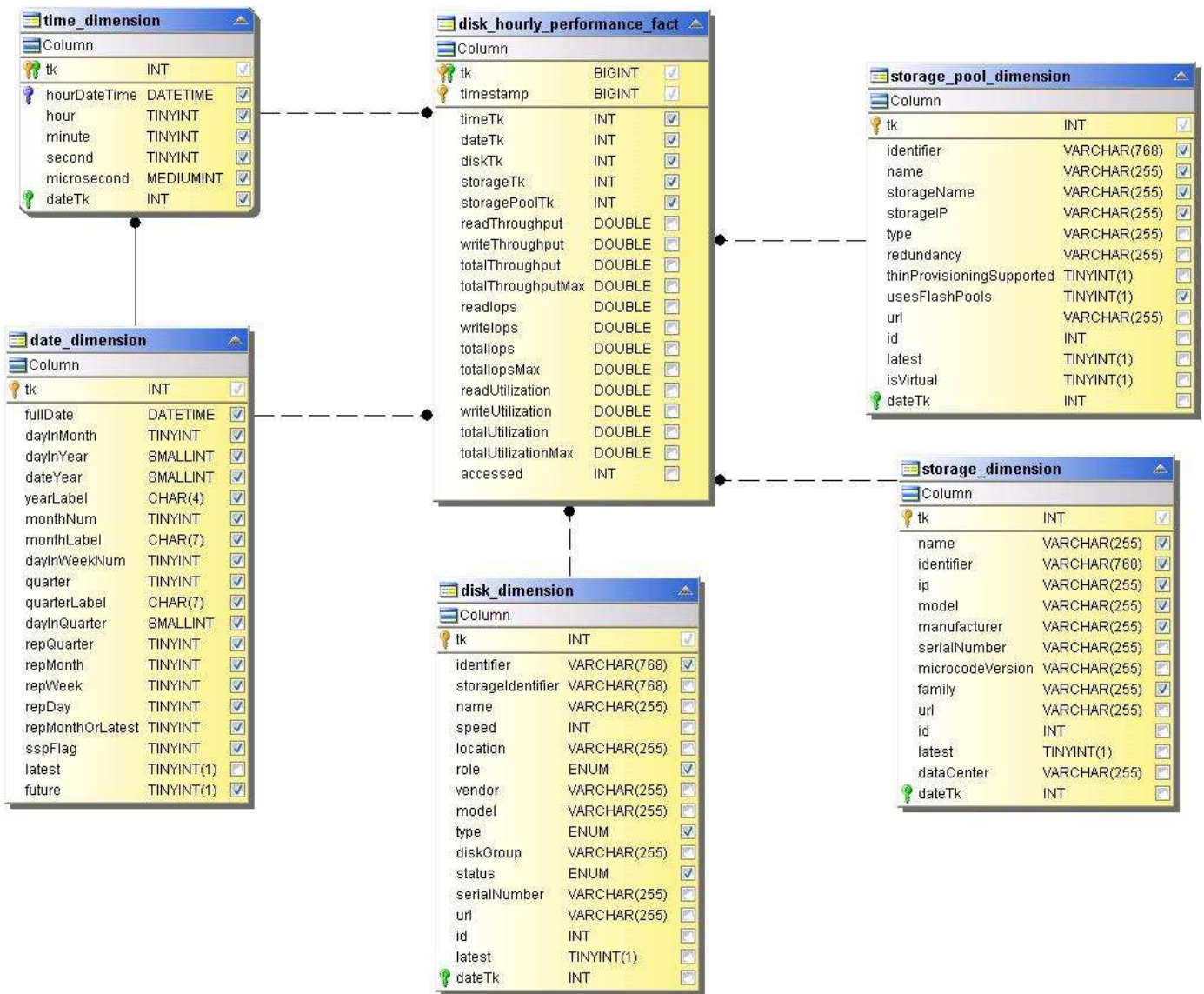
Volume de aplicação desempenho por hora



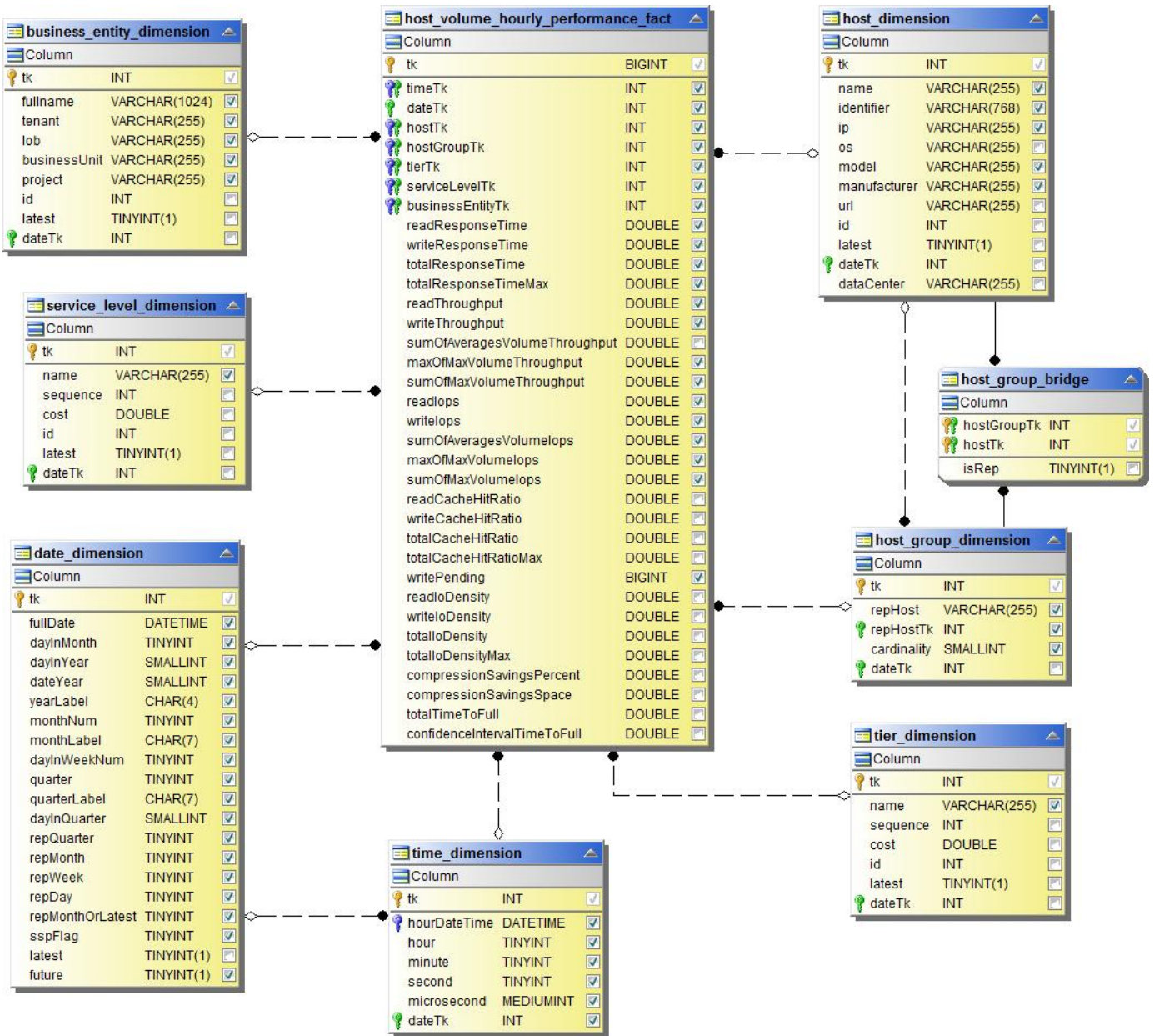
Desempenho diário do disco



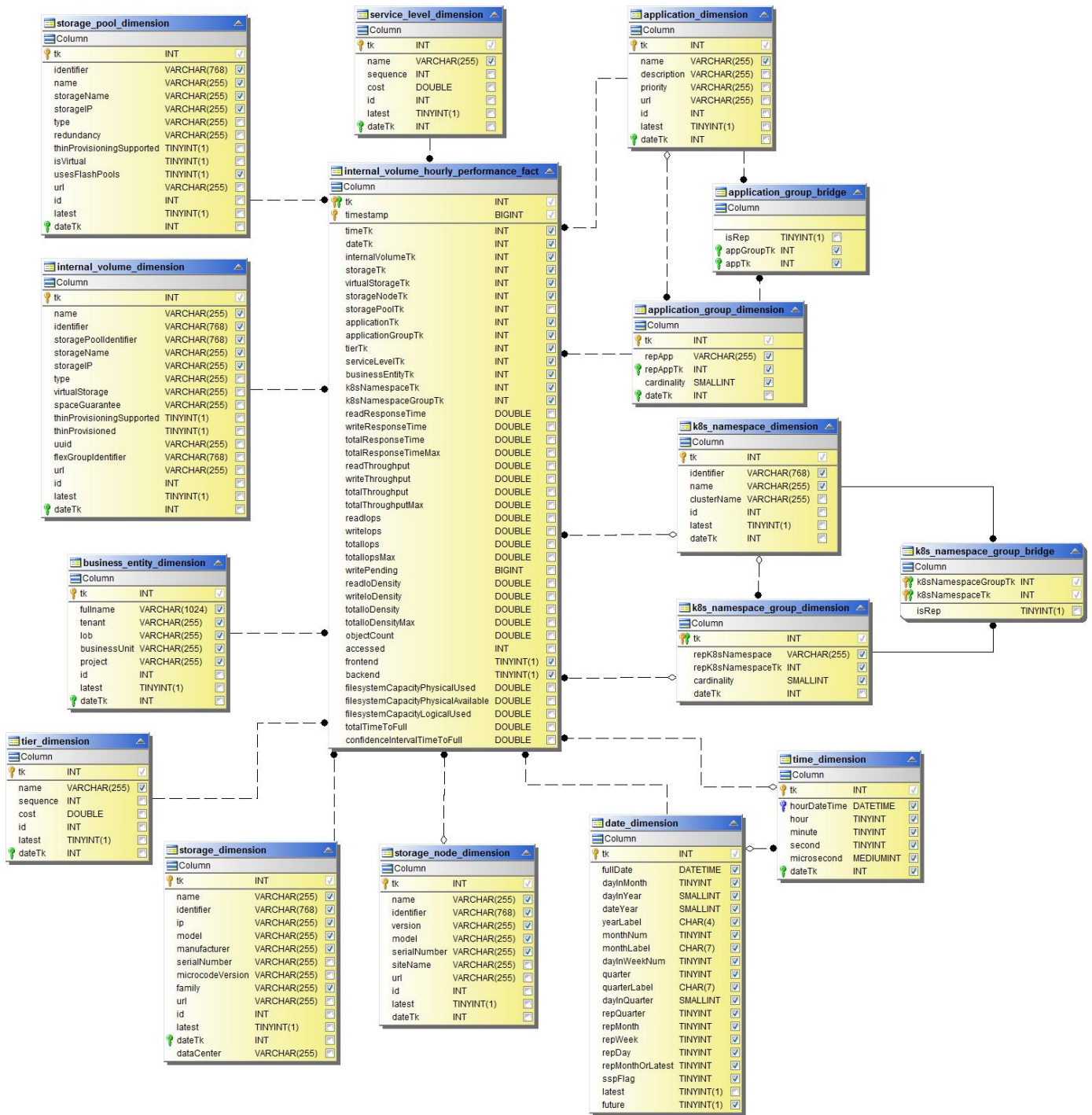
Desempenho de disco por hora



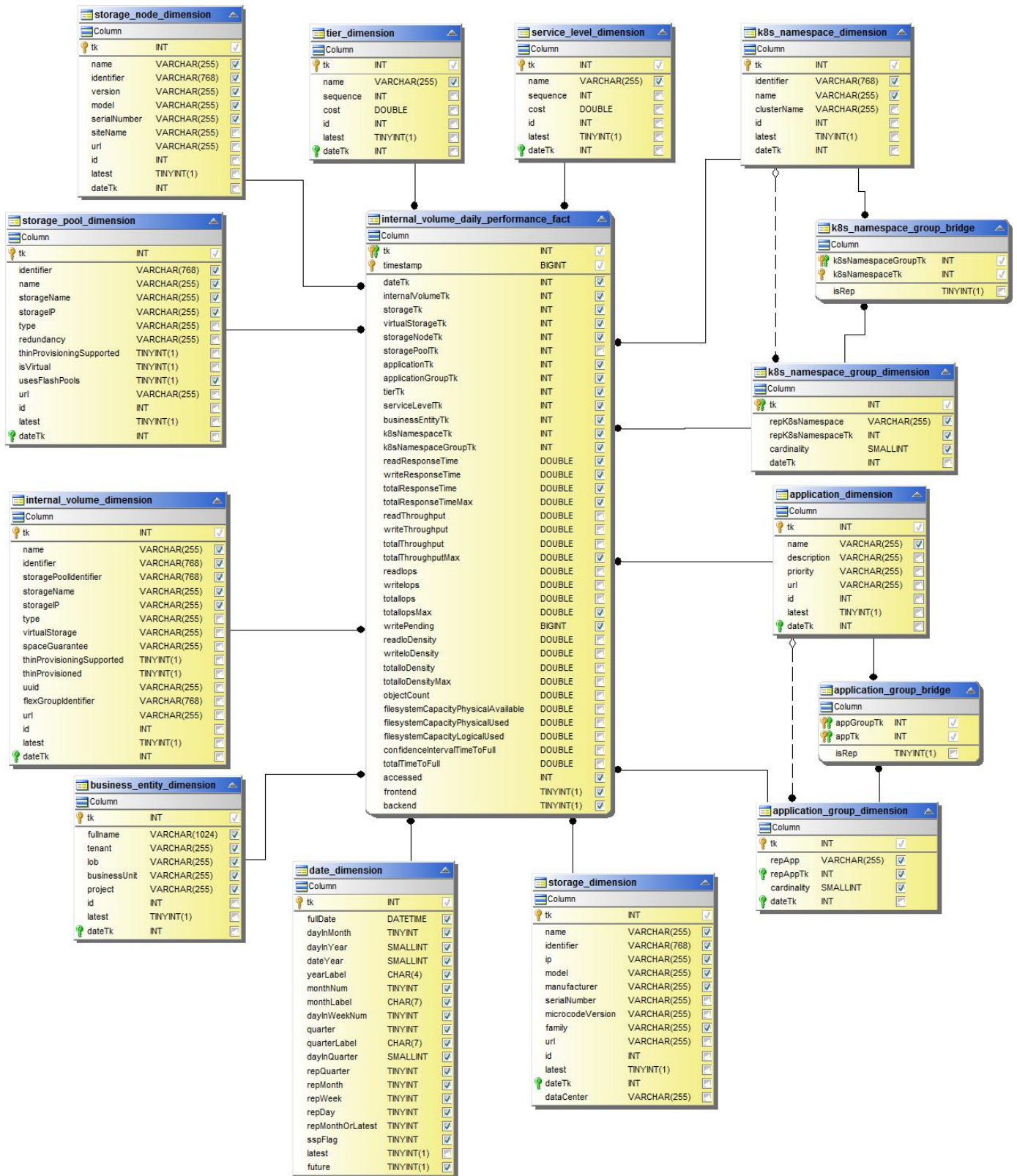
Hospede desempenho por hora



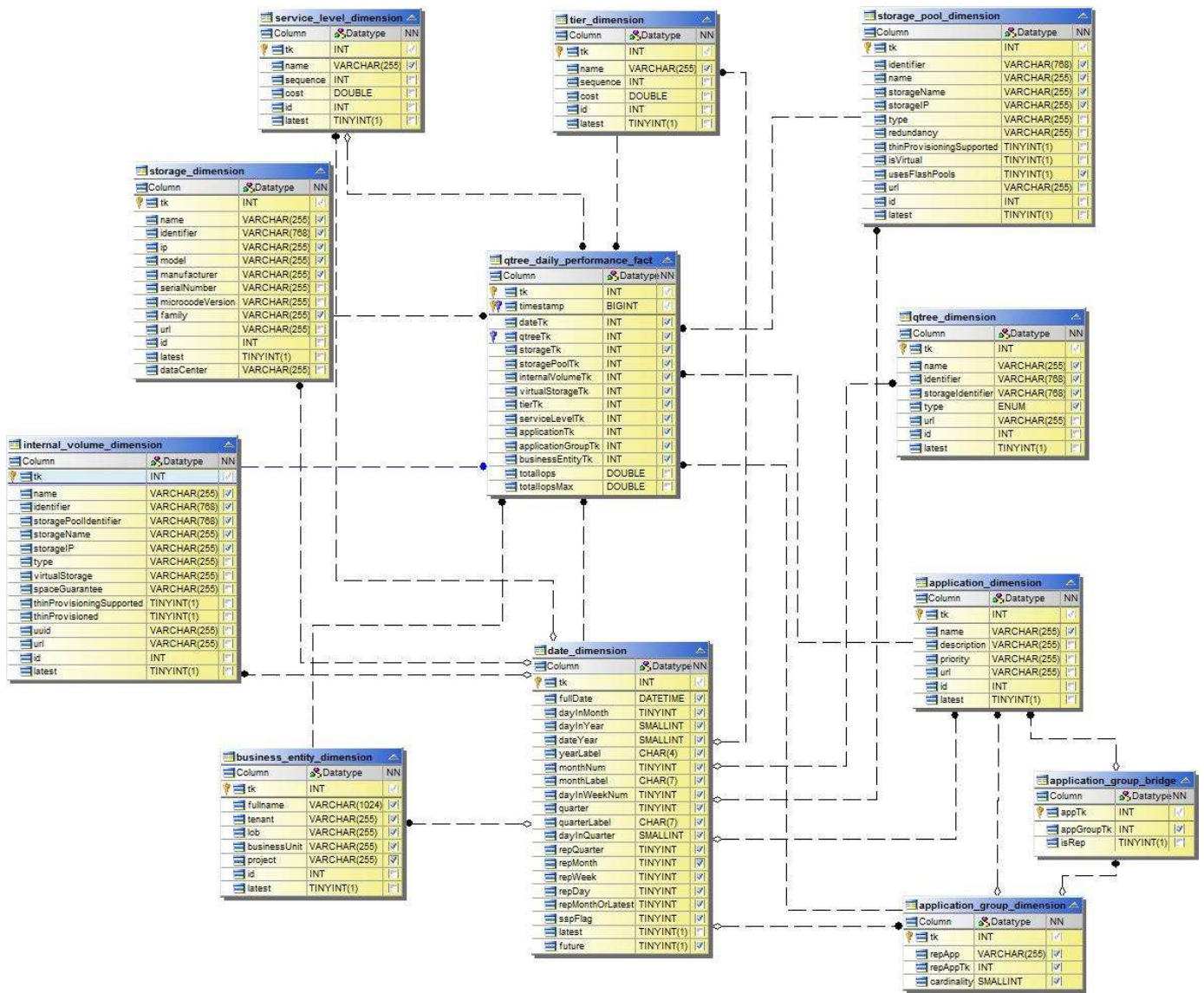
Desempenho de volume interno por hora



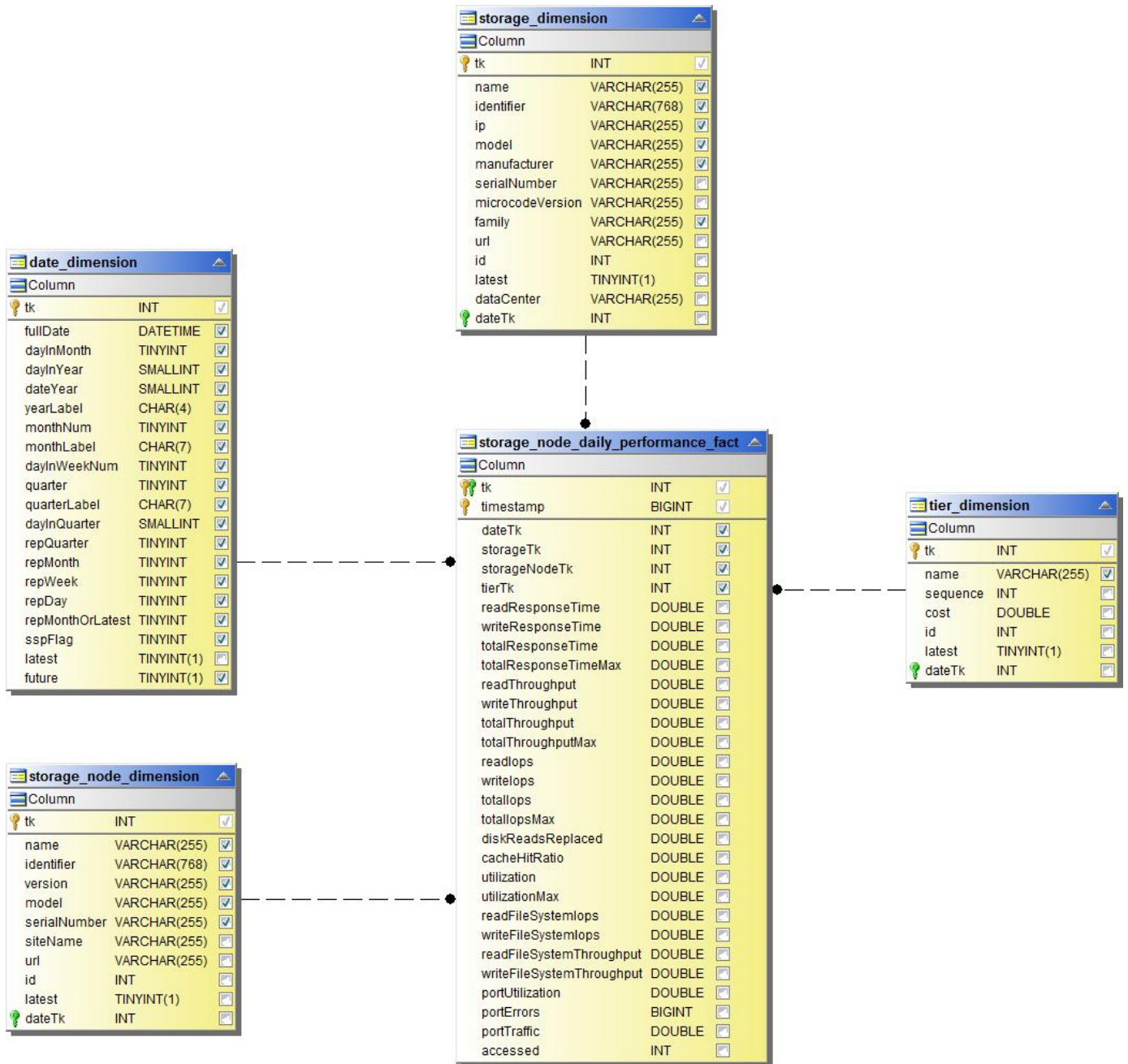
Desempenho diário de volume interno



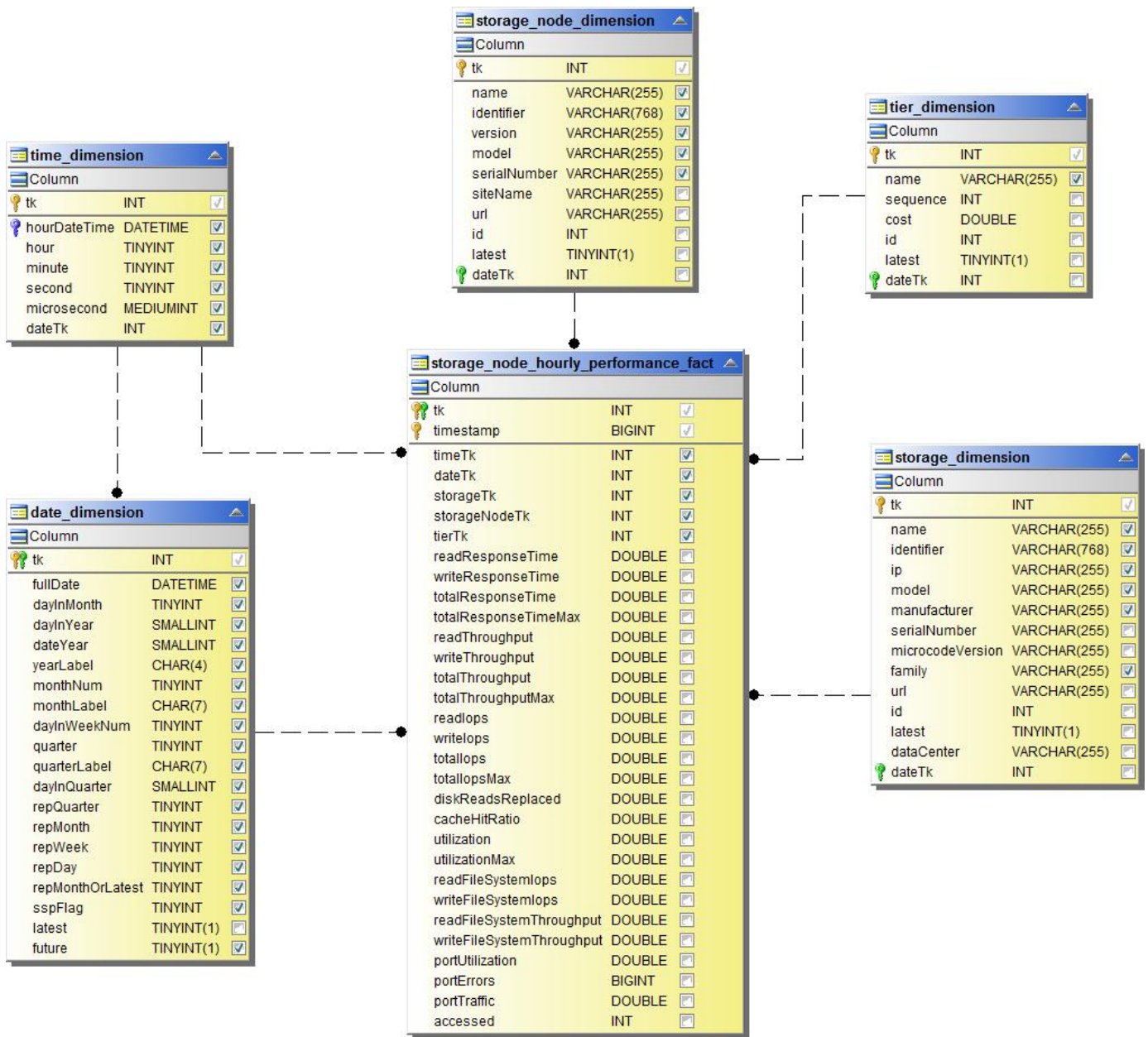
Desempenho diário de Qtree



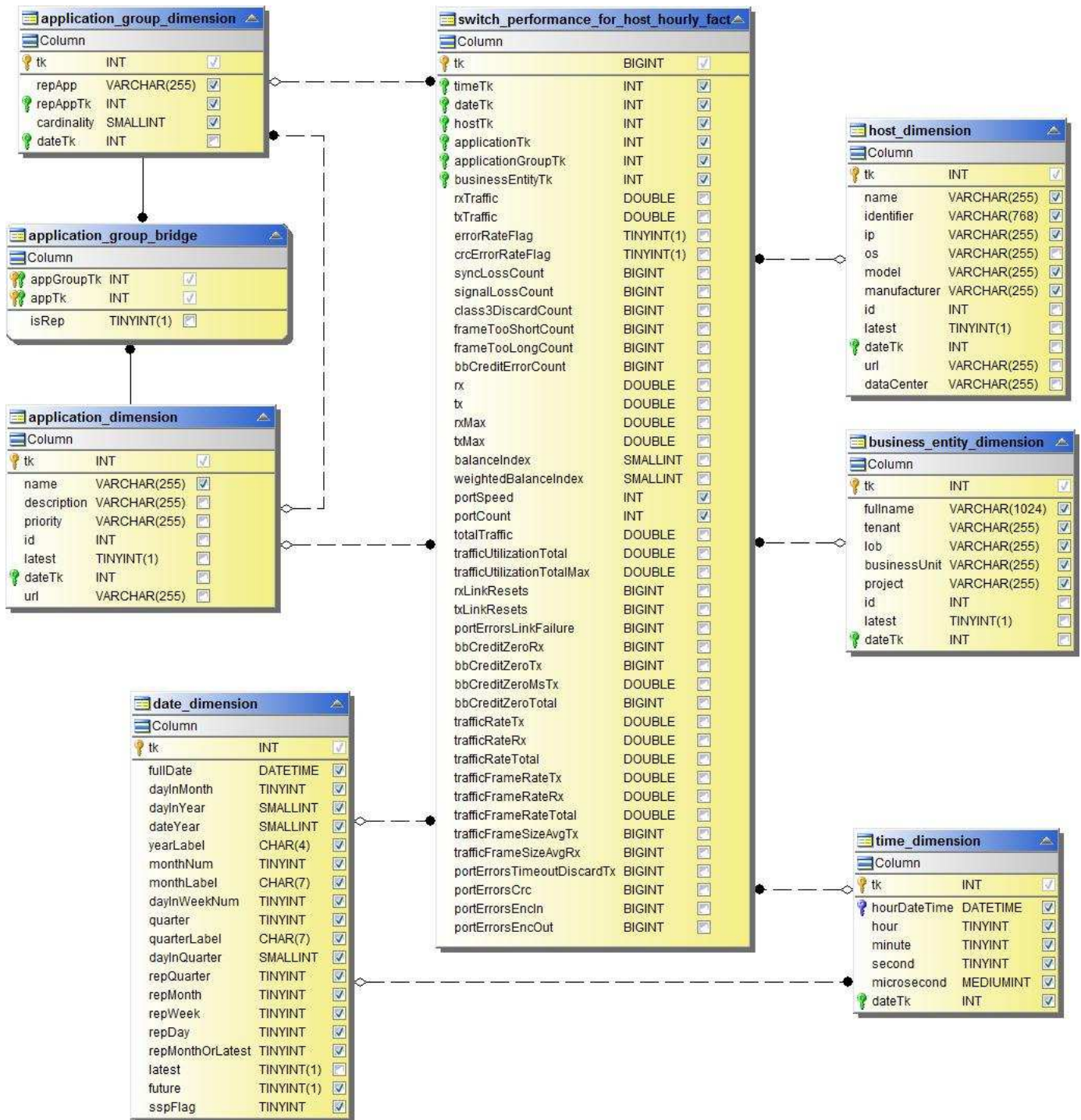
Desempenho diário do nó de storage



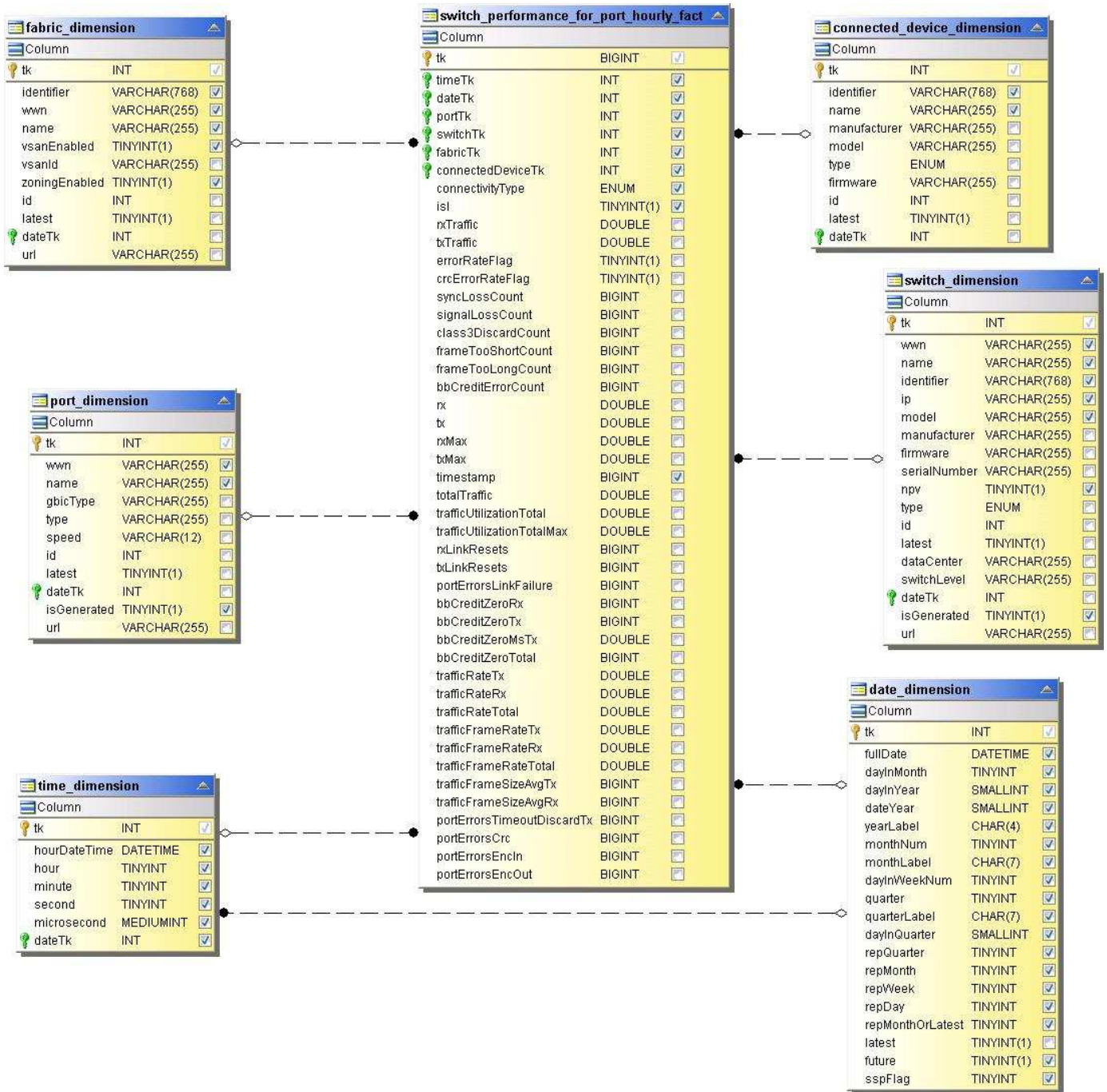
Desempenho por hora do nó de storage



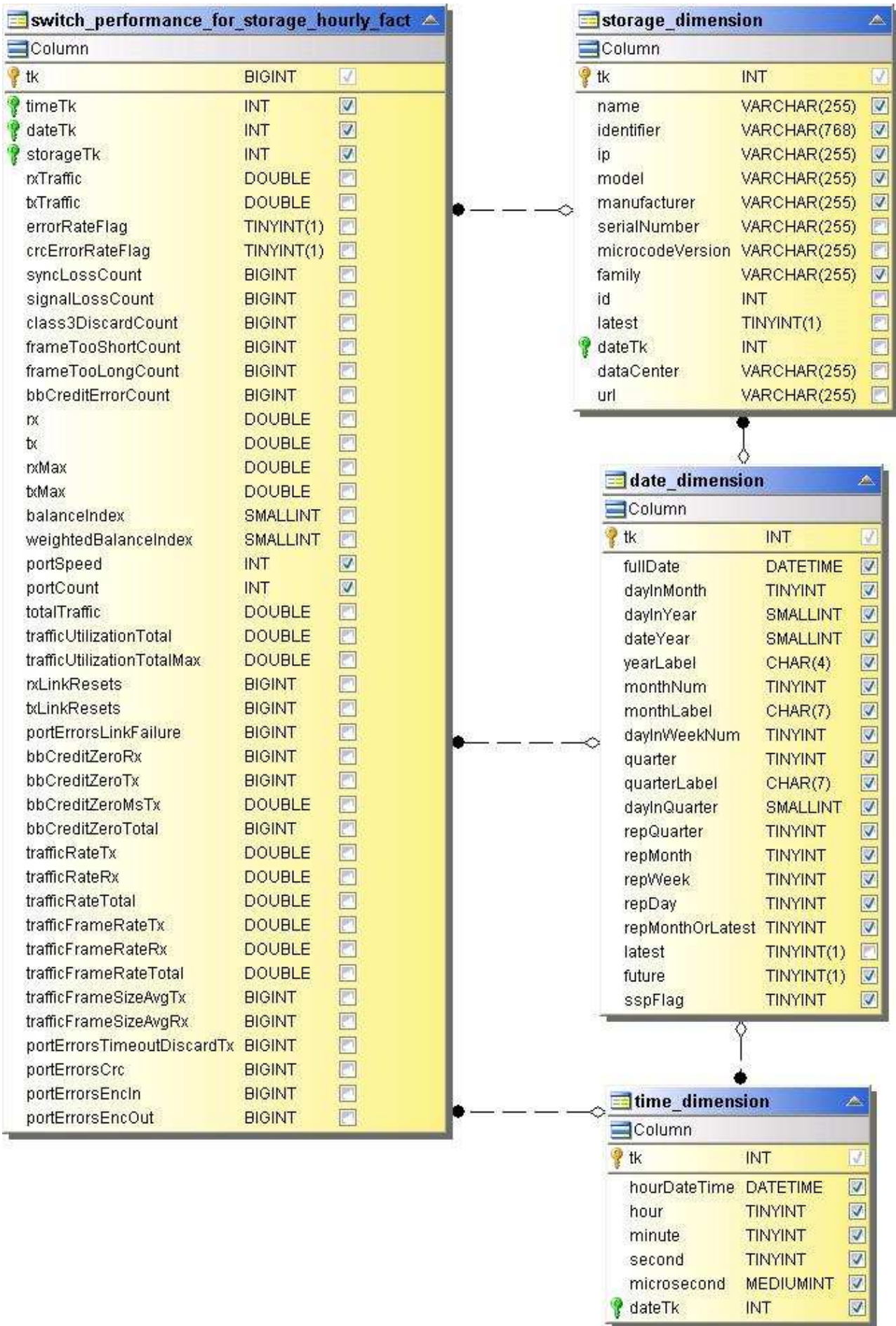
Mudar o desempenho por hora para o host



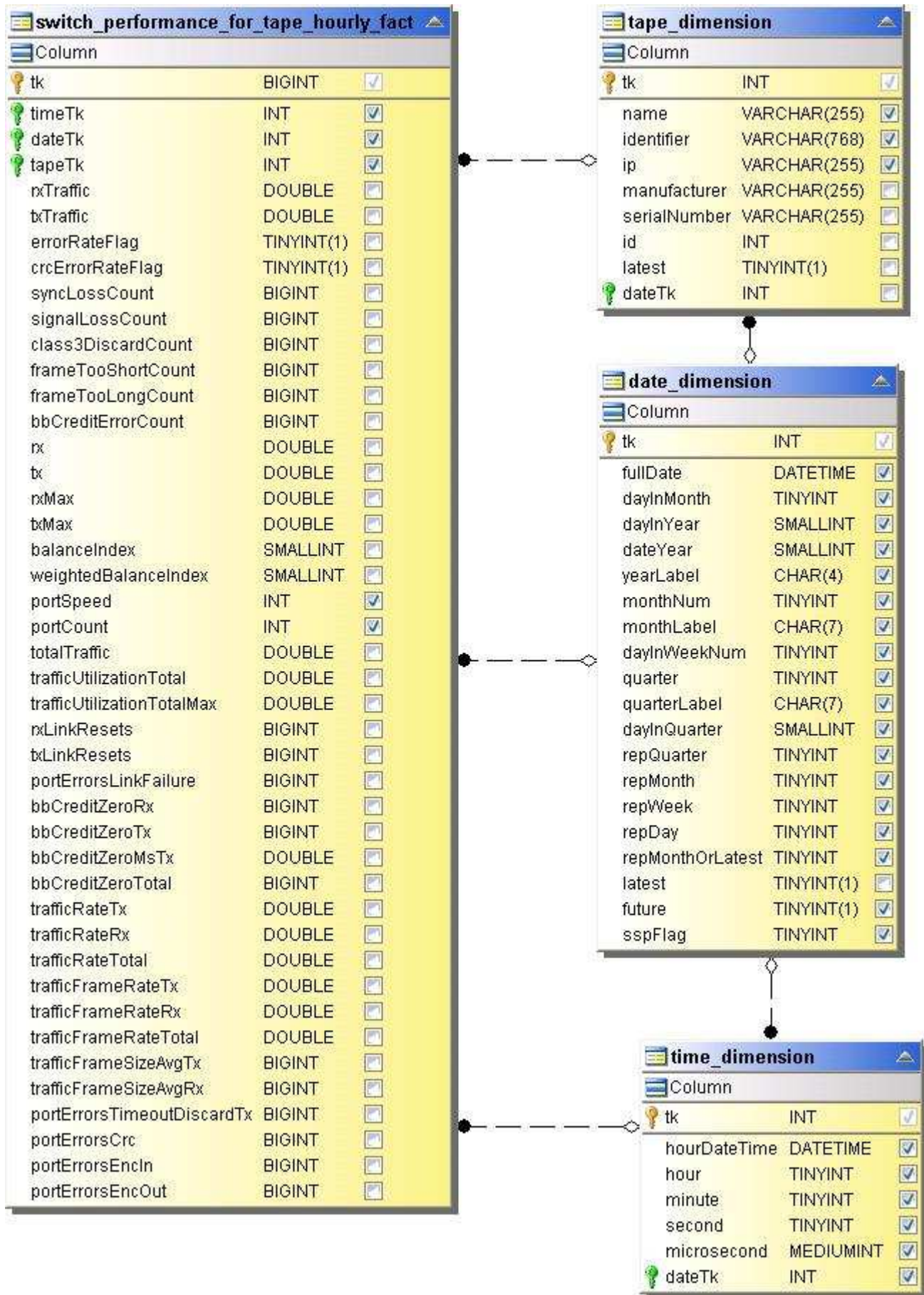
Mudar o desempenho por hora para a porta



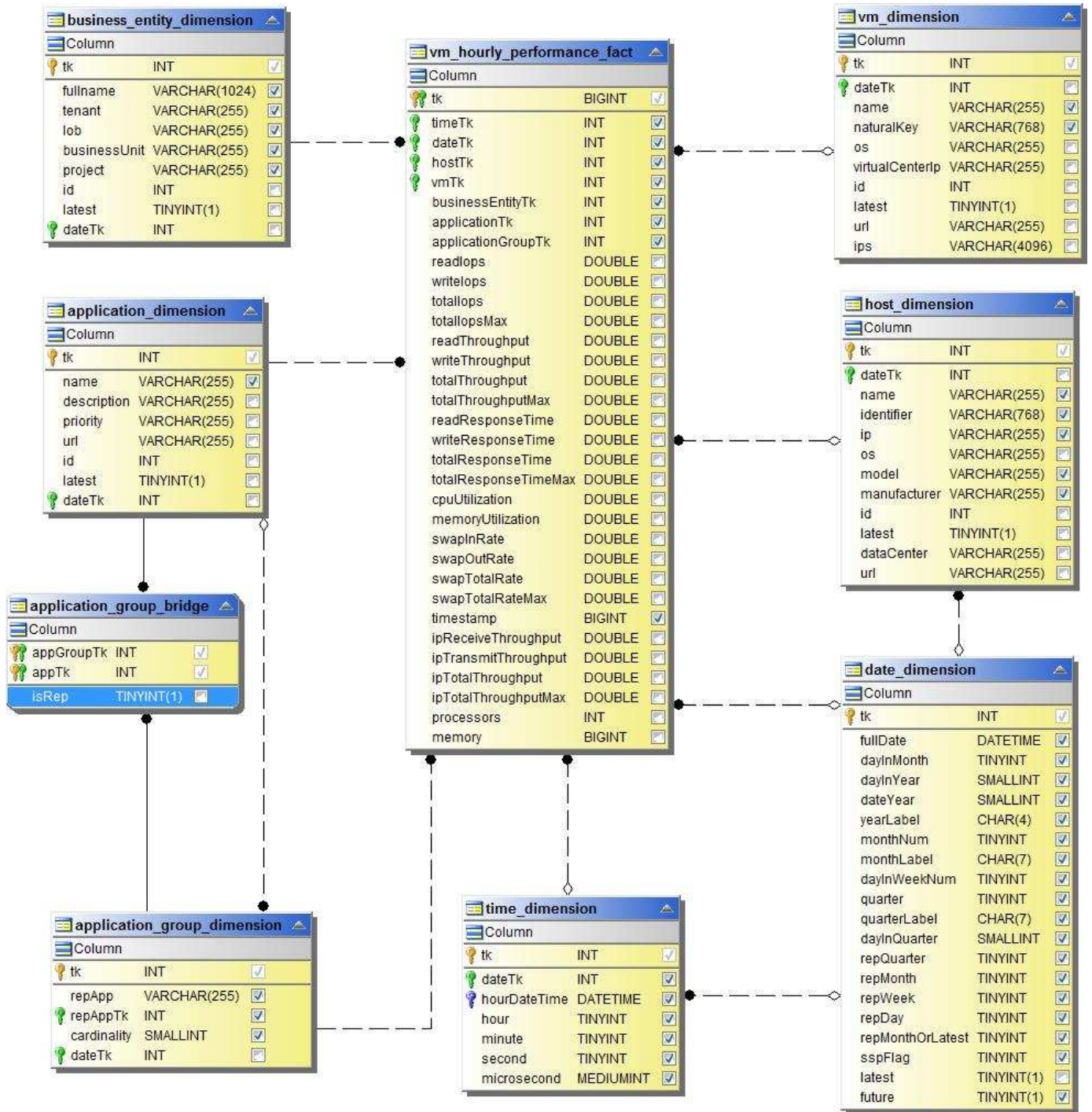
Altere o desempenho por hora para o armazenamento



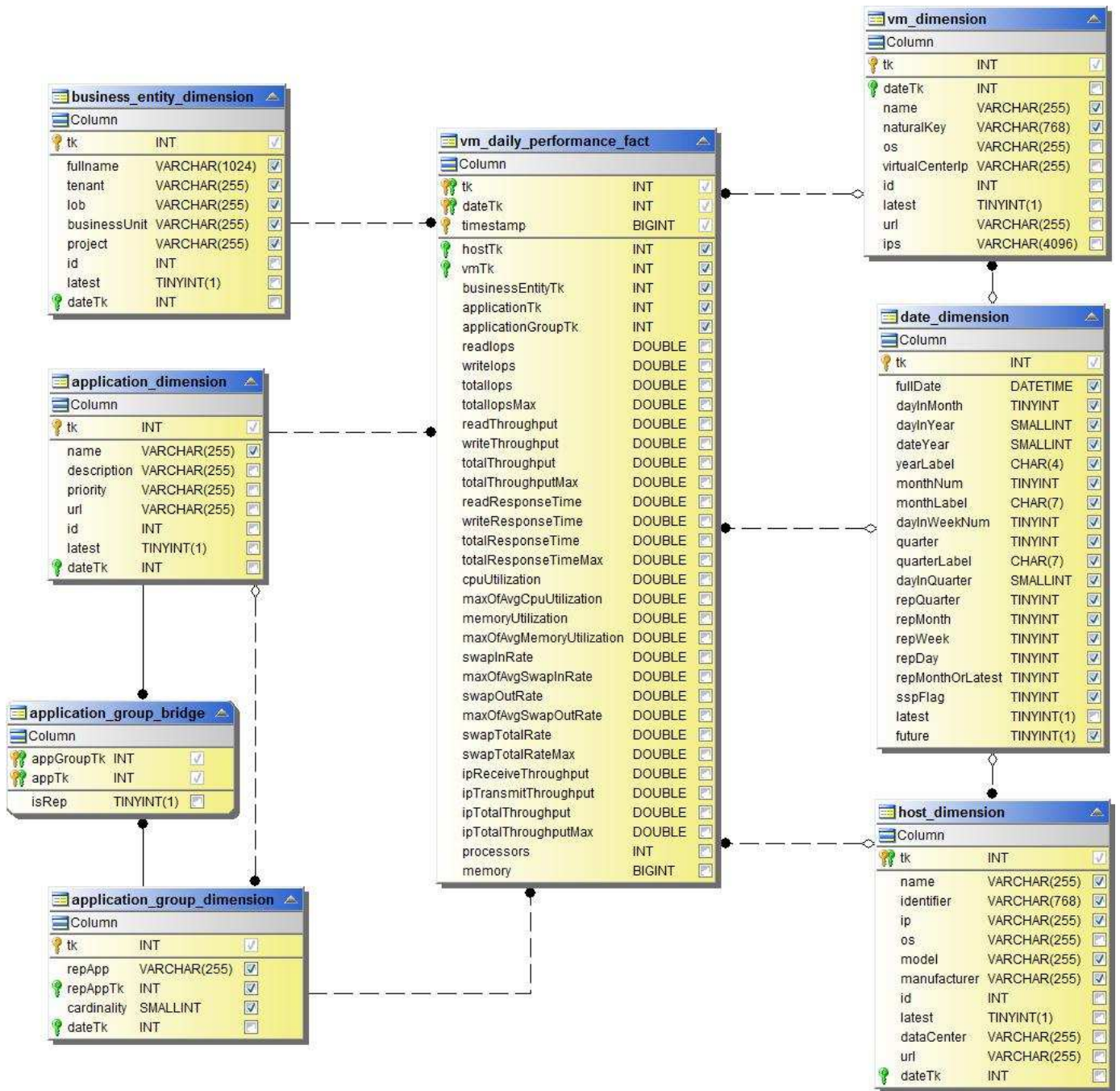
Mudar o desempenho de hora em hora para fita



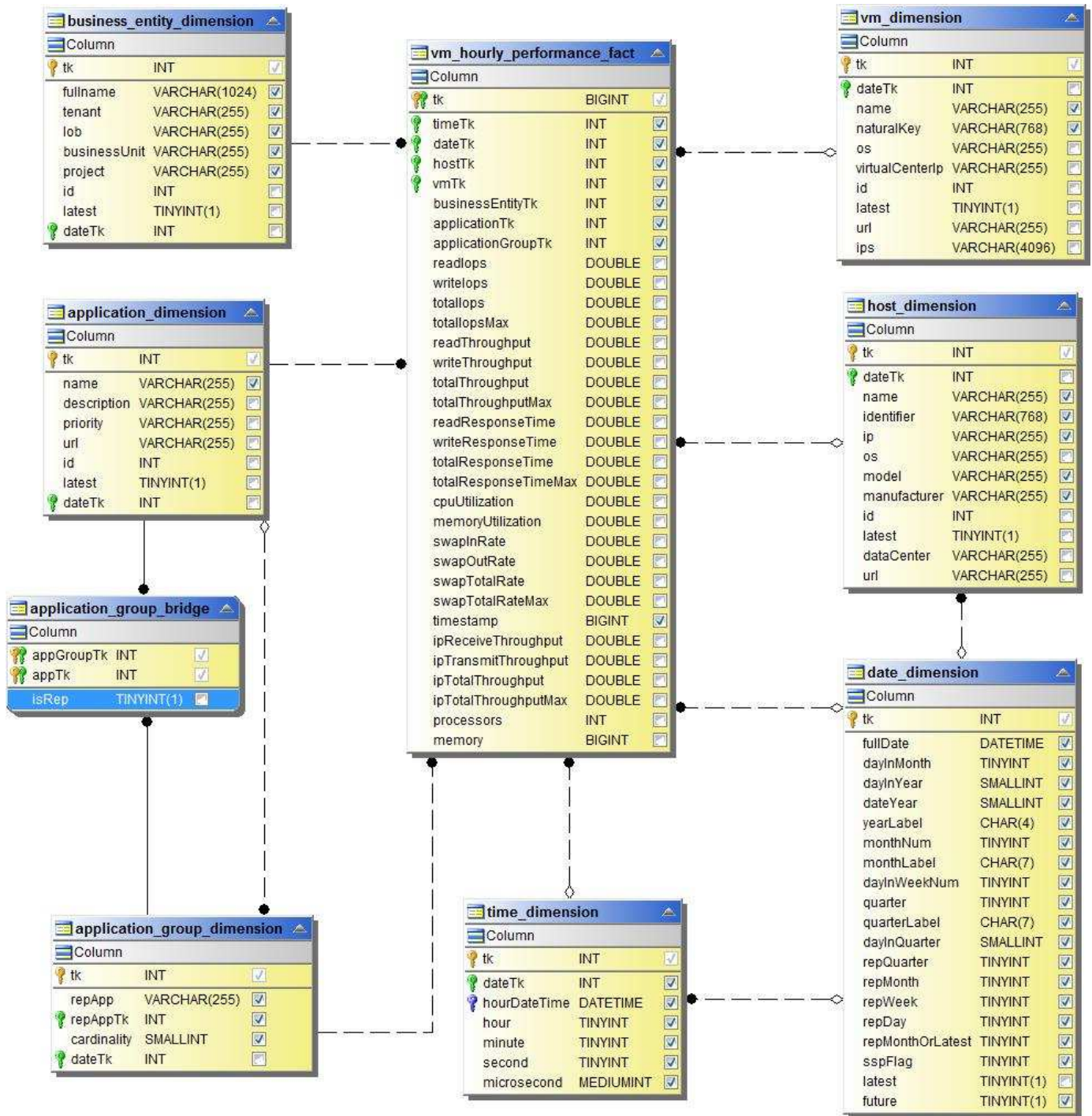
Performance de VM



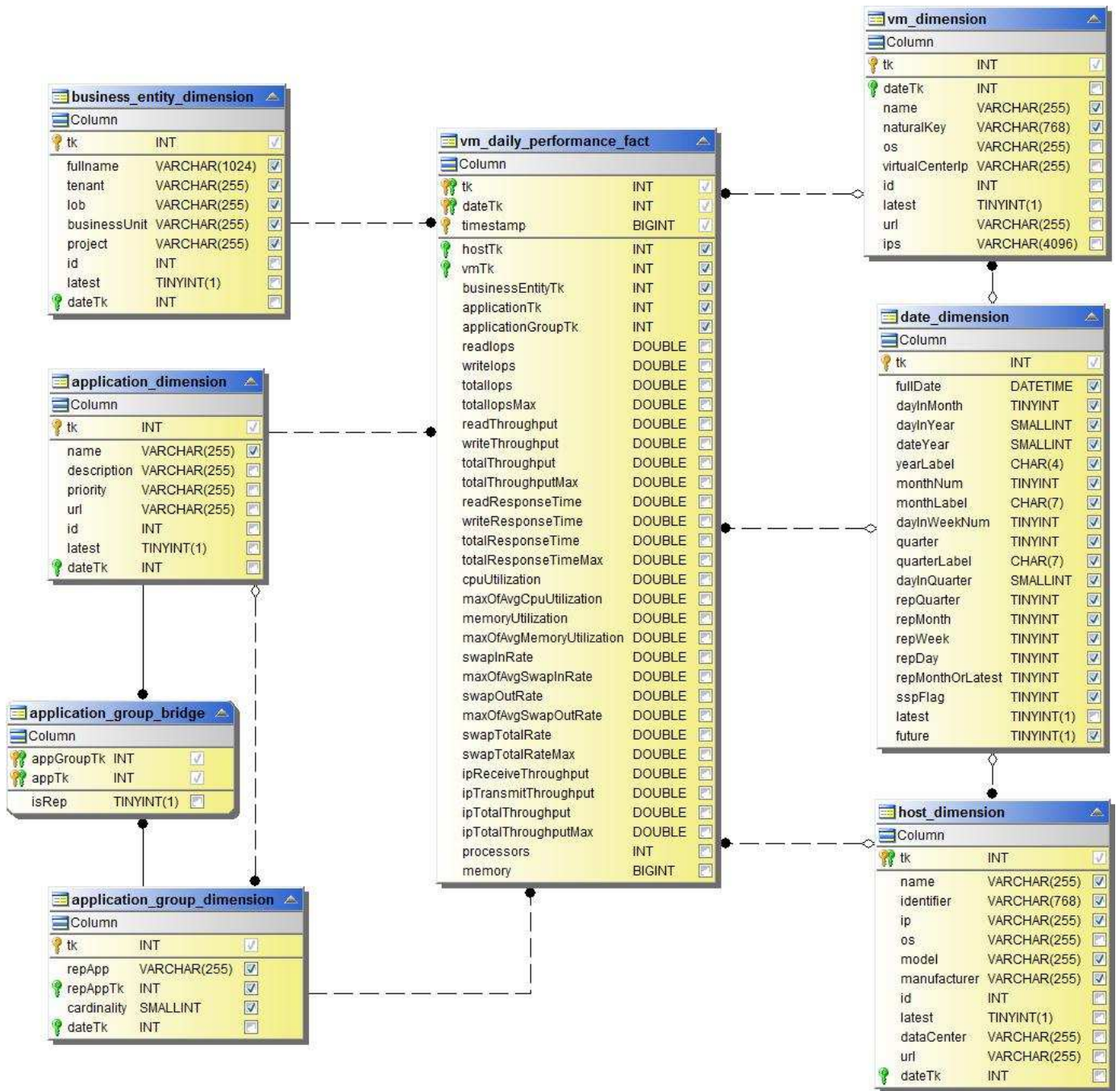
Desempenho diário da VM para o host



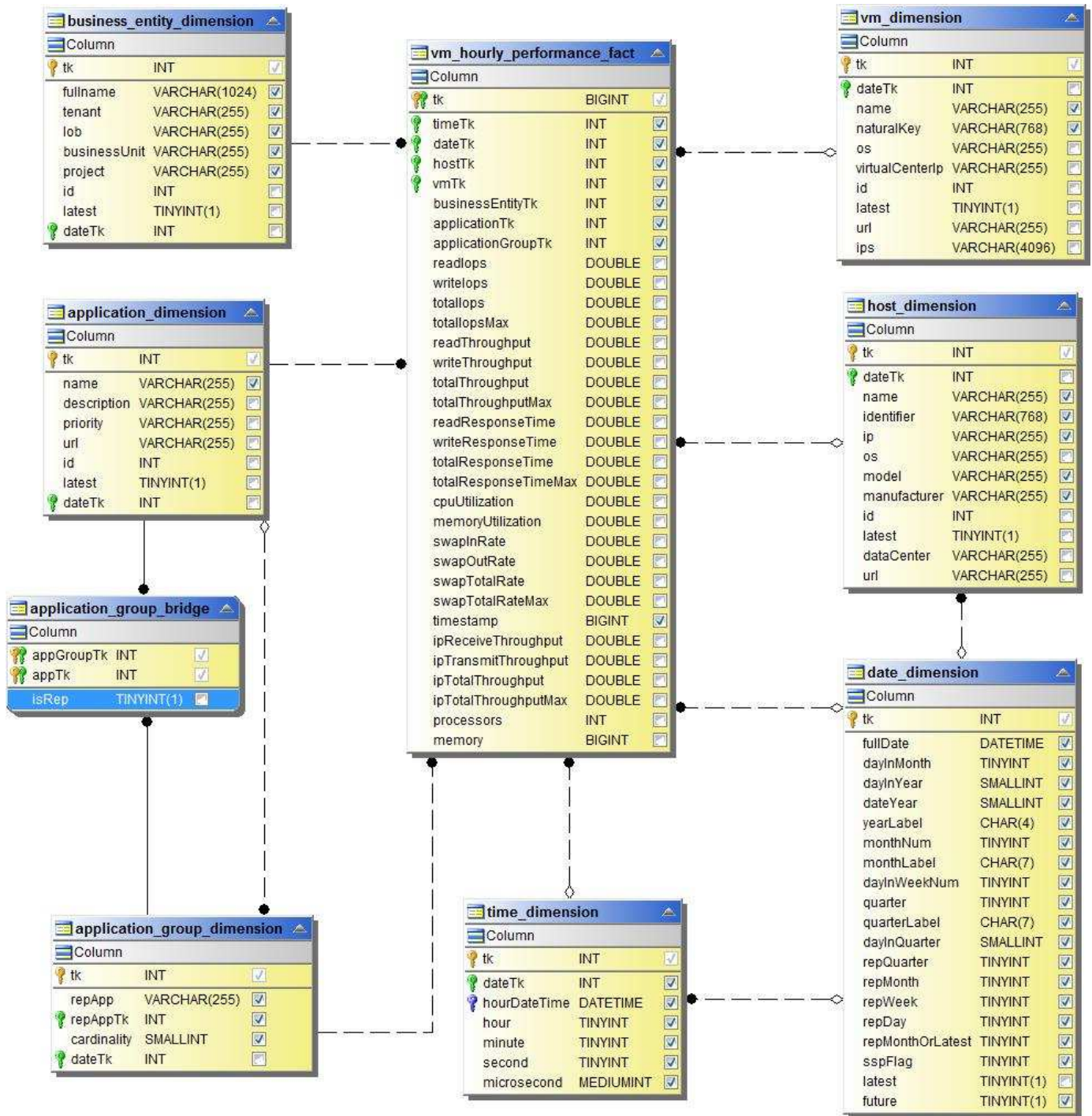
Desempenho da VM por hora para o host



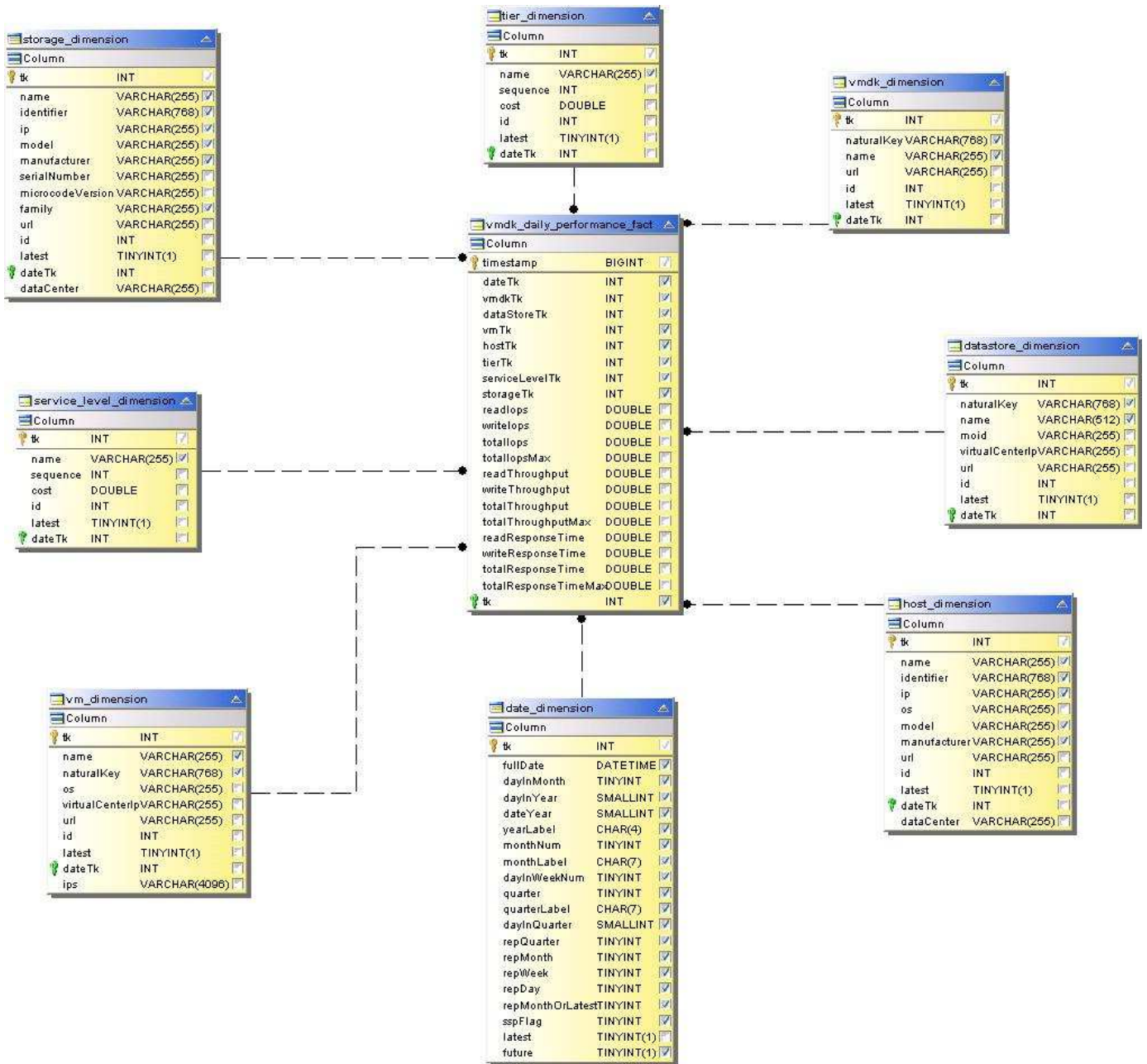
Desempenho diário da VM para o host



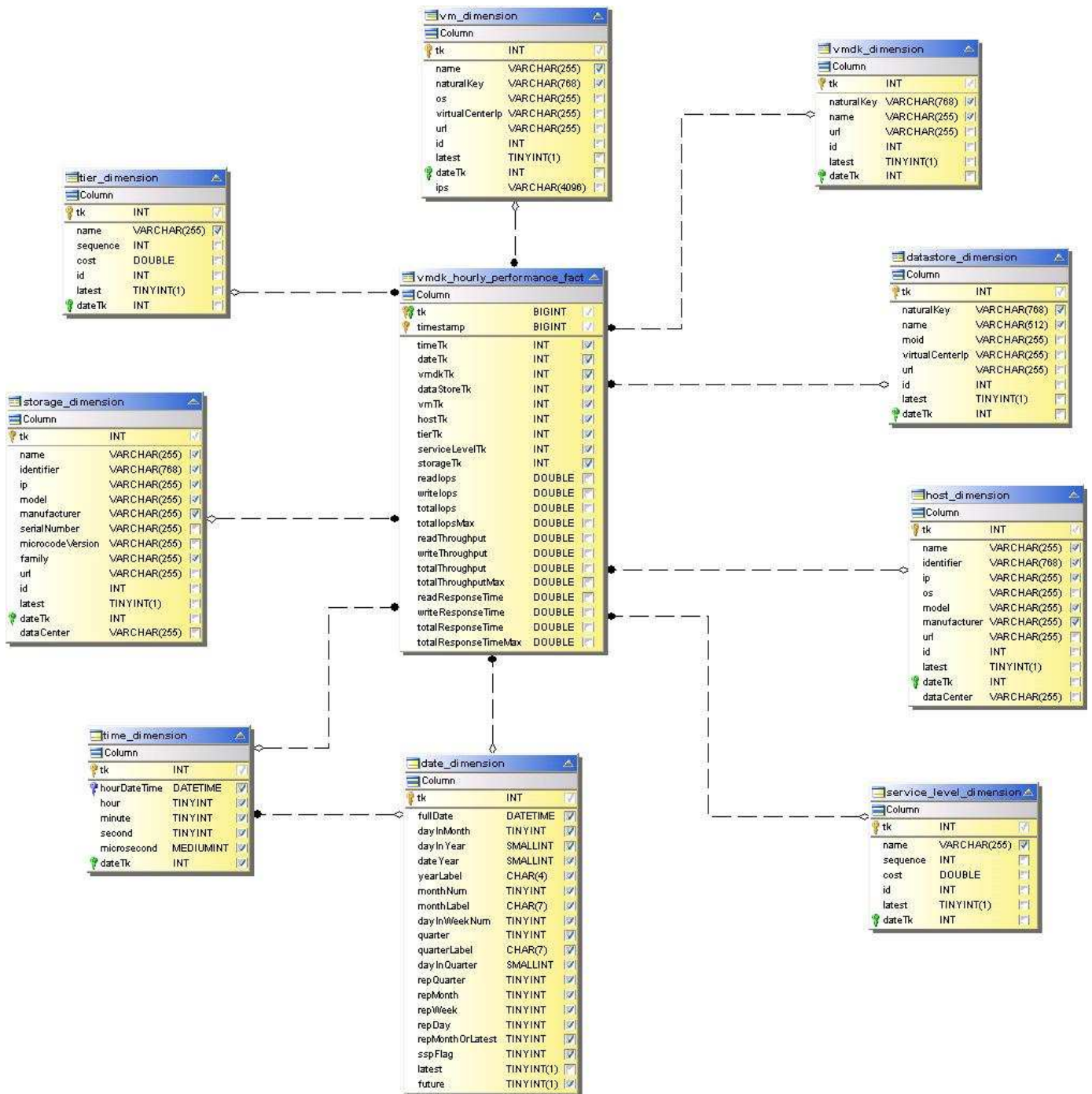
Desempenho da VM por hora para o host



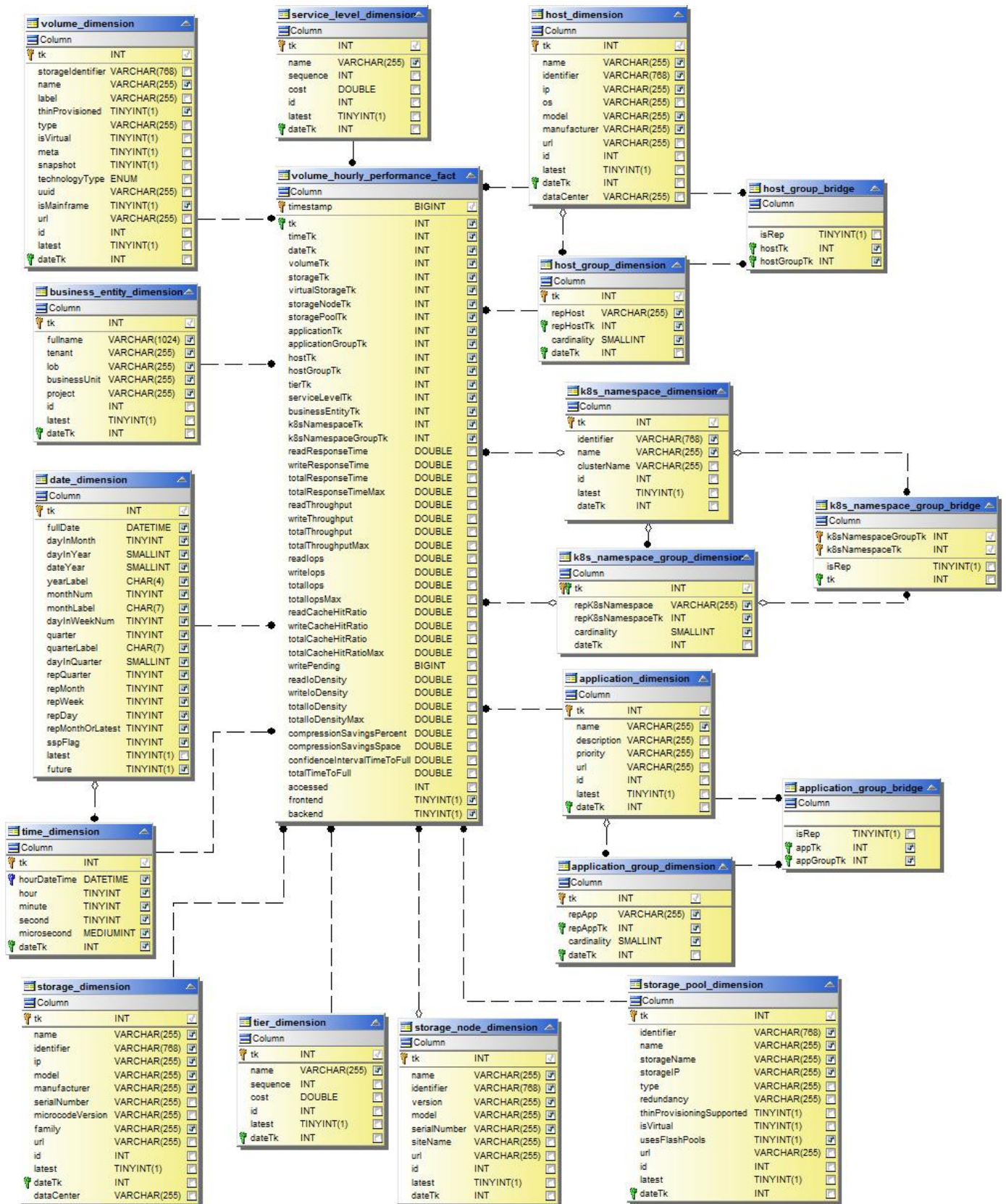
Desempenho diário do VMDK



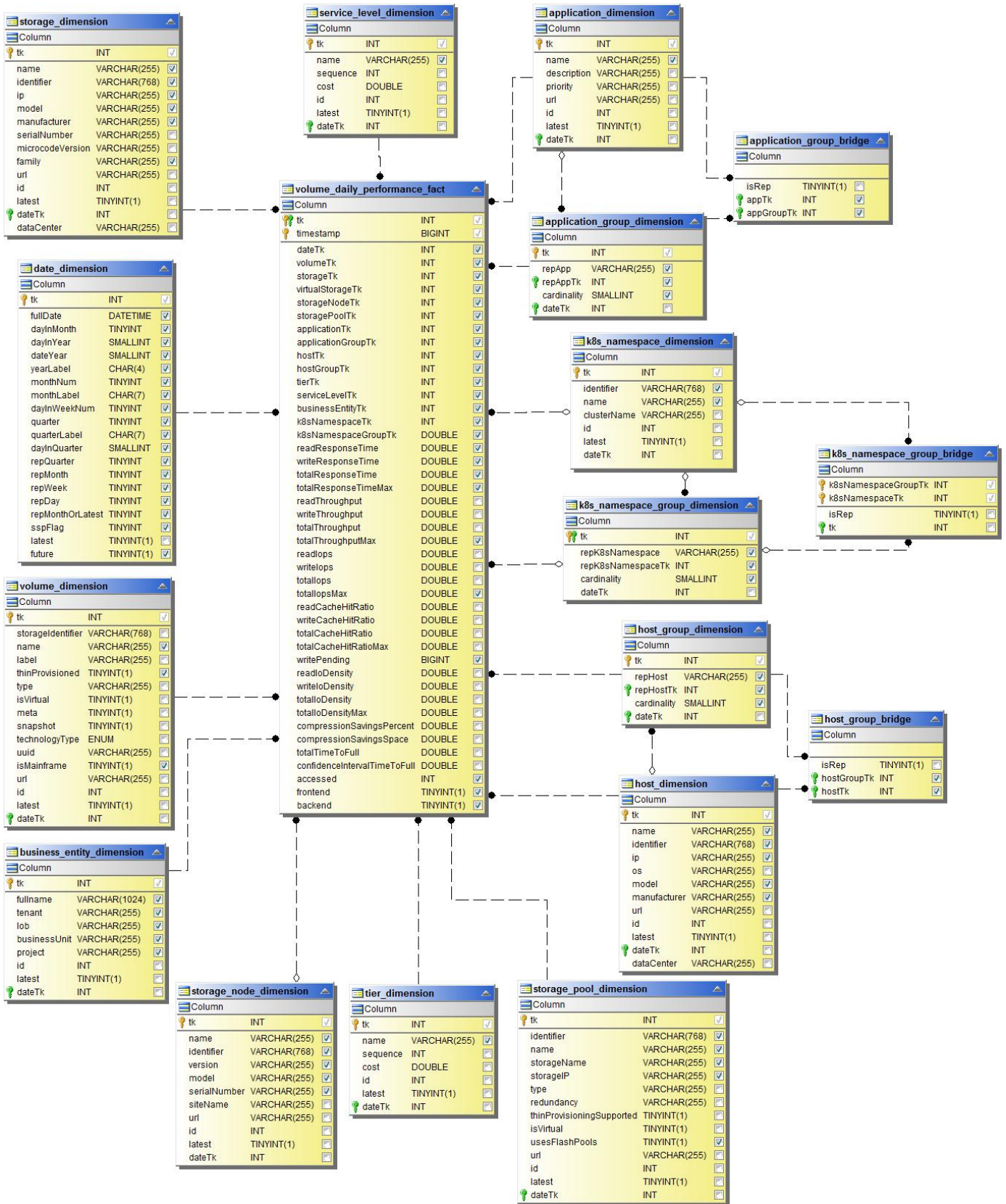
VMDK desempenho por hora



Desempenho por hora em volume



Volume de desempenho diário



Data Infrastructure Insights Schemas para relatórios

Essas tabelas e diagramas de esquema são fornecidos aqui como referência para o Data Infrastructure Insights Reporting.

"**Tabelas de esquema**" Em formato .PDF. Clique no link para abrir ou clique com o botão direito do Mouse e escolha *Salvar como...* para baixar.

"Diagramas de esquema"



O recurso relatórios está disponível no Data Infrastructure Insights "[Edição Premium](#)".

Kubernetes

Visão geral do cluster do Kubernetes

O Data Infrastructure Insights Kubernetes Explorer é uma ferramenta poderosa para exibir a integridade geral e o uso dos clusters do Kubernetes, além de permitir que você analise facilmente as áreas de investigação.

Clicar em **painéis > Kubernetes Explorer** abre a página de lista de clusters do Kubernetes. Esta página de visão geral contém uma tabela dos clusters do Kubernetes no seu locatário.



Filter By + ?

Clusters (2)

Name ↑	Overall Saturation (%)	CPU Saturation (%)	Memory Saturation (%)	Storage Saturation (%)	Nodes	Pods	Namespaces	Workloads
self	56	25	56	31	2	63	18	68
setoK3s	4	2	3	4	2	9	5	7

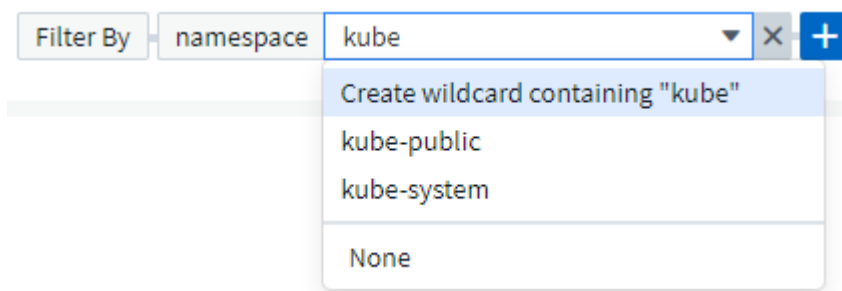
Lista de cluster

A lista de cluster exibe as seguintes informações para cada cluster no locatário:

- Cluster **Nome**. Clicar num nome de cluster abrirá o "[página de detalhes](#)" para esse cluster.
- **Percentagens de saturação**. A saturação geral é a mais alta da CPU, memória ou saturação de armazenamento.
- Número de * nós* no cluster. Clicar neste número abrirá a página da lista nó.
- Número de **pods** no cluster. Clicar neste número abrirá a página da lista Pod.
- Número de * namespaces* no cluster. Clicar nesse número abrirá a página de lista de namespace.
- Número de **cargas de trabalho** no cluster. Clicar neste número abrirá a página da lista carga de trabalho.

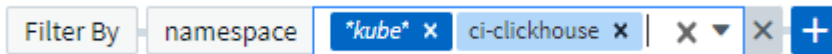
Refinando o filtro

Quando você está filtrando, à medida que você começa a digitar, você recebe a opção de criar um filtro * curinga* com base no texto atual. Selecionar esta opção irá retornar todos os resultados que correspondem à expressão curinga. Você também pode criar **expressões** usando NOT ou E, ou você pode selecionar a opção "nenhum" para filtrar valores nulos no campo.



Os filtros baseados em caracteres universais ou expressões (por exemplo, NÃO, E, "nenhum", etc.) são exibidos em azul escuro no campo de filtro. Os itens que você selecionar diretamente da lista são exibidos em

azul claro.



Os filtros do Kubernetes são contextuais, o que significa, por exemplo, que se você estiver em uma página de nó específica, o filtro pod_name listará apenas os pods relacionados a esse nó. Além disso, se você aplicar um filtro para um namespace específico, o filtro pod_name listará apenas pods nesse nó e nesse namespace.

Observe que a filtragem de caracteres curinga e expressão funciona com texto ou listas, mas não com valores numéricos, datas ou booleanos.

Antes de instalar ou atualizar o Operador de Monitoramento do Kubernetes do NetApp

Leia estas informações antes de instalar ou atualizar o ["Operador de monitoramento do Kubernetes"](#).

Componente	Requisito
Versão do Kubernetes	Kubernetes v1,20 e posterior.
Distribuições do Kubernetes	O Google Kubernetes Engine (GKE) Red Hat OpenShift Rancher Kubernetes Engine (RKE) VMware Tanzu é um dos nossos selecionados Jogos de Kubernetes
OS do Linux	O Data Infrastructure Insights não oferece suporte para nós executados com a arquitetura Arm64. Monitoramento de rede: Deve estar executando o kernel Linux versão 4.18.0 ou superior. O sistema operacional de fôto não é suportado.
Etiquetas	O Data Infrastructure Insights dá suporte ao monitoramento de nós do Kubernetes que estão executando o Linux, especificando um seletor de nós do Kubernetes que procura as seguintes etiquetas do Kubernetes nessas plataformas: Kubernetes v1,20 e superior: Kubernetes.io/os como plataforma de orquestração/Kubernetes: Cattle.io/os: linux
Comandos	Os comandos curl e kubectl devem estar disponíveis.; para obter melhores resultados, adicione esses comandos ao CAMINHO.
Conetividade	a cli do kubectl está configurada para se comunicar com o cluster K8s de destino e tem conetividade com a Internet ao seu ambiente Data Infrastructure Insights. Se você estiver atrás de um proxy durante a instalação, siga as instruções "Configurando o suporte Proxy" na seção da instalação do Operador. Para obter relatórios precisos de auditoria e dados, sincronize a hora na máquina do agente usando o Network Time Protocol (NTP) ou o Simple Network Time Protocol (SNTP).

Componente	Requisito
Outros	Se você estiver executando no OpenShift 4,6 ou superior, você deve seguir o "Instruções do OpenShift" além de garantir que esses pré-requisitos sejam atendidos.
Token de API	Se você estiver reimplantando o Operador (ou seja, está atualizando ou substituindo-o), não há necessidade de criar um novo token de API; você pode reutilizar o token anterior.

Coisas importantes a observar antes de começar

Se você estiver executando com um [proxy](#), tiver um [repositório personalizado](#), ou estiver usando [OpenShift](#), leia as seções a seguir cuidadosamente.

Leia também [Permissões](#) sobre .

Configurando o suporte Proxy

Há dois lugares onde você pode usar um proxy em seu local para instalar o Operador de Monitoramento do Kubernetes do NetApp. Estes podem ser os mesmos ou sistemas proxy separados:

- Proxy necessário durante a execução do snippet de código de instalação (usando "curl") para conectar o sistema onde o snippet é executado ao seu ambiente Data Infrastructure Insights
- Proxy necessário pelo cluster do Kubernetes de destino para se comunicar com seu ambiente Data Infrastructure Insights

Se você usar um proxy para um ou ambos, para instalar o Monitor operacional do Kubernetes do NetApp, primeiro você deve garantir que o proxy esteja configurado para permitir uma boa comunicação com o ambiente Insights da infraestrutura de dados. Por exemplo, a partir dos servidores/VMs a partir dos quais você deseja instalar o Operador, você precisa ter acesso ao Data Infrastructure Insights e poder baixar binários do Data Infrastructure Insights.

Para o proxy usado para instalar o Monitor operacional NetApp Kubernetes, antes de instalar o Operador, defina as variáveis de ambiente `http_proxy/https_proxy`. Para alguns ambientes proxy, você também pode precisar definir a variável `no_proxy environment`.

Para definir a(s) variável(s), execute as seguintes etapas em seu sistema **antes** de instalar o Operador de Monitoramento do Kubernetes do NetApp:

1. Defina a(s) variável(s) de ambiente `https_proxy` e/ou `http_proxy` para o usuário atual:
 - a. Se o proxy que está sendo configurado não tiver Autenticação (nome de usuário/senha), execute o seguinte comando:

```
export https_proxy=<proxy_server>:<proxy_port>
.. Se o proxy que está sendo configurado tiver Autenticação (nome de usuário/senha), execute este comando:
```

```
export
http_proxy=<proxy_username>:<proxy_password>@<proxy_server>:<proxy_port>
```

Para que o proxy usado para que o cluster do Kubernetes se comunique com o ambiente Insights de infraestrutura de dados, instale o Operador de Monitoramento do Kubernetes do NetApp depois de ler todas essas instruções.

Configure a seção proxy do AgentConfiguration no operator-config.yaml antes de implantar o Operador de Monitoramento do Kubernetes do NetApp.

```
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
    ...
  ...
```

Usando um repositório docker personalizado ou privado

Por padrão, o Operador de Monitoramento do Kubernetes do NetApp coletará imagens de contêiner do repositório de informações de infraestrutura de dados. Se você tiver um cluster do Kubernetes usado como destino para monitoramento e esse cluster estiver configurado para apenas extrair imagens de contêiner de um repositório ou Registro de contêiner personalizado ou privado do Docker, configure o acesso aos contêineres necessários pelo Operador de Monitoramento do Kubernetes do NetApp.

Execute o "trecho de recebimento de imagem" do bloco de instalação do Operador de Monitoramento do NetApp. Esse comando fará login no repositório Data Infrastructure Insights, extrairá todas as dependências de imagem do operador e fará logout do repositório Data Infrastructure Insights. Quando solicitado, insira a senha temporária do repositório fornecida. Este comando transfere todas as imagens utilizadas pelo operador, incluindo as funcionalidades opcionais. Veja abaixo quais recursos essas imagens são usadas.

Funcionalidade do operador principal e monitoramento do Kubernetes

- monitoramento de NetApp
- kube-rbac-proxy
- kube-state-metrics
- telegraf
- distroless-root-user

Registo de eventos

- bit fluente
- kuseurs-event-exporter

Desempenho de rede e mapa

- ci-net-observador

Envie a imagem do docker do operador para o seu repositório docker privado/local/empresarial de acordo com suas políticas corporativas. Certifique-se de que as tags de imagem e os caminhos de diretório para essas imagens em seu repositório sejam consistentes com os do repositório Data Infrastructure Insights.

Edite a implantação do operador de monitoramento no `operator-deployment.yaml` e modifique todas as referências de imagem para usar seu repositório Docker privado.

```
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>
```

Edite o `AgentConfiguration` no `operator-config.yaml` para refletir o novo local de repo do docker. Crie uma nova `imagePullSecret` para o seu repositório privado, para obter mais detalhes consulte <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
```

Instruções do OpenShift

Se você estiver executando no OpenShift 4,6 ou superior, você deve editar o `AgentConfiguration` em `operator-config.yaml` para ativar a configuração `runPrivileged`:

```
# Set runPrivileged to true SELinux is enabled on your kubernetes nodes
runPrivileged: true
```

O OpenShift pode implementar um nível adicional de segurança que pode bloquear o acesso a alguns componentes do Kubernetes.

Permissões

Se o cluster que você está monitorando contiver recursos personalizados que não tenham um ClusterRole que "[agregados para visualizar](#)", você precisará conceder manualmente ao operador acesso a esses recursos para monitorá-los com Registros de eventos.

1. Edite *operator-additional-permissions.yaml* antes de instalar, ou depois de instalar edite o recurso *ClusterRole/<namespace>-additional-permissions*
2. Crie uma nova regra para os apiGroups e recursos desejados com os verbos ["Get", "Watch", "list"]. Veja <https://kubernetes.io/docs/reference/access-authn-authz/rbac/>
3. Aplique as alterações ao cluster

Instalação e configuração do operador de monitoramento Kubernetes

O Data Infrastructure Insights oferece a coleção **Operador de Monitoramento do Kubernetes** para Kubernetes. Navegue até **Kubernetes > Collectors > Kubernetes Collector** para implantar um novo operador.

Antes de instalar o operador de monitoramento do Kubernetes

Consulte "[Pré-requisitos](#)" a documentação antes de instalar ou atualizar o Operador de Monitoramento do Kubernetes.

Instalando o Operador de Monitoramento do 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

clustername

Namespace

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.

3 Optional: Upload the operator images to your private repository

By default, the operator pulls container images from the Cloud Insights repository. To use a private repository, download the required images using the Image Pull command. Then upload them to your private repository maintaining the same tags and directory structure. Finally, update the image paths in `operator-deployment.yaml` and the docker repository settings in `operator-config.yaml`. For more information review [the documentation](#).

Copy Image Pull Snippet

Reveal Image Pull Snippet

Copy Repository Password

Reveal Repository Password

This password is valid for 24 hours.

4 Optional: Review available configuration options

Configure custom options such as proxy and private repository settings. Review the [instructions and available options](#).

5 Deploy the operator (create new or upgrade existing)

Execute the `kubectl` snippet to apply the following operator YAML files.

- `operator-setup.yaml` - Create the operator's dependencies.
- `operator-secrets.yaml` - Create secrets holding your API key.
- `operator-deployment.yaml`, `operator-cr.yaml` - Deploy the NetApp Kubernetes Monitoring Operator.
- `operator-config.yaml` - Apply the configuration settings if not already present.

Copy kubectl Apply Snippet

Reveal kubectl Apply Snippet

After deploying the operator, **delete or securely store `operator-secrets.yaml`**.

6 Next

Etapas para instalar o agente do operador de monitoramento do Kubernetes no Kubernetes:

1. Insira um nome de cluster e um namespace exclusivos. Se você [atualizar](#) é de um operador Kubernetes anterior, use o mesmo nome de cluster e namespace.
2. Uma vez que eles são inseridos, você pode copiar o snippet de comando de download para a área de transferência.
3. Cole o snippet em uma janela `bash` e execute-o. Os ficheiros de instalação do Operador serão transferidos. Observe que o snippet tem uma chave exclusiva e é válido por 24 horas.
4. Se você tiver um repositório personalizado ou privado, copie o trecho opcional Image Pull, cole-o em um shell `bash` e execute-o. Depois que as imagens tiverem sido puxadas, copie-as para o seu repositório privado. Certifique-se de manter as mesmas tags e estrutura de pastas. Atualize os caminhos em `operator-deployment.yaml`, bem como as configurações do repositório docker em `operator-config.yaml`.
5. Se desejar, revise as opções de configuração disponíveis, como proxy ou configurações de repositório privado. Você pode ler mais sobre "[opções de configuração](#)".
6. Quando estiver pronto, implante o Operador copiando o snippet de aplicação kubectl, baixando-o e executando-o.
7. A instalação prossegue automaticamente. Quando estiver concluído, clique no botão `Next`.
8. Quando a instalação estiver concluída, clique no botão `Next`. Certifique-se também de excluir ou armazenar com segurança o arquivo `operator-secrets.yaml`.

Se estiver usando um proxy, leia sobre [configurando proxy](#).

Se você tiver um repositório personalizado, leia sobre [usando um repositório docker personalizado/privado](#).

Componentes de monitoramento do Kubernetes

O monitoramento do Kubernetes do Data Infrastructure Insights é composto por quatro componentes de monitoramento:

- Métricas do cluster
- Desempenho de rede e mapa (opcional)
- Registos de eventos (opcional)
- Análise de mudança (opcional)

Os componentes opcionais acima são ativados por padrão para cada coletor do Kubernetes; se você decidir que não precisa de um componente para um coletor específico, você pode desativá-lo navegando para **Kubernetes > coletores** e selecionando *Modificar implantação* no menu "três pontos" do coletor à direita da tela.

NetApp / Observability / Collectors

Data Collectors 21 Acquisition Units 4 **Kubernetes Collectors**

Kubernetes Collectors (13)


[View Upgrade/Delete Documentation](#)

[+ Kubernetes Collector](#)

Filter...

Cluster Name ↑	Status	Operator Version	Network Performance and Map	Change Analysis	
au-pod	Outdated	1.1540.0	1.347.0	1.162.0	
jks-troublemaker	Latest	1.1579.0	N/A	1.201.0	
oom-test	Outdated	1.1555.0	N/A	1.161.0	Modify Deployment

O ecrã mostra o estado atual de cada componente e permite desativar ou ativar componentes para esse coletor, conforme necessário.

 **kubernetes**
Kubernetes

Modify Deployment

Cluster Information

Kubernetes Cluster
ci-demo-01

Network Performance and Map
Enabled - Online

Event Logs
Enabled - Online

Change Analysis
Enabled - Online

Deployment Options

[Need Help?](#)

Network Performance and Map

Event Logs

Change Analysis

Cancel

Complete Modification

Atualização para o operador de monitoramento mais recente do Kubernetes

Determine se existe um AgentConfiguration com o Operador existente (se o seu namespace não for o *NetApp-monitoring* padrão, substitua o namespace apropriado):

```
kubectl -n netapp-monitoring get agentconfiguration netapp-monitoring-configuration
```

Se existir uma configuração AgentConfiguration:

- **Instale** O operador mais recente sobre o operador existente.
 - Certifique-se de que está [puxando as imagens mais recentes do recipiente](#) se estiver a utilizar um repositório personalizado.

Se o AgentConfiguration não existir:

- Anote o nome do cluster conforme reconhecido pelo Data Infrastructure Insights (se o namespace não for o monitoramento padrão do NetApp, substitua o namespace apropriado):

```
kubectl -n netapp-monitoring get agent -o jsonpath='{.items[0].spec.cluster-name}'
```

* Crie uma cópia de segurança do Operador existente (se o seu namespace não for o NetApp-monitoring predefinido, substitua o namespace apropriado):

```
kubectl -n netapp-monitoring get agent -o yaml > agent_backup.yaml
```

* <<to-remove-the-kubernetes-monitoring-operator,Desinstalar>> O operador existente.

* <<installing-the-kubernetes-monitoring-operator,Instale>> O operador mais recente.

- Use o mesmo nome de cluster.
- Depois de baixar os arquivos YAML do Operador mais recentes, coloque as personalizações encontradas no Agent_backup.yaml para o operador-config.yaml baixado antes de implantar.
- Certifique-se de que está [puxando as imagens mais recentes do recipiente](#) se estiver a utilizar um repositório personalizado.

Parando e iniciando o Operador de Monitoramento do Kubernetes

Para parar o operador de monitoramento do Kubernetes:

```
kubectl -n netapp-monitoring scale deploy monitoring-operator --replicas=0
```

Para iniciar o operador de monitoramento do Kubernetes:

```
kubectl -n netapp-monitoring scale deploy monitoring-operator --replicas=1
```

Desinstalação

Para remover o operador de monitoramento do Kubernetes

Observe que o namespace padrão para o Operador de Monitoramento do Kubernetes é "NetApp-monitoring". Se você tiver definido seu próprio namespace, substitua esse namespace nesses e todos os comandos e arquivos subsequentes.

As versões mais recentes do operador de monitoramento podem ser desinstaladas com os seguintes comandos:

```
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>
```

Se o operador de monitoramento foi implantado em seu próprio namespace dedicado, exclua o namespace:

```
kubectl delete ns <NAMESPACE>
```

Se o primeiro comando retornar "nenhum recurso encontrado", use as instruções a seguir para desinstalar versões mais antigas do operador de monitoramento.

Execute cada um dos seguintes comandos em ordem. Dependendo da sua instalação atual, alguns desses comandos podem retornar mensagens "objeto não encontrado". Essas mensagens podem ser ignoradas com segurança.

```
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>
```

Se uma restrição de contexto de segurança foi criada anteriormente:

```
kubectl delete scc telegraf-hostaccess
```

Sobre o Kube-State-metrics

O Operador de Monitoramento do Kubernetes do NetApp instala suas próprias métricas de estado do kube para evitar conflitos com outras instâncias.

Para obter informações sobre métricas Kube-State, ["esta página"](#) consulte .

Configurar/personalizar o Operador

Essas seções contêm informações sobre como personalizar a configuração do operador, trabalhar com proxy, usar um repositório docker personalizado ou privado ou trabalhar com o OpenShift.

Opções de configuração

As configurações mais comumente modificadas podem ser configuradas no recurso personalizado *AgentConfiguration*. Você pode editar esse recurso antes de implantar o operador editando o arquivo *operator-config.yaml*. Este arquivo inclui exemplos comentados de configurações. Consulte a lista de ["definições disponíveis"](#) para obter a versão mais recente do operador.

Você também pode editar esse recurso depois que o operador tiver sido implantado usando o seguinte comando:

```
kubectl -n netapp-monitoring edit AgentConfiguration
Para determinar se a versão implantada do operador suporta
AgentConfiguration, execute o seguinte comando:
```

```
kubectl get crd agentconfigurations.monitoring.netapp.com
Se você vir uma mensagem "erro do servidor (NotFound)", seu operador deve
ser atualizado antes de poder usar o AgentConfiguration.
```

Configurando o suporte Proxy

Há dois lugares onde você pode usar um proxy em seu locatário para instalar o Operador de Monitoramento do Kubernetes. Estes podem ser os mesmos ou sistemas proxy separados:

- Proxy necessário durante a execução do snippet de código de instalação (usando "curl") para conectar o sistema onde o snippet é executado ao seu ambiente Data Infrastructure Insights
- Proxy necessário pelo cluster do Kubernetes de destino para se comunicar com seu ambiente Data Infrastructure Insights

Se você usar um proxy para um ou ambos, para instalar o Monitor operacional Kubernetes, primeiro você deve garantir que o proxy esteja configurado para permitir uma boa comunicação com o ambiente Insights da infraestrutura de dados. Se você tiver um proxy e puder acessar o Data Infrastructure Insights do servidor/VM a partir do qual deseja instalar o Operador, o proxy provavelmente estará configurado corretamente.

Para o proxy usado para instalar o Monitor operacional Kubernetes, antes de instalar o Operador, defina as variáveis de ambiente `http_proxy/https_proxy`. Para alguns ambientes proxy, você também pode precisar definir a variável `no_proxy environment`.

Para definir a(s) variável(s), execute as seguintes etapas em seu sistema **antes** de instalar o Operador de Monitoramento do Kubernetes:

1. Defina a(s) variável(s) de ambiente `https_proxy` e/ou `http_proxy` para o usuário atual:
 - a. Se o proxy que está sendo configurado não tiver Autenticação (nome de usuário/senha), execute o seguinte comando:

```
export https_proxy=<proxy_server>:<proxy_port>
.. Se o proxy que está sendo configurado tiver Autenticação (nome de usuário/senha), execute este comando:
```

```
export
http_proxy=<proxy_username>:<proxy_password>@<proxy_server>:<proxy_port>
```

Para que o proxy usado para que o cluster do Kubernetes se comunique com o ambiente Data Infrastructure Insights, instale o Operador de Monitoramento do Kubernetes depois de ler todas essas instruções.

Configure a seção proxy do AgentConfiguration no `operator-config.yaml` antes de implantar o Operador de Monitoramento do Kubernetes.

```
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
  ...
  ...
```

Usando um repositório docker personalizado ou privado

Por padrão, o operador de monitoramento do Kubernetes coletará imagens de contêntor do repositório Data Infrastructure Insights. Se você tiver um cluster do Kubernetes usado como destino para monitoramento e esse cluster estiver configurado para extrair apenas imagens de contêntor de um repositório ou Registro de contêntor personalizado ou privado do Docker, configure o acesso aos contêntores necessários pelo Operador de Monitoramento do Kubernetes.

Execute o "trecho de recebimento de imagem" do bloco de instalação do Operador de Monitoramento do NetApp. Esse comando fará login no repositório Data Infrastructure Insights, extrairá todas as dependências de imagem do operador e fará logout do repositório Data Infrastructure Insights. Quando solicitado, insira a senha temporária do repositório fornecida. Este comando transfere todas as imagens utilizadas pelo operador, incluindo as funcionalidades opcionais. Veja abaixo quais recursos essas imagens são usadas.

Funcionalidade do operador principal e monitoramento do Kubernetes

- monitoramento de NetApp
- ci-kube-rbac-proxy
- ci-ksm
- ci-telegraf
- distroless-root-user

Registro de eventos

- ci-fluente-bit
- ci-kurein-event-exporter

Desempenho de rede e mapa

- ci-net-observador

Envie a imagem do docker do operador para o seu repositório docker privado/local/empresarial de acordo com suas políticas corporativas. Certifique-se de que as tags de imagem e os caminhos de diretório para essas imagens em seu repositório sejam consistentes com os do repositório Data Infrastructure Insights.

Edite a implantação do operador de monitoramento no `operator-deployment.yaml` e modifique todas as referências de imagem para usar seu repositório Docker privado.

```
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>
```

Edite o `AgentConfiguration` no `operator-config.yaml` para refletir o novo local de repo do docker. Crie uma nova `imagePullSecret` para o seu repositório privado, para obter mais detalhes consulte <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
```

Instruções do OpenShift

Se você estiver executando no OpenShift 4,6 ou superior, você deve editar o `AgentConfiguration` em `operator-config.yaml` para ativar a configuração `runPrivileged`:

```
# Set runPrivileged to true SELinux is enabled on your kubernetes nodes  
runPrivileged: true
```

O OpenShift pode implementar um nível adicional de segurança que pode bloquear o acesso a alguns componentes do Kubernetes.

Tolerações e taints

O `NetApp-ci-telegraf-ds`, o `NetApp-CI-Fluent-bit-ds` e o `NetApp-CI-NET-Observer-L4-DS` DaemonSets devem agendar um pod em cada nó do cluster para coletar corretamente os dados em todos os nós. O operador foi

configurado para tolerar alguns **taints** conhecidos. Se você tiver configurado quaisquer taints personalizados em seus nós, impedindo assim que os pods sejam executados em cada nó, você poderá criar uma **tolerância** para essas taints. ["Em AgentConfiguration"](#) Se você tiver aplicado taints personalizados a todos os nós do cluster, também será necessário adicionar as tolerâncias necessárias à implantação do operador para permitir que o pod do operador seja agendado e executado.

Saiba mais sobre o Kubernetes ["Taints e Tolerations"](#).

Volte ao ["Página de Instalação do Operador de Monitoramento do Kubernetes do NetApp"](#)

Uma Nota sobre Segredos

Para remover a permissão do Operador de Monitoramento do Kubernetes para exibir segredos em todo o cluster, exclua os seguintes recursos do arquivo *operator-setup.yaml* antes de instalar:

```
ClusterRole/netapp-ci-<namespace>-agent-secret-clusterrole
ClusterRoleBinding/netapp-ci-<namespace>-agent-secret-clusterrolebinding
```

Se for uma atualização, exclua também os recursos do cluster:

```
kubectl delete ClusterRole/netapp-ci-<namespace>-agent-secret-clusterrole
kubectl delete ClusterRoleBinding/netapp-ci-<namespace>-agent-secret-clusterrolebinding
```

Se a análise de mudança estiver ativada, modifique o *AgentConfiguration* ou *operator-config.yaml* para descomentar a seção de gerenciamento de alterações e inclua *kindsToIgnoreFromWatch: "segredos"* na seção Gerenciamento de alterações. Observe a presença e a posição de aspas simples e duplas nesta linha.

```
# 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"
...
```

Verificando assinaturas de imagem do Operador de Monitoramento do Kubernetes

A imagem para o operador e todas as imagens relacionadas que ele implanta são assinadas pelo NetApp. Você pode verificar manualmente as imagens antes da instalação usando a ferramenta de cografia ou configurar um controlador de admissão do Kubernetes. Para obter mais detalhes, consulte ["Documentação do Kubernetes"](#).

A chave pública usada para verificar as assinaturas de imagem está disponível no bloco de instalação do Operador de Monitoramento em *Opcional: Carregue as imagens do operador para o seu repositório privado* >

chave Pública de assinatura de imagem

Para verificar manualmente uma assinatura de imagem, execute as seguintes etapas:

1. Copie e execute o snippet de recebimento de imagem
2. Copie e insira a senha do repositório quando solicitado
3. Armazenar a chave Pública de assinatura de imagem (dii-image-signing.pub no exemplo)
4. Verifique as imagens usando o cosign. Consulte o exemplo a seguir de uso de 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}]
```

Solução de problemas

Algumas coisas para tentar se você encontrar problemas para configurar o operador de monitoramento do Kubernetes:

Problema:	Tente isto:
Não vejo um hiperlink/conexão entre o meu volume persistente do Kubernetes e o dispositivo de armazenamento de back-end correspondente. Meu volume persistente do Kubernetes é configurado usando o nome de host do servidor de armazenamento.	Siga as etapas para desinstalar o agente Telegraf existente e reinstalar o agente Telegraf mais recente. Você precisa estar usando o Telegraf versão 2,0 ou posterior, e o storage de cluster do Kubernetes precisa ser monitorado ativamente pelo Data Infrastructure Insights.
Estou vendo mensagens nos logs que se assemelham ao seguinte: E0901 15 352:21 v1:39,962145 1 k8s reflector.go:178] k8s.io/kube-State-metrics/internal/store/builder.go:352: Falha ao listar *v1.MutatingWebhookConfiguration: O servidor não conseguiu encontrar o recurso solicitado E0901 15:k8s:43,168161 1 reflector.go:178] 21.io/kube-State-State-lease	Essas mensagens podem ocorrer se você estiver executando o kube-State-metrics versão 2.0.0 ou superior com versões do Kubernetes abaixo de 1,20. Para obter a versão do Kubernetes: <i>Kubectl version</i> para obter a versão do kube-State-metrics: <i>Kubectl get deploy/kube-State-metrics -o jsonpath leases'</i> para evitar que essas mensagens aconteçam, os usuários podem modificar sua implantação do kube-State-metrics para desativar os seguintes: <i>Mutatinghookhooks</i>

Problema:	Tente isto:
<p>Vejo mensagens de erro do Telegraf semelhantes às seguintes, mas o Telegraf inicia e executa: Oct 11 14:23:41 ip-172-31-39-47 systemd[1]: Iniciou o agente de servidor orientado a plug-in para relatar métricas no InfluxDB. Oct 11 14:23:41 ip-172-31-39-47 telegraf[1827]: Tempo 2021-10-11T14:23:41Z" não foi possível criar o diretório de cache. /Etc/telegraf/.cache/floco de neve, err: Mkdir /etc/telegraf/.CA che: Permissão negada. Ignorado. Func"gostonflake.(*defaultLogger).Errorf" file "log.go:120" Oct:10 ip-23-41Z-39-47 telegraf[1827]: 2021" 31"erro de 11 14:23:41:172". Abra /etc/telegraf/.cache/floco de neve/ocsp_response_cache.json: nenhum arquivo ou diretório desse tipo de arquivo ou diretório.(*defaultLogger).Errorf" arquivo "log.go:120 23" Oct 2021 41Z:10 ip-172-31-39-47 telegraf[1827]: 11 14-23:41 A iniciar o Telegraf 1.19.3</p>	<p>Este é um problema conhecido. "Este artigo do GitHub"Consulte para obter mais detalhes. Enquanto o Telegraf estiver ativo e em execução, os usuários podem ignorar essas mensagens de erro.</p>
<p>No Kubernetes, meu(s) pod(s) Telegraf está relatando o seguinte erro: "Erro no processamento de informações de mountstats: Failed to open mountstats file: /Hostfs/proc/1/mountstats, error: Open /hostfs/proc/1/mountstats: Permission denied"</p>	<p>Se o SELinux estiver habilitado e aplicando, provavelmente impedirá que o(s) pod(s) Telegraf acesse o arquivo /proc/1/mountstats no nó Kubernetes. Para superar essa restrição, edite a configuração do agentConfiguration e ative a configuração RUNGED Privileged. Para obter mais detalhes, consulte "Instruções do OpenShift" .</p>
<p>No Kubernetes, meu pod Telegraf ReplicaSet está relatando o seguinte erro: [inputs.prometheus] erro no plugin: Não foi possível carregar o par de chaves /etc/kupere/pki/etcd/Server.crt:/etc/kuGES/pki/etcd/Server.key: Open /etc/kuurge/pki/etcd/Server.crt: nenhum arquivo ou diretório</p>	<p>O pod Telegraf ReplicaSet destina-se a ser executado em um nó designado como mestre ou para o etcd. Se o pod ReplicaSet não estiver sendo executado em um desses nós, você receberá esses erros. Verifique se seus nós master/etcd têm manchetes neles. Se o fizerem, adicione as tolerâncias necessárias ao Telegraf ReplicaSet, telegraf-rs. Por exemplo, edite o ReplicaSet... kubectl edite rs telegraf-RS ...e adicione as tolerâncias apropriadas à especificação. Em seguida, reinicie o pod ReplicaSet.</p>
<p>Tenho um ambiente PSP/PSA. Isso afeta meu operador de monitoramento?</p>	<p>Se o seu cluster Kubernetes estiver em execução com a Política de Segurança do Pod (PSP) ou a admissão de Segurança do Pod (PSA), você deverá fazer o upgrade para o Operador de Monitoramento do Kubernetes mais recente. Siga estes passos para atualizar para o Operador atual com suporte para PSP/PSA: 1. Desinstalar o operador de monitoramento anterior: kubectl delete 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-rolebinding cluster-rolebinding.-rolebinding 2. Instale a versão mais recente do operador de monitorização.</p>

Problema:	Tente isto:
<p>Deparei-me com problemas ao tentar implementar o Operador e tenho PSP/PSA em utilização.</p>	<p>1. Edite o agente usando o seguinte comando: <code>Kubectl -n <name-space> edit Agent</code> 2. Marque "Segurança-política-ativada" como "falsa". Isso desativará as políticas de Segurança do Pod e a admissão de Segurança do Pod e permitirá que o Operador implante. Confirme usando os seguintes comandos: <code>Kubectl Get PSP</code> (deve mostrar a Política de Segurança Pod removida) <code>kubectl get all -n <namespace></code></p>
<p><code>grep -i psp</code> (deve mostrar que nada é encontrado)</p>	<p>Erros "ImagePullBackoff" vistos</p>
<p>Esses erros podem ser vistos se você tiver um repositório docker personalizado ou privado e ainda não tiver configurado o Operador de Monitoramento do Kubernetes para reconhecê-lo adequadamente. Leia mais sobre a configuração para repositório personalizado/privado.</p>	<p>Estou tendo um problema com a implantação do meu operador de monitoramento e a documentação atual não me ajuda a resolvê-lo.</p>
<p>Capture ou anote a saída dos comandos a seguir e entre em Contato com a equipe de suporte técnico.</p> <pre data-bbox="136 865 802 1325"> 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 </pre>	<p>Os pods NET-Observer (Workload Map) no namespace Operator estão em CrashLoopBackOff</p>
<p>Esses pods correspondem ao coletor de dados do mapa de workload para observabilidade de rede. Tente estes:</p> <ul style="list-style-type: none"> • Verifique os logs de um dos pods para confirmar a versão mínima do kernel. Por exemplo: <code>---- [ci-tenant-id]:"your-tenant-id", "Collector-cluster": "your-k8s-cluster-name", "ambiente": "prod", "nível": "erro", "msg": "falhou na validação. Razão: A versão 3.10.0 do kernel é menor que a versão mínima do kernel de 4.18.0", "Time": "2022-11-09T08:23:08Z" ----</code> • os pods do Net-Observer requerem que a versão do kernel do Linux seja pelo menos 4.18.0. Verifique a versão do kernel usando o comando <code>"uname -r"</code> e certifique-se de que eles são <code>> 4.18.0</code> 	<p>Os pods estão em execução no namespace do operador (padrão: Monitoramento NetApp), mas nenhum dado é exibido na IU para mapa de workload ou métricas do Kubernetes em consultas</p>

Problema:	Tente isto:
<p>Verifique a configuração de hora nos nós do cluster K8S. Para uma auditoria precisa e relatórios de dados, é altamente recomendável sincronizar a hora na máquina do agente usando o Network Time Protocol (NTP) ou o Simple Network Time Protocol (SNTP).</p>	<p>Alguns dos pods net-observer no namespace Operador estão no estado pendente</p>
<p>NET-Observer é um DaemonSet e executa um pod em cada nó do cluster k8s. • Observe o pod que está no estado pendente e verifique se ele está enfrentando um problema de recurso para CPU ou memória. Certifique-se de que a memória e a CPU necessárias estão disponíveis no nó.</p>	<p>Estou vendo o seguinte em meus logs imediatamente após instalar o Operador de Monitoramento do Kubernetes: [inputs.prometheus] erro no plugin: Erro ao fazer solicitação HTTP para <a href="http://kube-state-metrics.<namespace>.svc.cluster.local:8080/metrics">http://kube-state-metrics.<namespace>.svc.cluster.local:8080/metrics: Get <a href="http://kube-state-metrics.<namespace>.svc.cluster.local:8080/metrics">http://kube-state-metrics.<namespace>.svc.cluster.local:8080/metrics: Dial tcp: Lookup kube-State-metrics.<namespace>.svc.cluster.local: nenhum host</p>
<p>Normalmente, essa mensagem só é vista quando um novo operador é instalado e o pod <i>telegraf-rs</i> está ativo antes do pod <i>ksm</i> estar ativo. Essas mensagens devem parar quando todos os pods estiverem em execução.</p>	<p>Não vejo nenhuma métrica sendo coletada para os CronJobs do Kubernetes que existem no meu cluster.</p>
<p>Verifique a versão do Kubernetes (isto é <code>kubectl version, </code>). Se for v1,20.x ou inferior, esta é uma limitação esperada. A versão kube-State-metrics implantada com o Operador de Monitoramento do Kubernetes suporta apenas v1.CronJob. Com o Kubernetes 1,20.x e abaixo, o recurso CronJob está em v1beta.CronJob. Como resultado, as métricas de estado do kube não conseguem encontrar o recurso CronJob.</p>	<p>Depois de instalar o operador, os pods telegraf-ds entram em CrashLoopBackOff e os logs do pod indicam "su: Authentication failure".</p>
<p>Edite a seção telegraf em <i>AgentConfiguration</i> e defina <i>dockerMetricCollectionEnabled</i> como false. Para obter mais detalhes, consulte o "opções de configuração". ... spec: ... telegraf: ... - Name: docker run-mode : - DaemonSet substituições: - Chave: DOCKER_UNIX_SOCKET_PLACEHOLDER valor: unix:///run/docker.sock</p>	<p>Vejo mensagens de erro repetitivas semelhantes às seguintes nos meus logs do Telegraf: E! [Agent] erro ao gravar em outputs.http: Post "/https://<tenant_url>/rest/v1/Lake/ingest/influxdb": Prazo de contexto excedido (Client.Timeout excedido enquanto aguarda cabeçalhos)</p>
<p>Edite a seção telegraf em <i>AgentConfiguration</i> e aumente <i>outputTimeout</i> para 10s. Para obter mais detalhes, consulte o "opções de configuração".</p>	<p>Estou faltando dados <i>involvedobject</i> para alguns Registros de eventos.</p>
<p>Certifique-se de que seguiu os passos indicados na "Permissões" seção acima.</p>	<p>Por que estou vendo dois pods de operador de monitoramento em execução, um chamado NetApp-CI-monitoring-operator-<pod> e o outro chamado Monitoring-operator-<pod>?</p>

Problema:	Tente isto:
<p>A partir de 12 de outubro de 2023, o Data Infrastructure Insights refatorou a operadora para melhor atender nossos usuários; para que essas alterações sejam totalmente adotadas, você retire o operador antigo deve e instale o novo.</p>	<p>Os eventos do meu kubernetes pararam inesperadamente de reportar ao Data Infrastructure Insights.</p>
<p>Recuperar o nome do pod de exportador de eventos:</p> <pre>kubectl -n netapp-monitoring get pods</pre>	<p>grep event-exporter</p>
<pre>awk '{print \$1}'</pre>	<pre>sed 's/event-exporter./event-exporter/'</pre> <p>Deve ser "NetApp-CI-event-exporter" ou "event-exporter". Em seguida, edite o agente de monitoramento <code>kubectl -n netapp-monitoring edit agent</code> e defina o valor para <code>LOG_FILE</code> para refletir o nome do pod de exportador de eventos apropriado encontrado na etapa anterior. Mais especificamente, <code>LOG_FILE</code> deve ser definido como <code>"/var/log/containers/NetApp-CI-event-exporters.log"</code> ou <code>"/var/log/containers/event-exporters*.log"</code></p> <pre>.... fluent-bit: ... - name: event-exporter-ci substitutions: - key: LOG_FILE values: - /var/log/containers/netapp-ci-event-exporter*.log</pre> <p>Alternativamente, pode-se desinstalar também e reinstalar o agente.</p>
<p>Estou vendo POD(s) implantado(s) pelo Operador de Monitoramento do Kubernetes travarem devido a recursos insuficientes.</p>	<p>Consulte o Operador de Monitoramento do Kubernetes "opções de configuração" para aumentar os limites de CPU e/ou memória conforme necessário.</p>
<p>Uma imagem ausente ou uma configuração inválida fez com que os pods de métricas de estado do NetApp-ci-kube falhassem na inicialização ou se preparassem. Agora o StatefulSet está preso e as alterações de configuração não estão sendo aplicadas aos pods NetApp-CI-kube-State-metrics.</p>	<p>O StatefulSet está em um "quebrado" estado. Depois de corrigir quaisquer problemas de configuração, salte os pods NetApp-CI-kube-State-metrics.</p>
<p>Os pods de métricas de estado do NetApp-ci-kube falham ao iniciar depois de executar uma atualização do Operador do Kubernetes, lançando o ErrImagePull (falha ao puxar a imagem).</p>	<p>Tente redefinir os pods manualmente.</p>

Problema:	Tente isto:
<p>"Evento descartado como sendo mais antigo do que maxEventAgeSeconds" mensagens estão sendo observadas para o meu cluster Kubernetes em Log Analysis.</p>	<p>Modifique o Operador <i>agentConfiguration</i> e aumente o <i>event-exporter-maxEventAgeds</i> (ou seja, para 60s), <i>event-exporter-kubeQPS</i> (ou seja, para 100) e <i>event-exporter-kubeBurst</i> (ou seja, para 500). Para obter mais detalhes sobre essas opções de configuração, consulte a "opções de configuração" página.</p>
<p>Telegraf avisa ou trava por causa de memória bloqueável insuficiente.</p>	<p>Tente aumentar o limite de memória bloqueável para o Telegraf no sistema operacional/nó subjacente. Se aumentar o limite não for uma opção, modifique a configuração do agente NKMO e defina <i>desprotegido</i> como <i>true</i>. Isto instruirá o Telegraf a não tentar reservar páginas de memória bloqueadas. Embora isso possa representar um risco de segurança, pois segredos descryptografados podem ser trocados para o disco, ele permite a execução em ambientes onde não é possível reservar memória bloqueada. Para obter mais detalhes sobre as opções de configuração <i>desprotegidas</i>, consulte a "opções de configuração" página.</p>
<p>Vejo mensagens de aviso do Telegraf que se assemelham às seguintes: <i>W! [Inputs.diskio] não é possível reunir o nome do disco para "vdc": Erro ao ler /dev/vdc: nenhum arquivo ou diretório</i></p>	<p>Para o Operador de Monitoramento do Kubernetes, essa mensagem de aviso é benigna e pode ser ignorada com segurança. Alternativamente, edite a seção telegraf em <i>AgentConfiguration</i> e defina <i>runDsPrivileged</i> como <i>true</i>. Para obter mais detalhes, consulte "opções de configuração do operador" a .</p>

Problema:	Tente isto:
<p>Meu pod fluent-bit está falhando com os seguintes erros: [2024 10/16 14/10/16 14 16:16 2024 23:23] [error] [/src/fluent-bit/plugins/in_tail/tail_fs_inotify.c:360 errno.24] muitos arquivos abertos [2024/10/16 14:16:23] [error] falha na inicialização tail,0 [Engine] [input]</p>	<p>Tente alterar suas configurações <i>fsnotify</i> no cluster:</p> <pre data-bbox="824 226 1477 919"> 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> </pre> <p>Reinicie o Fluent-bit.</p> <p>Observação: Para tornar essas configurações persistentes entre as reinicializações do nó, você precisa colocar as seguintes linhas em <i>/etc/sysctl.conf</i></p> <pre data-bbox="824 1192 1477 1444"> fs.inotify.max_user_instances=<something larger than current setting> fs.inotify.max_user_watches=<something larger than current setting> </pre>

Informações adicionais podem ser encontradas na ["Suporte"](#) página ou no ["Matriz de suporte do Data Collector"](#).

Opções de configuração do operador de monitoramento Kubernetes

A ["Operador de monitoramento do Kubernetes"](#) configuração pode ser personalizada.

A tabela abaixo lista as opções possíveis para o arquivo *AgentConfiguration*:

Componente	Opção	Descrição
agente		Opções de configuração comuns a todos os componentes que o operador pode instalar. Estes podem ser considerados como opções "globais".
	DockerRepo	Uma substituição dockerRepo para extrair imagens de repositórios docker privados de clientes em comparação com o repositório docker Data Infrastructure Insights. O padrão é repositório docker do Data Infrastructure Insights
	DockerImagePullSecret	Opcional: Um segredo para o repositório privado dos clientes
	Nome exclusivo	Campo de texto livre que identifica exclusivamente um cluster em todos os clusters de clientes. Isso deve ser exclusivo para um locatário do Data Infrastructure Insights. O padrão é o que o cliente insere na IU para o campo "Nome do cluster"
	Proxy Format: Proxy: Server: Port: Username: Password: NoProxy: IsTelegrafProxyEnabled: IsAuProxyEnabled: IsFluentbitProxyEnabled: IsCollectorProxyEnabled:	Opcional para definir proxy. Este é geralmente o proxy corporativo do cliente.
telegraf		Opções de configuração que podem personalizar a instalação do telegraf do Operador
	ColeçãoInterval	Intervalo de coleta de métricas, em segundos (máx. 60s)
	DsCpuLimit	Limite de CPU para telegraf ds
	DsMemLimit	Limite de memória para telegraf ds
	DsCpuRequest	Pedido de CPU para telegraf ds
	DsMemRequest	Pedido de memória para telegraf ds
	RsCpuLimit	Limite de CPU para telegraf rs
	RsMemLimit	Limite de memória para telegraf rs
	RsCpuRequest	Pedido de CPU para telegraf rs
	RsMemRequest	Pedido de memória para telegraf rs
	Privilégios em execução	Execute o recipiente <i>telegraf-monstats-poller</i> do DaemonSet no modo privilegiado. Defina isso como verdadeiro se o SELinux estiver habilitado em seus nós do Kubernetes.
	RunDsPrivileged	Defina runDsPrivileged como true para executar o contentor telegraf DaemonSet no modo privilegiado.
	BatchSize	Consulte " Documentação de configuração do Telegraf "

Componente	Opção	Descrição
	BufferLimit	Consulte " Documentação de configuração do Telegraf "
	RoundInterval	Consulte " Documentação de configuração do Telegraf "
	ColeçãoJitter	Consulte " Documentação de configuração do Telegraf "
	precisão	Consulte " Documentação de configuração do Telegraf "
	FlushInterval	Consulte " Documentação de configuração do Telegraf "
	FlushJitter	Consulte " Documentação de configuração do Telegraf "
	OutputTimeout (tempo limite de saída)	Consulte " Documentação de configuração do Telegraf "
	DsTolerations	tolerâncias adicionais do telegraf-ds.
	RsTolerations	tolerâncias adicionais telegraf-rs.
	SkipProcessorsAfterAgregadores	Consulte " Documentação de configuração do Telegraf "
	não protegido	Consulte este " Problema de Telegraf conhecido ". A configuração <i>desprotegido</i> instruirá o Operador de Monitoramento do Kubernetes a executar o Telegraf com o <code>--unprotected</code> sinalizador.
kube-state-metrics		Opções de configuração que podem personalizar a instalação de métricas de estado kube do Operador
	CpuLimit	Limite de CPU para implantação de métricas de estado do kube
	MemLimit	Limite de MEM para implantação de métricas de estado do kube
	CpuRequest	Solicitação de CPU para implantação de métricas de estado do kube
	MemRequest	Solicitação de MEM para implantação de métricas de estado do kube
	recursos	uma lista separada por vírgulas de recursos a serem capturados. exemplo: cronjobs,daemonsets,deployments,ingresses,jobs,na mespaces,nodos,persistentvolumeclaims,persistentvolumes,pods,replicaset,resourcequotas,se rviços,statfulsets
	tolerâncias	tolerações adicionais de métricas de estado do kube.
	etiquetas	uma lista separada por vírgulas de recursos que kube-state-metrics deve capturar

Componente	Opção	Descrição
registos		Opções de configuração que podem personalizar a coleta de logs e a instalação do Operador
	ReadFromHead	verdadeiro/falso, deve o bit fluente ler o log da cabeça
	tempo limite	tempo limite, em segundos
	Modo dnsMode	TCP/UDP, modo para DNS
	tolerações de bits fluentes	tolerações adicionais fluent-bit-ds.
	tolerância de evento-exportador	tolerância adicional ao exportador de eventos.
	Evento-exportador-maxEventAgeSeconds	idade máxima do evento exportador de eventos. Consulte https://github.com/jkroepke/resmoio-kubernetes-event-exporter
mapa de workload		Opções de configuração que podem personalizar a coleta e instalação do mapa de carga de trabalho do Operador.
	CpuLimit	Limite de CPU para NET Observer ds
	MemLimit	limite mem para o observador líquido ds
	CpuRequest	Pedido de CPU para NET Observer ds
	MemRequest	pedido de mem para net observer ds
	MetricAggregationInterval	intervalo de agregação métrica, em segundos
	BpfPollInterval	Intervalo de enquete BPF, em segundos
	EnableDNSLookup	Verdadeiro/falso, ative a pesquisa de DNS
	I4-tolerâncias	net-observer-I4-ds tolerâncias adicionais.
	Privilégios em execução	True/FALSE - defina Privileged como true se o SELinux estiver habilitado em seus nós do Kubernetes.
gerenciamento de alterações		Opções de configuração para o Gerenciamento e análise de alterações do Kubernetes
	CpuLimit	Limite de CPU para change-observer-Watch-rs
	MemLimit	Limite MEM para mudança-observador-server-rs
	CpuRequest	Pedido de CPU para change-observer-Watch-rs
	MemRequest	pedido de mem para mudança-observador-watch-rs
	FailureDeclaraçãoInterval Mins	Intervalo em minutos após o qual uma implantação não-bem-sucedida de uma carga de trabalho será marcada como falhou
	DeployAggrIntervalSeconds	Frequência na qual os eventos em andamento de implantação da carga de trabalho são enviados
	NonWorkloadAggrIntervalSeconds	Frequência na qual implantações que não são de carga de trabalho são combinadas e enviadas

Componente	Opção	Descrição
	TermsToRedact	Um conjunto de expressões regulares usadas em nomes env e mapas de dados cujo valor será editado termos de exemplo:"pwd", "password", "token", "apikey", "api-key", "jwt"
	AdicionalKindsToWatch	Uma lista separada por vírgulas de tipos adicionais para assistir do conjunto padrão de tipos observados pelo coletor
	KindsToIgnoreFromWatch	Uma lista separada por vírgulas de tipos a ignorar da observação do conjunto padrão de tipos observados pelo coletor
	LogRecordAggrIntervalSecs	Frequência com a qual os Registros de log são enviados para IC do coletor
	tolerâncias de relógio	tolerâncias adicionais do change-observer-watch-ds. Apenas formato de linha única abreviada. Exemplo: Tecla: taint1, operador: Existe, efeito: NoSchedule, tecla: taint2, operador: Existe, efeito: NoExecute'

Exemplo de arquivo AgentConfiguration

Abaixo está um exemplo de arquivo *AgentConfiguration*.

```

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/manager-
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,persistent
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'

# # 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 in minutes after which a non-successful deployment of a
workload will be marked as failed
# failureDeclarationIntervalMins: '30'

# # Frequency at which workload deployment in-progress events are sent
# deployAggrIntervalSeconds: '300'

# # Frequency at which non-workload deployments are combined and sent
# nonWorkloadAggrIntervalSeconds: '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: ''

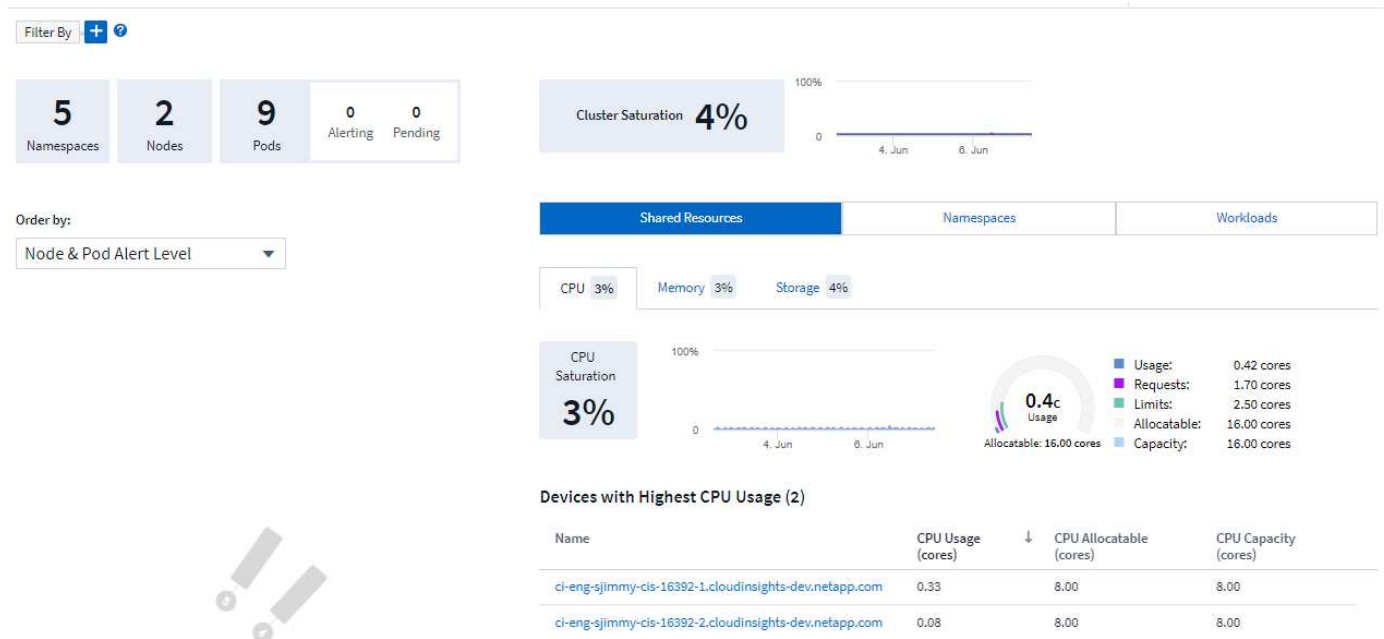
# # Frequency with which log records are sent to CI from the collector
# logRecordAggrIntervalSeconds: '20'

# # 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: ''

```

Página de detalhes do cluster do Kubernetes

A página de detalhes do cluster do Kubernetes exibe uma visão geral detalhada do cluster do Kubernetes.



Contagens de namespace, nó e Pod

As contagens na parte superior da página mostram o número total de namespaces, nós e pods no cluster, bem como o número de pods que estão atualmente alertando e pendentes.

Recursos compartilhados e saturação

No canto superior direito da página de detalhes está a saturação do cluster como uma porcentagem atual,

bem como um gráfico mostrando a tendência recente ao longo do tempo. A saturação de cluster é a mais alta da CPU, memória ou saturação de armazenamento em cada ponto do tempo.

Abaixo disso, a página mostra por padrão o uso de **recursos compartilhados**, com guias para CPU, memória e armazenamento. Cada guia mostra a porcentagem de saturação e a tendência ao longo do tempo, com detalhes de uso adicionais. Para armazenamento, o valor mostrado é o maior da saturação de backend e sistema de arquivos, que são calculados independentemente.

Os dispositivos com a maior utilização são apresentados numa tabela na parte inferior. Clique em qualquer link para explorar esses dispositivos.

Namespaces

A guia namespaces exibe uma lista de todos os namespaces em seu ambiente Kubernetes, mostrando o uso de CPU e memória, bem como uma contagem de cargas de trabalho em cada namespace. Clique nos links Nome para explorar cada namespace.

Shared Resources	Namespaces	Workloads	
Namespaces (5)			
Name ↓	CPU Usage (cores)	Memory Usage (GiB)	Workload Count
netapp-monitoring	0.25	0.38	4
kube-system	0.01	0.03	3
kube-public	0.00	0.00	0
kube-node-lease	0.00	0.00	0
default	0.00	<0.01	1

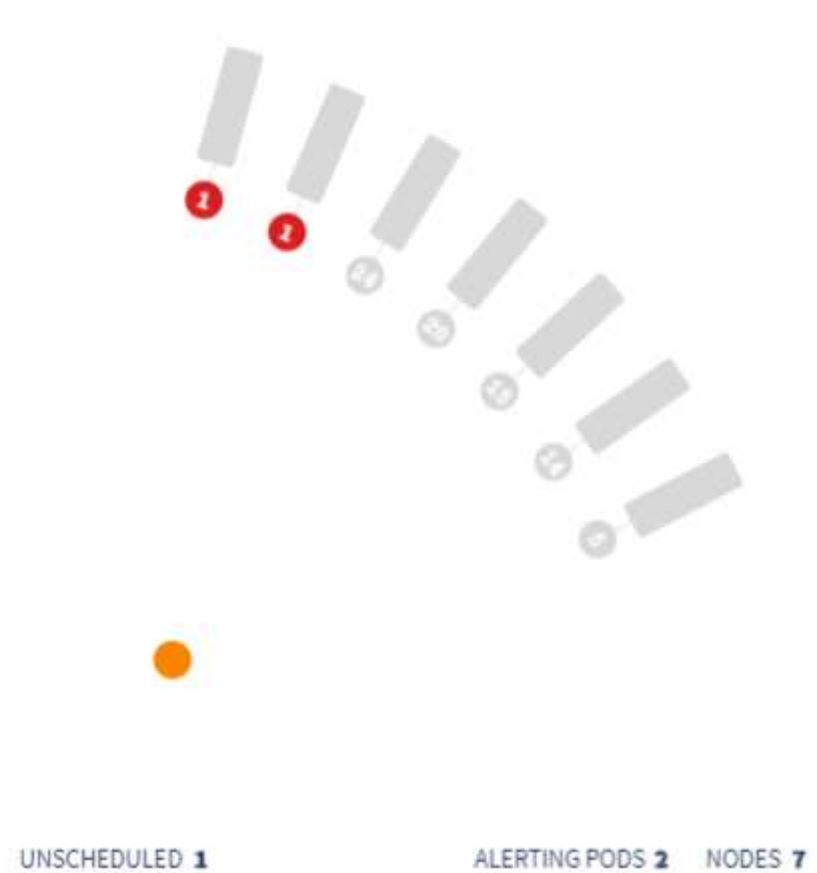
Workloads

Da mesma forma, a guia cargas de trabalho exibe uma lista das cargas de trabalho em cada namespace, mostrando novamente o uso da CPU e da memória. Clicar nos links de namespace faz drill em cada um.

Workloads (8)

Name ↓	CPU Usage (cores)	Memory Usage (GiB)	Namespace
telegraf-rs-lf9gg	0.24	0.24	netapp-monitoring
telegraf-ds-k957c	0.01	0.10	netapp-monitoring
nginx	0.00	<0.01	default
monitoring-operator-6fcf4755ff-p2cs6	<0.01	0.02	netapp-monitoring
metrics-server-7b4f8b595-f7j9f	<0.01	0.01	kube-system
local-path-provisioner-64d457c485-289gx	<0.01	0.01	kube-system
kube-state-metrics-7995866f8c-t8c49	<0.01	0.01	netapp-monitoring
coredns-5d69dc75db-nkw5p	<0.01	0.01	kube-system

A "roda" do grupo



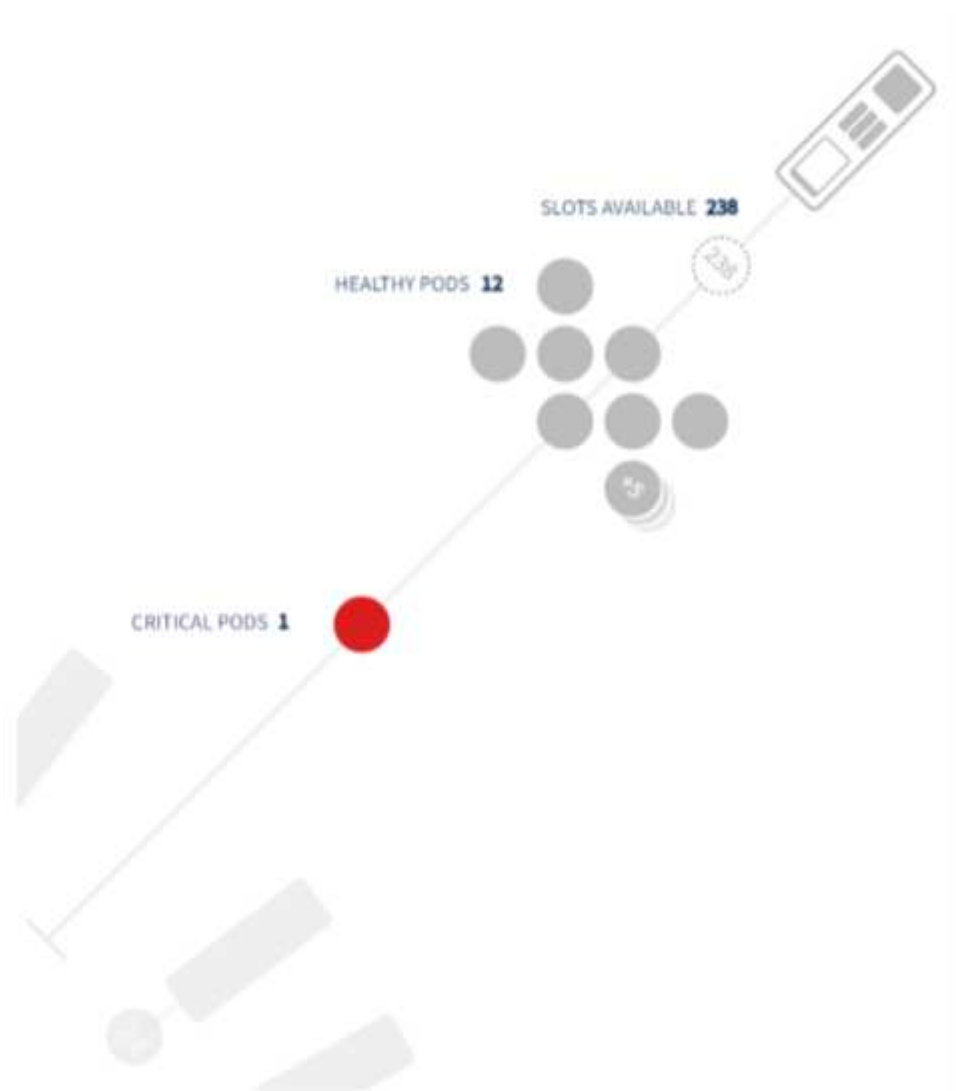
A seção "roda" do cluster fornece o estado do nó e do pod em um relance, que você pode detalhar para obter mais informações. Se o cluster contiver mais nós do que podem ser exibidos nesta área da página, você poderá girar a roda usando os botões disponíveis.

Os pods ou nós de alerta são exibidos em vermelho. As áreas de "aviso" são apresentadas a laranja. Os pods não programados (ou seja, não anexados) serão exibidos no canto inferior da "roda" do cluster.

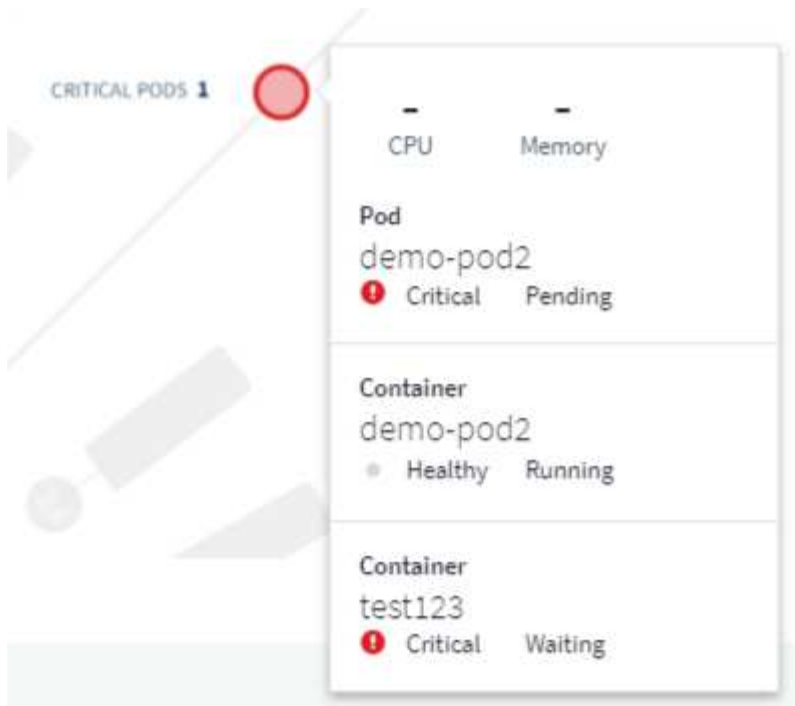
Passar o Mouse sobre um pod (círculo) ou Node (barra) estenderá a visão do nó.



Clicar no pod ou nó nessa exibição aumentará o zoom para a exibição nó expandido.



A partir daqui, você pode passar o Mouse sobre um elemento para exibir detalhes sobre esse elemento. Por exemplo, passar o Mouse sobre o pod crítico neste exemplo exibe detalhes sobre esse pod.



Você pode visualizar informações de sistema de arquivos, memória e CPU passando o Mouse sobre os elementos Node.



Uma nota sobre os medidores

Os medidores de memória e CPU mostram três cores, uma vez que mostram *used* em relação à *capacidade_allocatable_* e *total Capacity*.

Monitoramento e mapa de desempenho de rede do Kubernetes


O recurso Kubernetes Network Performance Monitoring and Map simplifica a solução de problemas mapeando dependências entre serviços (também chamadas de cargas de trabalho) e oferece visibilidade em tempo real das latências de desempenho e anomalias de rede para identificar problemas de desempenho antes que eles afetem os usuários. Essa funcionalidade ajuda as organizações a reduzir os custos gerais analisando e auditando os fluxos de tráfego do Kubernetes.

Principais recursos:

- O mapa de carga de trabalho apresenta dependências e fluxos de carga de trabalho do Kubernetes e destaca problemas de rede e desempenho.
- Monitore o tráfego de rede entre pods, cargas de trabalho e nós do Kubernetes; identifique a origem dos problemas de latência e tráfego.
- Reduzir os custos gerais analisando o tráfego de rede de entrada, saída, cross-region e cross-zone.

Pré-requisitos

Para poder usar o monitoramento e o mapa de desempenho de rede do Kubernetes, você deve ter configurado o "[Operador de monitoramento do Kubernetes do NetApp](#)" para ativar essa opção. Durante a implementação do Operador, selecione a caixa de verificação "Network Performance and Map" (desempenho da rede e mapa) para ativar. Você também pode habilitar essa opção navegando para uma página inicial do Kubernetes e selecionando "Modificar implantação".

 **kubernetes**
Kubernetes

Configure Data Acquisition

Review Kubernetes cluster information and choose additional data to collect.

Cluster Information

Kubernetes Cluster stream8	Network Performance and Map Disabled	Events Log Disabled
-------------------------------	---	------------------------

Deployment Options

[Need Help?](#)

- Network Performance and Map
- Events Log

[Complete Setup](#)

Monitores

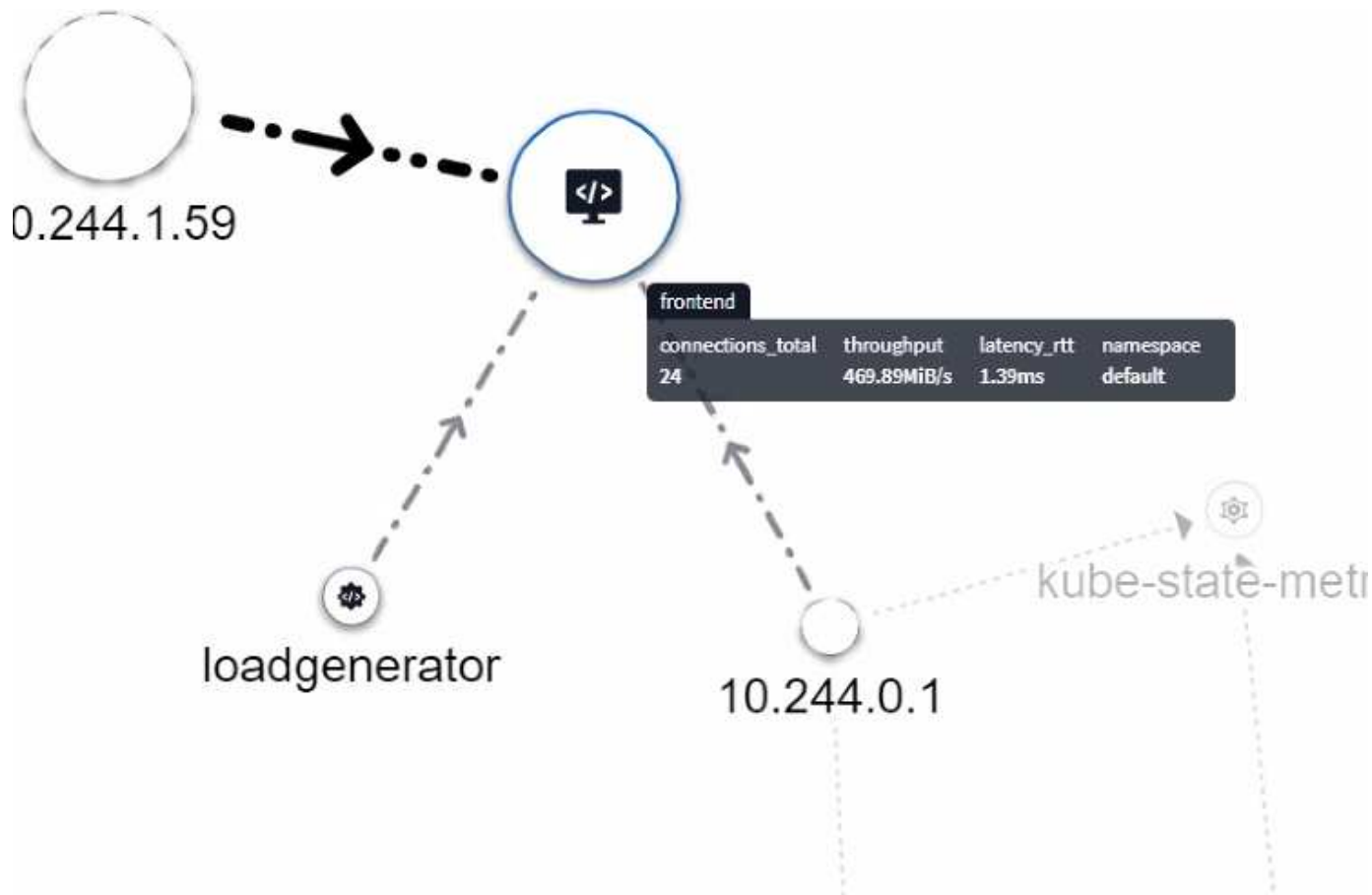
O mapa de carga de trabalho utiliza "monitores" para obter informações. O Data Infrastructure Insights fornece uma série de monitores padrão do Kubernetes (observe que eles podem ser *Pausado* por padrão. Você pode *Resume* (ou seja, ativar) os monitores que você deseja), ou você pode criar monitores personalizados para objetos kubernetes, que o mapa de carga de trabalho também usará.

Você pode criar alertas de métricas do Data Infrastructure Insights em qualquer um dos tipos de objeto abaixo. Certifique-se de que os dados estão agrupados pelo tipo de objeto padrão.

- kuseurea.workflow
- kuasse.daemonset
- kubernetes.deployment
- kuseurs.cronjob
- kuasse.job
- kuseixos.replicaset
- kuasse.statefulset
- kuasse.pod
- kubernetes.network_traffic_l4

O mapa

O mapa mostra os serviços/cargas de trabalho e seus relacionamentos entre si. Setas mostram direções de tráfego. Passar o Mouse sobre uma carga de trabalho exibe informações resumidas para essa carga de trabalho, como você pode ver neste exemplo:

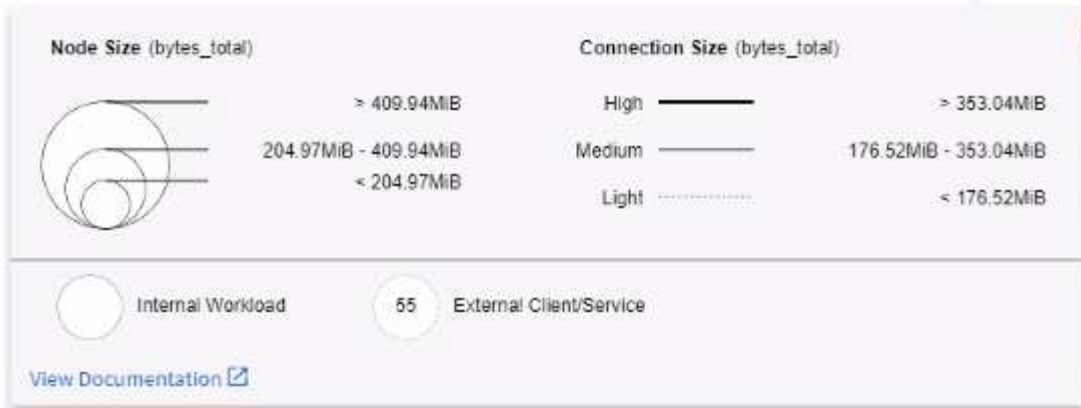


Os ícones dentro dos círculos representam diferentes tipos de serviço. Observe que os ícones só serão visíveis se os objetos subjacentes tiverem [etiquetas](#).



O tamanho de cada círculo indica o tamanho do nó. Observe que esses tamanhos são relativos, o nível de zoom do navegador ou o tamanho da tela podem afetar os tamanhos reais dos círculos. Da mesma forma, o estilo de linha de tráfego oferece uma visão rápida do tamanho da conexão; linhas sólidas arrojadas são tráfego alto, enquanto linhas pontilhadas de luz são tráfego mais baixo.

Os números dentro dos círculos são o número de conexões externas que estão sendo processadas pelo serviço.



Detalhes e alertas do workload

Os círculos exibidos em cores indicam um alerta de nível crítico ou de aviso para a carga de trabalho. Passe o Mouse sobre o círculo para obter um resumo do problema ou clique no círculo para abrir um painel de deslizamento com mais detalhes.

NetApp Cloud Insights | Tutorial 0% Complete | Getting Started

demo / Workload Map

Filter By: cluster All

Node Size: bytes_total | Connection Size: bytes_total

Showing 98 connections

External IP | point-of-sale | netapp-fitness-store-01-locust | coredns | frontend | payment | order | users | order-postgres | users-redis | users-mongo | cart

151.101.130.133 | 1.66.133 | 151.101.2.133 | 10.42.7.16 | 10.42.1.133 | 151.101.194.133

payment | Go to Asset Page | Last 7 Days

Summary 2 | Network 2 | Pods & Storage

Workload Details

Cluster: ci-demo-01 | Namespace: netapp-fitness-store-01 | Type: Deployment | Pods: 1/00

Labels: app: netapp-fitness, app.kubernetes.io/component: integration, app.kubernetes.io/managed-by: Helm, service: payment, version: 1.0.0

Alerts Detected (2)

Network - Warning 2

2 items found

alertid	triggeredTime	currentSeverity	monitor	triggeredOn	activeStatus
AL-683	5 days ago Apr 5, 2023 7:57 AM	Resolved	Workload Network Latency-RTT High (Outdated)	Src_Cluster: ci-demo-01 Src_Namespace: netapp-fitness-store-01 Src_Workload_Name: payment Src_Workload_Kind: Deployment	Resolved
AL-630	7 days ago Apr 3, 2023 10:26 AM	Resolved	Workload Network Latency-RTT High (Outdated)	Src_Cluster: ci-demo-01	Resolved

Network Traffic

All Traffic | Inbound | Outbound

Connections Total: 50k | Throughput: 0.07

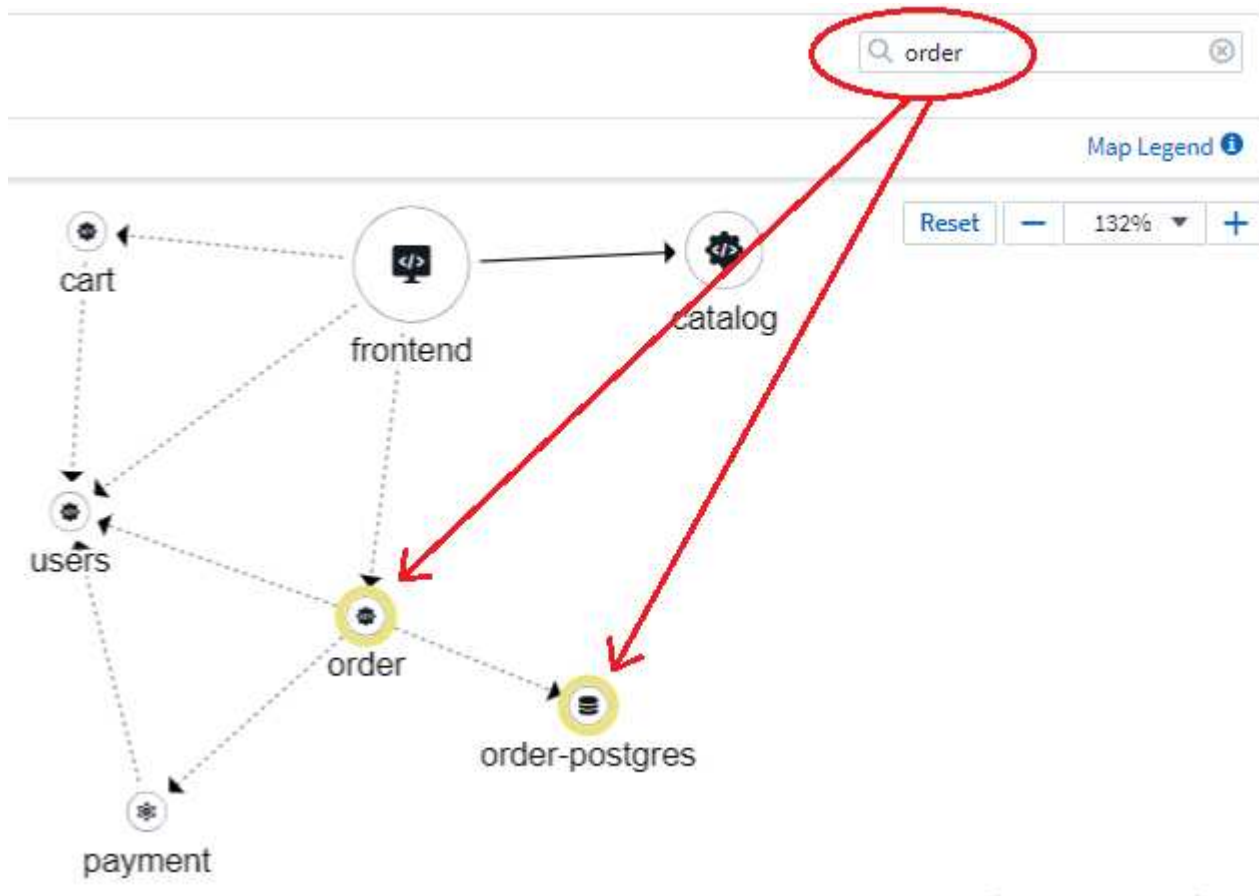
Encontrando e filtrando

Como acontece com outros recursos do Data Infrastructure Insights, você pode facilmente definir filtros para se concentrar nos objetos específicos ou atributos de carga de trabalho desejados.

Filter By: cluster All scope_cluster All

Node Size: bytes_total Connection Size: bytes_total

Da mesma forma, digitar uma string no campo *find* destacará as cargas de trabalho correspondentes.



Etiquetas de workload

As etiquetas de carga de trabalho são necessárias se pretender que o mapa identifique os tipos de cargas de trabalho apresentadas (ou seja, os ícones de círculo). As etiquetas são derivadas da seguinte forma:

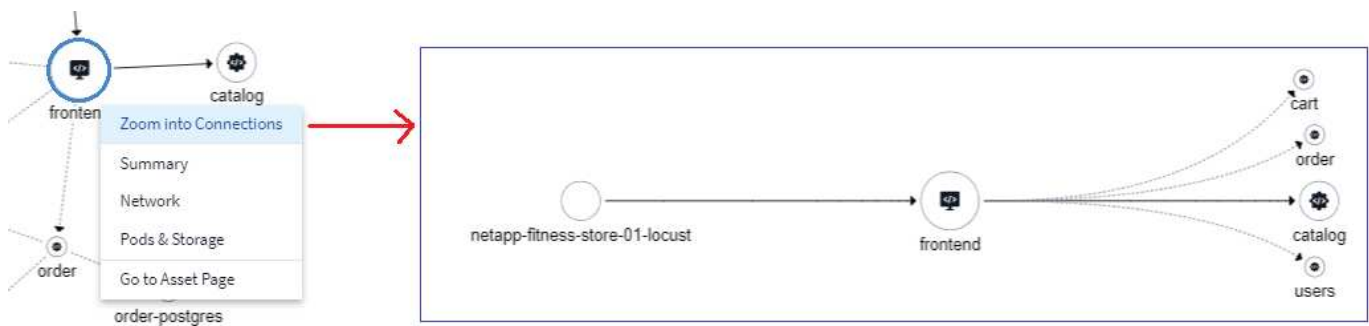
- Nome do serviço/aplicativo em execução em termos genéricos
- Se a fonte for um pod:
 - A etiqueta é derivada da etiqueta da carga de trabalho do pod
 - Etiqueta esperada na carga de trabalho: `App.kureau.io/component`
 - Referência do nome da etiqueta: <https://kubernetes.io/docs/concepts/overview/working-with-objects/common-labels/>
 - Etiquetas recomendadas:
 - frontend

- back-end
 - banco de dados
 - cache
 - fila de espera
 - kafka
- Se a fonte for externa ao cluster kubernetes:
 - O Data Infrastructure Insights tentará analisar o nome DNS resolvido para extrair o tipo de serviço.

Por exemplo, com um nome DNS resolvido de `s3.eu-north-1.amazonaws.com`, o nome resolvido é analisado para obter S3 como o tipo de serviço.

Mergulhe fundo

Clicar com o botão direito do Mouse em uma carga de trabalho apresenta opções adicionais para explorar ainda mais. Por exemplo, a partir daqui, você pode aumentar o zoom para ver as conexões para essa carga de trabalho.



Ou você pode abrir o painel deslizante de detalhes para visualizar diretamente a guia *Summary*, *Network* ou *Pod & Storage*.



Summary	Network	Pods & Storage
---------	----------------	----------------

Network Activities - Inbound (1) 

src_workload...	src_namespace	src_workload_...	throughpu... ↓	connections_t...	latency_rtt (ms)	tcp_retransmit...
netapp-fitness...	locust	Deployment	14,193,748.78	653.19	3.74	2,578.00

Network Activities - Outbound (4) 

dst_workloa...	dst_namespace	dst_workload_...	throughpu... ↓	connections_t...	latency_rtt (ms)	tcp_retransmit...
catalog	netapp-fitness-...	Deployment	14,166,417.02	2,425.07	149.37	13,850.00
cart	netapp-fitness-...	Deployment	12,479.90	638.97	65.10	0.00
order	netapp-fitness-...	Deployment	4,515.16	161.84	65.07	0.00

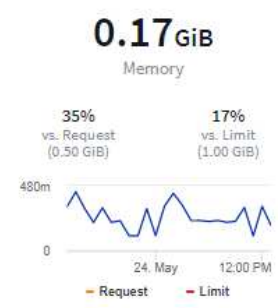
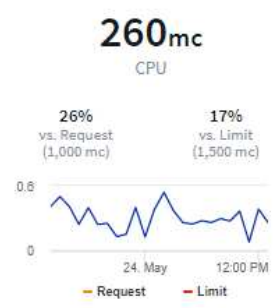
Finalmente, selecionar *Go to Asset Page* abrirá a página de destino detalhada do ativo para a carga de trabalho.

Filter By + ?

2/2
Pods: Current / Desired

2 Up-to-date 0 Unavailable

Namespace netapp-fitness-store-01	Type Deployment	Date Created Apr 11, 2023 11:34 AM
Labels -		



0.00GiB
Total PVC Capacity claimed

Highest CPU Demand by Pod

- 132.76m frontend-7...9f8f-284kb
- 127.55m frontend-7...9f8f-gd8mk

Highest Memory Demand by Pod

- 0.09 GiB frontend-7...9f8f-284kb
- 0.09 GiB frontend-7...9f8f-gd8mk

Pods (2)

Pod Name ↑	Status	Healthy Containers	cpu_usage_nanocores (mc)	memory_rss_bytes (GiB)
frontend-7fccd9f8f-284kb	● Healthy Running	1 of 1	133	0.09
frontend-7fccd9f8f-gd8mk	● Healthy Running	1 of 1	128	0.09

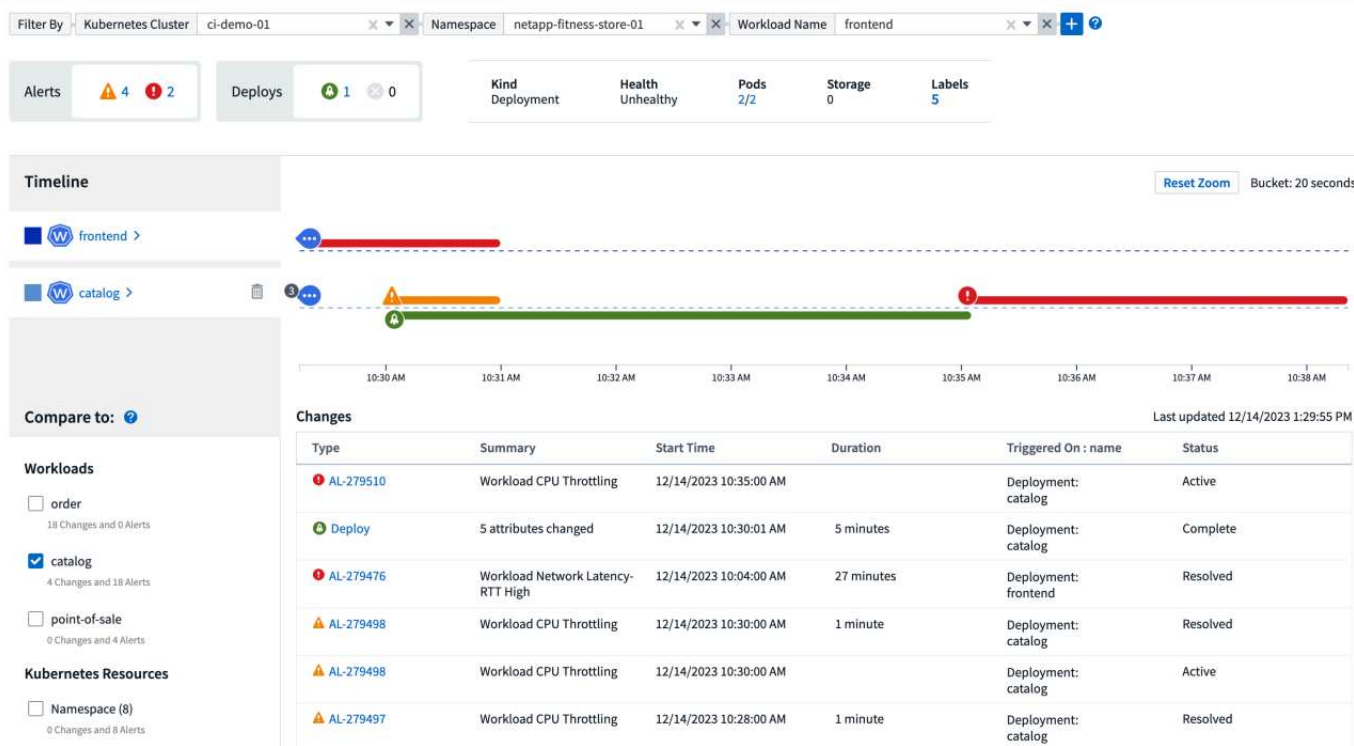
Kubernetes Change Analytics

O Kubernetes Change Analytics oferece uma visão completa das mudanças recentes no seu ambiente K8s. Alertas e status de implantação estão ao seu alcance. Com o Change Analytics, você pode controlar todas as alterações de implantação e configuração e correlacioná-las com a integridade e a performance dos serviços, da infraestrutura e dos clusters do K8s.

Como a análise de mudanças ajuda?

- Em ambientes Kubernetes de vários locatários, as interrupções podem ocorrer devido a alterações mal configuradas. O Change Analytics ajuda com isso, fornecendo um único painel para visualizar e correlacionar a integridade dos workloads e as alterações de configuração. Isso pode ajudar na solução de problemas de ambientes dinâmicos do Kubernetes.

Para exibir o Kubernetes Change Analytics, navegue até **Kubernetes > Change Analysis**.



A página é atualizada automaticamente com base no intervalo de tempo selecionado no momento. Intervalos de tempo menores significam uma atualização mais frequente do ecrã.

Filtragem

Assim como todos os recursos do Data Infrastructure Insights, filtrar a lista de alterações é intuitivo: Na parte superior da página, insira ou selecione valores para seu cluster, namespace ou workload do Kubernetes.

Ao filtrar para um cluster, namespace e workload específicos (juntamente com quaisquer outros filtros definidos), você verá uma linha do tempo das implantações e alertas para essa carga de trabalho nesse namespace no cluster. Aumente ainda mais o zoom clicando e arrastando no gráfico para focar em um intervalo de tempo mais específico.

Filter By: Kubernetes Cluster stream-54 | Namespace kube-system | Workload Name coredns

Alerts 0 8 | Deploys 0 0

Kind: Deployment | Health: Healthy | Pods: 1/1 | Storage: 0 | Labels: 3

Timeline Bucket: 6 minutes

coredns >

Compare to: ?

Changes Last updated 11/28/2023 3:17:05 PM

Type	Summary	Start Time	Duration	Triggered On : name	Status
AL-2982989	once Workload Down copy	11/28/2023 3:07:00 PM	1 minute	Deployment: coredns	Resolved
AL-2982989	once Workload Down copy	11/28/2023 3:07:00 PM		Deployment: coredns	Active
AL-2982887	once Workload Down copy	11/28/2023 3:01:00 PM	1 minute	Deployment: coredns	Resolved
AL-2982887	once Workload Down copy	11/28/2023 3:01:00 PM		Deployment: coredns	Active
AL-2982782	once Workload Down copy	11/28/2023 2:57:00 PM	0 milliseconds	Deployment: coredns	Resolved
AL-2982782	once Workload Down copy	11/28/2023 2:57:00 PM		Deployment: coredns	Active
AL-2982441	once Workload Down copy	11/28/2023 2:32:00 PM	1 minute	Deployment: coredns	Resolved
AL-2982441	once Workload Down copy	11/28/2023 2:32:00 PM		Deployment: coredns	Active

Estado rápido

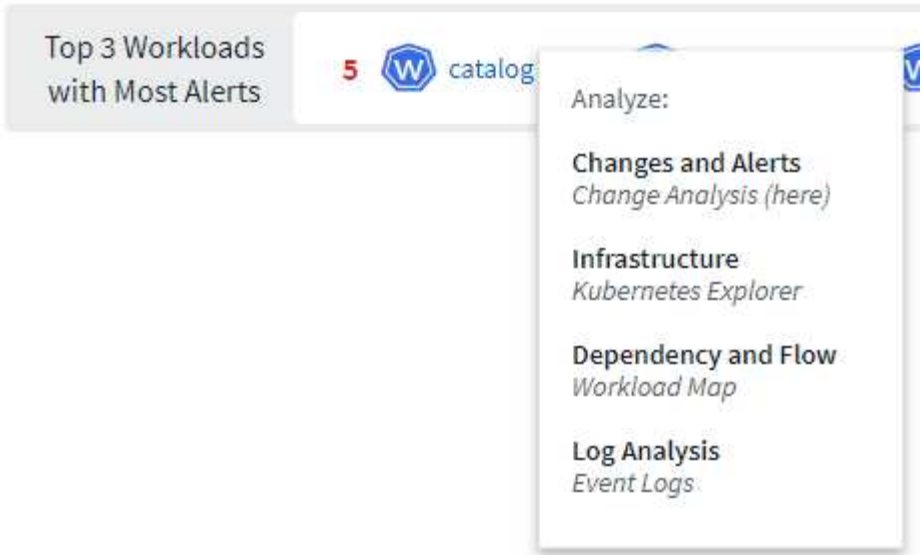
Abaixo da área de filtragem estão vários indicadores de alto nível. À esquerda está o número de alertas (Aviso e crítico). Este número inclui alertas *ative*, bem como *resolved*. Para ver apenas alertas *ative*, defina um filtro para "Status" e escolha "Ativo".

Alerts 6 17

O status de implantação também é mostrado aqui. Novamente, o padrão é mostrar a contagem de implantações *Started*, *Complete* e *Failed*. Para ver apenas implantações *Failed*, defina um filtro para "Status" e selecione "Failed".

Deploys 36 4

Os 3 principais workloads com mais alertas são os próximos. O número em vermelho ao lado de cada carga de trabalho indica o número de alertas relacionados a essa carga de trabalho. Clique no link carga de trabalho para explorar a infraestrutura (Kubernetes Explorer), dependências (mapa de carga de trabalho) ou análise de log (logs de eventos).



Painel de detalhes

Selecionar uma alteração na lista abre um painel descrevendo a alteração com mais detalhes. Por exemplo, selecionar uma implantação com falha mostra um resumo da implantação, com tempos de início e fim, duração e onde a implantação foi acionada, com links para explorar esses recursos. Ele também exibe o motivo da falha, quaisquer alterações relacionadas e quaisquer eventos associados.

Deploy Failed



Summary

Start Time

10/18/2023 2:40:01 PM

End Time

10/18/2023 2:50:02 PM

Duration

10 minutes

Triggered On

 ci-demo-01 >

 netapp-fitness-store-01 >

 billing-accounts >

Triggered On : kind

Deployment

Failure Detail

Reason For Failure

ProgressDeadlineExceeded - ReplicaSet "billing-accounts-6ddc7df546" has timed out progressing.

Message

Failed deploy

Changes (2)

Attribute Name	Previous	New
spec.template.spec.containers[0].image	210811600188.dkr.ecr.us-east-1.amazonaws.com/sm-billing-accounts-apis:1.0.0	210811600188.dkr.ecr.us-east-1.amazonaws.com/sm-billing-accounts-apis:1.0.09
metadata.annotations.deployment.kubernetes.io/revision	2964	2965

[All Changes Diff](#)

Associated Events

[Event Logs](#)

Close

A seleção de um Alerta fornece detalhes sobre o alerta, incluindo o monitor que acionou o alerta, bem como um gráfico que mostra uma linha do tempo visual para o alerta.

Essenciais de ONTAP

O ONTAP Essentials é um conjunto de painéis e fluxos de trabalho que fornece visões gerais detalhadas dos seus inventários e workloads do ONTAP. Você pode ver os seguintes termos usados ao trabalhar no ONTAP Essentials:

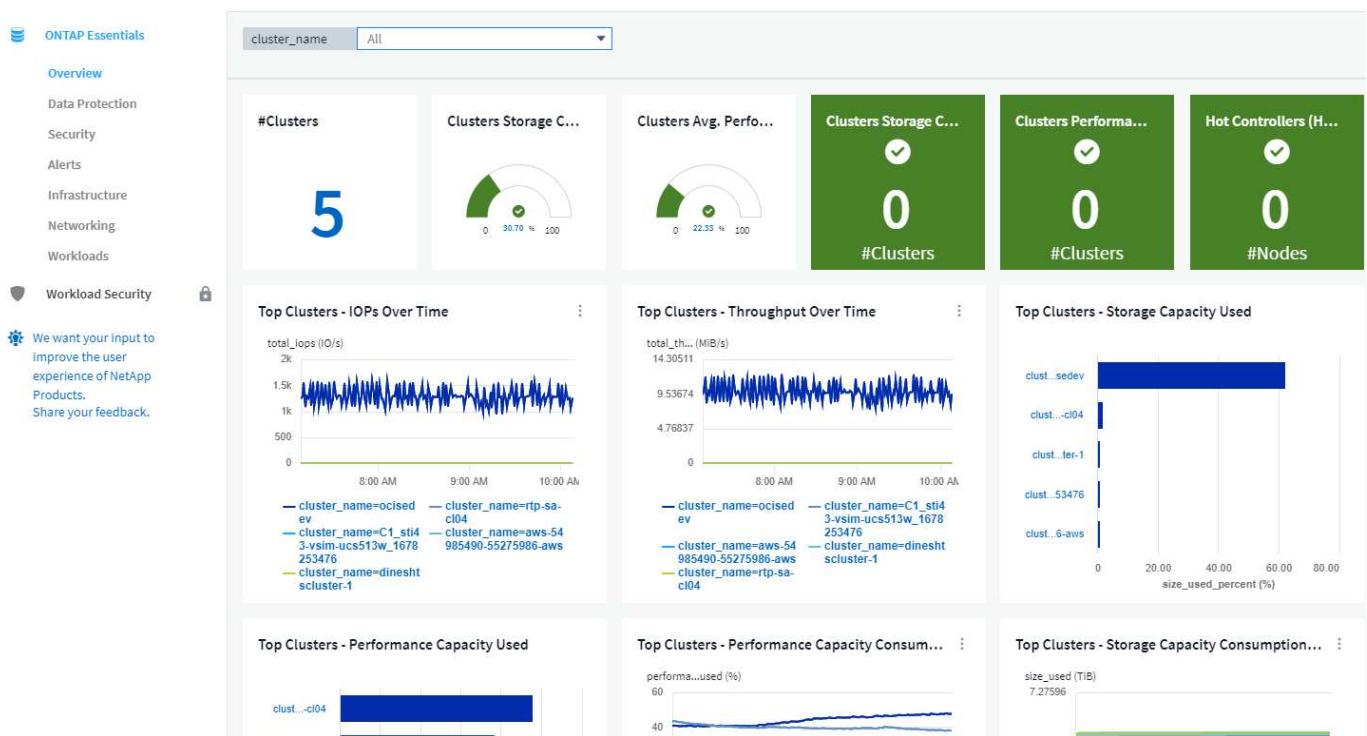
- Infraestrutura/Inventário: Objetos que fornecem serviços de storage/rede para dados do usuário
- Cargas de trabalho: Objetos que fornecem interface aos usuários para ler/gravar dados.
- Proteção de dados: Objetos que podem ser protegidos com as tecnologias de proteção de dados da NetApp

Para obter termos e definições adicionais relacionados ao ONTAP, consulte a ["Coletor de dados ONTAP"](#) documentação.

O ONTAP Essentials requer pelo menos um coletor de dados ONTAP funcional com dados coletados nos últimos sete dias.

Visão geral

Para começar a explorar, selecione **ONTAP Essentials** no menu principal de informações sobre infraestrutura de dados.



O painel **Visão geral** exibe informações úteis, como o número de clusters no localatário, com suas porcentagens gerais de capacidade e desempenho. Você também verá dados preditivos sobre o número de dias esperados até que a capacidade de storage ou a capacidade de performance fiquem sem espaço. Além disso, se quaisquer controladores em sua infraestrutura estiverem sendo executados com sua CPU em mais de 65% - potencialmente colocando seu cluster em risco em caso de failover - o ONTAP Essentials mostra esses controladores como controladores "quentes".

Gráficos informativos dão-lhe uma olhada no desempenho ao longo do tempo, bem como avarias de uso de capacidade. Cada um desses gráficos ou pontos de dados pode ser usado como ponto de partida para exploração ou investigação.

Nota: Um número de "dias para cheio" de "0" (zero) indica que dias para cheio é estimado em mais de 90 dias. Em outras palavras, seus sistemas não correm o risco de ficar sem espaço em breve.

Proteção de dados

A página **proteção de dados** mostra o status dos volumes protegidos por **cópias Snapshot** ou **políticas SnapMirror**.

Na seção *Visão geral da proteção local*, os gráficos fornecem as seguintes informações para volumes protegidos por cópias Snapshot:

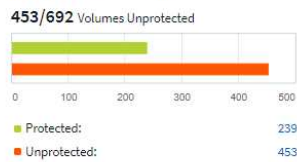
- O número de volumes protegidos pelas cópias Snapshot e os não protegidos.
- O número de volumes que estão usando ou excedendo o espaço de reserva para as cópias Snapshot.
- O número de volumes em intervalos específicos de contagem de cópias Snapshot (ou seja, menos de 10 cópias, 10 a 200, etc.).

Na seção *Visão geral da proteção remota*, os gráficos fornecem informações relacionadas a volumes protegidos pelas políticas do SnapMirror:

- O número de relacionamentos saudáveis e insalubres do SnapMirror.
- O número de relacionamentos do SnapMirror que apresentam atraso no objetivo do ponto de restauração (RPO) com base no status de atraso.
- O número de relacionamentos protegidos por tipos de proteção de volume SnapMirror, como volume SnapMirror, relacionamentos SVMDR, relacionamentos FlexGroup SnapMirror, relacionamentos de grupo de consistência de continuidade de negócios (SMBC) da SnapMirror, bem como volumes desprotegidos.
- O número de relacionamentos protegidos pelos tipos de relacionamento do SnapMirror, como espelhamento assíncrono, cofre assíncrono, espelhamento assíncrono, StrictSync e sincronização.

Local Protection Overview

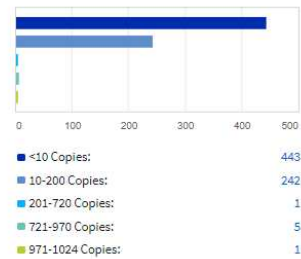
Snapshot Volume Protection



Snapshot Reserve Space



Snapshot Copy Count

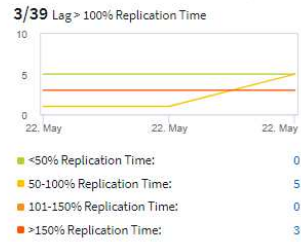


Remote Protection Overview

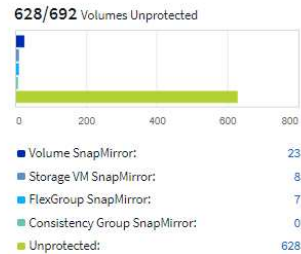
Unhealthy SnapMirror Relationships



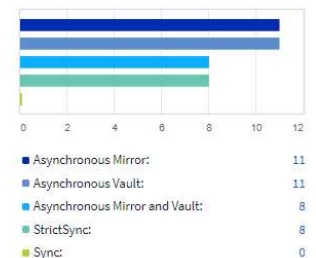
SnapMirror Volume Lag



SnapMirror Volume Protection



SnapMirror Relationship Types



A grade *clusters* na parte inferior da página fornece detalhes relacionados ao seguinte:

- Volumes não protegidos por snapshots.
- Volumes que invadem o espaço de reserva do snapshot.
- Volumes não protegidos pelas políticas do SnapMirror e pelas relações do SnapMirror com atraso.
- Relacionamentos de SnapMirror pouco saudáveis.

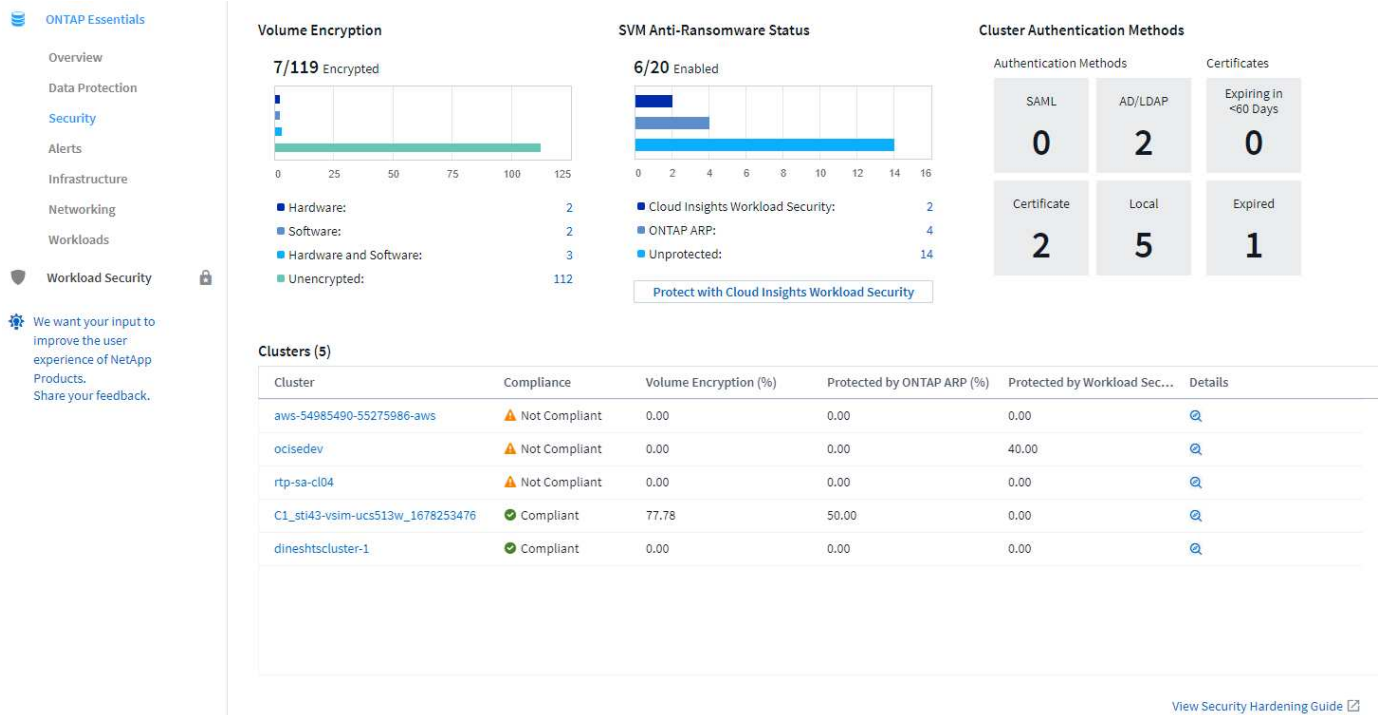
Clusters (6)

Cluster	Volumes Not Protected by Snapshots ↓	Volumes Breaching Snapshot Reserve Space	Volumes Not Protected by SnapMirror	SnapMirror Relationships Experiencing Lag	Unhealthy SnapMirror Relationships
ftp-sa-cl01	304	1	393	0	1
umeng-aff300-01-02	123	20	160	1	3
annapook-vsimg12	7	4	7	0	3
C1_sti11-vsimg-ucs574m_16832i 0	0	0	0	0	0
C1_sti43-vsimg-ucs513w_167825 0	0	0	0	0	0
ci-cs-fas8060-01-02	0	0	0	0	0

Segurança

O Painel de Segurança oferece uma visão instantânea da situação de segurança atual, mostrando gráficos para criptografia de volume de hardware e software, status anti-ransomware e métodos de autenticação de cluster. Os critérios de segurança são avaliados com base nas recomendações definidas no "[Guia de endurecimento de Segurança da NetApp para ONTAP 9](#)".






Selecione qualquer uma das contagens de criptografia ou anti-ransomware para mergulhar no seu ambiente.



O painel de segurança do ONTAP Essentials monitora seu ambiente para determinar o status de conformidade do cluster. Consulte "[Categorias de conformidade de cluster](#)" para saber mais. O ONTAP Essentials usa os seguintes monitores para determinar a conformidade:

Nome do monitor	Nome do atributo (exibido em Detalhes do cluster)	Valor em conformidade com o atributo
Modo FIPS desativado	Modo FIPS	Ativado
Cifras inseguras de cluster para SSH	Configurações de SSH seguras	Sim
Protocolo Telnet ativado	Telnet	Desativado
Shell remoto ativado	Shell remoto	Desativado
Utilizador Admin local predefinido ativado	Usuário Administrador padrão	Desativado
MD5 Palavra-passe com hash	MD5 em uso	Não
Comunicação por pares de cluster não encriptada	Peering de clusters	Encriptado/sem Peer
Transporte HTTPS AutoSupport desativado	AutoSupport usando HTTPS	Sim
Nenhum servidor NTP está configurado	Protocolo de hora de rede	Configurado
Contagem de servidor NTP baixa	Protocolo de hora de rede	Configurado
Banner de login de cluster desativado	Banner de login	Ativado
Encaminhamento de registo não encriptado	Encaminhamento de registos encriptado	Sim

Observe que se um monitor acima estiver desativado, os detalhes do cluster mostrarão o valor como "não verificado" para o atributo de conformidade de segurança correspondente.

Cluster	Compliance
aws-54985490-55275986-aws	 Not Compliant
ocisedev	 Not Compliant
rtp-sa-cl04	 Not Compliant
C1_sti43-vsimsim-ucs513w_1678253476	 Compliant
dineshtscluster-1	 Compliant

Para SVMs, o painel Segurança analisa os seguintes monitores:


Nome do monitor	Nome do atributo (exibido nas Configurações da VM de armazenamento)	Valor em conformidade com o atributo
Armazenamento VM cifras inseguras para SSH	Configurações de SSH seguras	Sim
Banner de login da VM de armazenamento desativado	Banner de login	Ativado
Registo de auditoria da VM de armazenamento desativado	Registo de auditoria	Ativado


Na lista de cluster, selecione *Ver Detalhes* para cada cluster para abrir um painel "slideout" mostrando as configurações atuais de *Cluster*, *Storage VM*, ou *Anti-ransomware*.


Os detalhes do cluster incluem status da conexão, informações do certificado e muito mais:
















Cluster Name:  C1_sti43-vsimsim-ucs513w_1678253476



Cluster Settings 

Storage VM Settings 






















Storage VM Anti-Ransomware 

Settings	Status
FIPS mode	 Disabled
Secure SSH Settings	 Not Checked
Telnet	 Disabled
Remote Shell	 Disabled
Default Admin User	 Enabled
MD5 in use	 No
Cluster Peering	 No Peer
AutoSupport using HTTPS	 Yes
Network Time Protocol	 Only 1 server is configured
Login Banner	 Not Checked
Log Forwarding Encrypted	N/A
Valid Cluster Certificate	 Yes
Certificate Issuer Type	 Self-Signed
SAML Users Configured	 No
LDAP Users Configured	 Yes
Active Directory Users Configured	 Yes

Close

Os detalhes da VM de armazenamento mostram informações de auditoria e SSH:

Cluster Name:  rtp-sa-cl04

Cluster Settings 	Storage VM Settings 	Storage VM Anti-Ransomware 	
Storage VM	Login Banner	Audit Log	Secure SSH Settings
mattsvm07_04	 Disabled	N/A	 Yes
sf-svmdr1	 Disabled	N/A	 Yes
ss_balajicifs	 Disabled	N/A	 Yes
ss_balajicifs_1_encrypted	 Disabled	N/A	 Yes
test1	 Enabled	 Disabled	 Yes
test2	 Disabled	N/A	 Yes
test3	 Disabled	N/A	 Yes
cl04_data_svm1	 Enabled	 Enabled	 Yes

Os detalhes do Anti-ransomware mostram se uma VM de storage está protegida pela proteção contra ransomware da ONTAP ou pela segurança de carga de trabalho dos Insights da infraestrutura de dados. Observe que a coluna ARP do ONTAP exibe o status atual da proteção contra ransomware integrada do ONTAP, que é configurada no sistema ONTAP. O Data Infrastructure Insights Workload Security pode ser habilitado selecionando "proteger" nessa coluna.

Cluster Name:  ocisedev



Cluster Settings 	Storage VM Settings 	Storage VM Anti-Ransomware 
Storage VM	Protected by Workload Security	Protected by ONTAP ARP
CloudComplianceSVM	<input type="button" value="Protect"/>	N/A
t1appSVM01	<input type="button" value="Protect"/>	N/A
tawny_mirror	<input type="button" value="Protect"/>	N/A
demoGroupShares	 Protected	N/A
demoGroupShares2 	 Protected	N/A

Alertas

Aqui você pode visualizar os alertas ativos no seu locatário e analisar rapidamente possíveis problemas. Selecione a guia *resolvido* para exibir alertas que foram resolvidos.

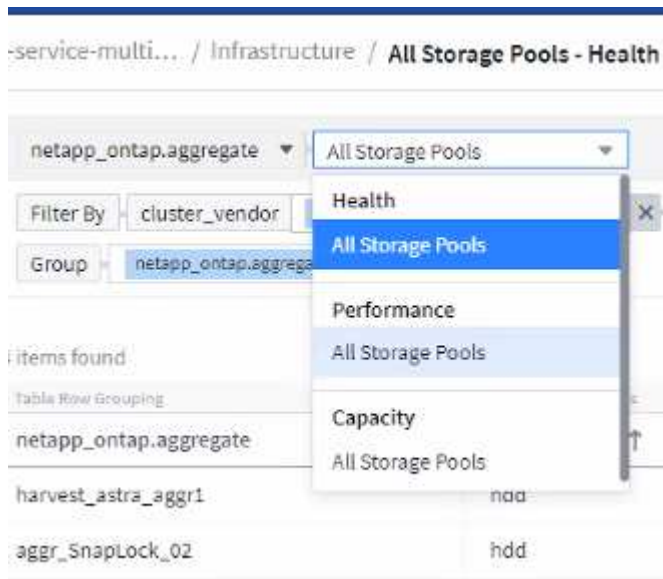
We want your input to improve the user experience of NetApp Products. Share your feedback.

Active (28) Resolved (0)

Filter By	triggeredOn	cluster_vendor: NetApp	status	New	In process	currentSeverity	Warning	Critical	
Alerts (28) Change All Alerts Status									
alertId	triggeredTime	currentSeverity	monitor	triggeredOn	status	hasCorrective Actions			
AL-169	3 hours ago Mar 9, 2023 7:12 AM	Warning	CVO NTP Server Count is ...	cluster_name: aws-54985490-55275986-aws cluster_vendor: NetApp cluster_uuid: 3407e797-be51-11ed-9476-eb015bbf1f0e cluster_model: CDvM200	New	✓			
AL-172	3 hours ago Mar 9, 2023 7:12 AM	Warning	CVO Default Local Admin ...	cluster_name: aws-54985490-55275986-aws cluster_vendor: NetApp cluster_uuid: 3407e797-be51-11ed-9476-eb015bbf1f0e cluster_model: CDvM200	New	✓			
AL-168	3 hours ago Mar 9, 2023 7:12 AM	Warning	CVO Storage VM Login Ba...	cluster_model: CDvM200 cluster_name: aws-54985490-55275986-aws cluster_vendor: NetApp cluster_uuid: 3407e797-be51-11ed-9476-eb015bbf1f0e vserver_uuid: 08f5ffb0-be52-11ed-9476-eb015bbf1f0e vserver_name: vs0	New	✓			
AL-171	3 hours ago Mar 9, 2023 7:12 AM	Warning	CVO Cluster Login Banner...	cluster_uuid: 3407e797-be51-11ed-9476-eb015bbf1f0e cluster_name: aws-54985490-55275986-aws cluster_vendor: NetApp cluster_model: CDvM200	New	✓			
AL-170	3 hours ago Mar 9, 2023 7:12 AM	Warning	CVO FIPS Mode Disabled	cluster_name: aws-54985490-55275986-aws cluster_vendor: NetApp cluster_uuid: 3407e797-be51-11ed-9476-eb015bbf1f0e cluster_model: CDvM200	New	✓			

Infraestrutura

A página ONTAP Essentials **infraestrutura** oferece uma visualização da integridade e desempenho do cluster, usando consultas pré-criadas (ainda mais personalizáveis) em todos os objetos ONTAP básicos. Selecione o tipo de objeto que deseja explorar (cluster, pool de armazenamento, etc.) e escolha se deseja exibir informações de integridade ou desempenho. Defina filtros para mergulhar mais fundo em sistemas individuais.



Página de infraestrutura mostrando a integridade do cluster:

Observability

ONTAP Essentials

- Overview
- Data Protection
- Infrastructure
- Workloads
- Security

We want your input to improve the user experience of NetApp Products. Share your feedback.

hhndks4 / Infrastructure / All Clusters - Health Last 3 Hours

netapp_ontap.cluster All Clusters

Filter By cluster_vendor NetApp

Group netapp_ontap.cluster

3 items found

Table Row Grouping	Metrics & Attributes			
netapp_ontap.cluster	fips_enabled ↑	cluster_version	node_count	cluster_location
rtp-sa-cl07	false	NetApp Release 9.8P13: Fri Jul 15 22:...	2	SA East Lab, RTP 1.3, Jxx
umeng-aff300-05-06	false	NetApp Release 9.9.1P9X3: Tue Apr 1...	2	GDL QQ 22
umeng-aff300-01-02	false	NetApp Release Metropolitan_9.11...	2	GDL

Rede

A rede essencial do ONTAP oferece visualizações para sua infraestrutura FC, NVMe FC, Ethernet e iSCSI. Nessas páginas, você pode explorar coisas como portas nos clusters e nos nós deles.

ONTAP Essentials

Overview

Data Protection

Alerts

Infrastructure

Networking

Workloads

Active (86) Resolved (0)

Filter By triggeredOn cluster_vendor: NetApp status New In process currentSeverity Warning Critical

Alerts (86) Change All Alerts Status

alertId	triggeredTime ↓	currentSeverity	monitor	triggeredOn	status	hasCorrective Actions
AL-356704	12 hours ago Sep 9, 2022 2:16 AM	Critical	Snapshot Reserve Space ...	cluster_name: rtp-sa-cl04 vserver_name: test_ran volume_name: thick_vol_2 cluster_uuid: f34cd2c8-f1b3-11e9-b97f-00a0985f6587 cluster_vendor: NetApp cluster_model: AFF8040	New	✓
AL-355988	a day ago Sep 8, 2022 11:00 AM	Warning	User Quota Capacity Soft ...	cluster_name: rtp-sa-cl06 volume: qtreesvol1 quota_type: user user_or_group: 16716 cluster_uuid: da294f0d-ad92-11e6-9969-00a0987b8fe8 cluster_vendor: NetApp cluster_model: FAS2552	New	✓

Workloads

Visualize e explore workloads em LUNs/volumes, compartilhamentos NFS ou SMB ou Qtrees no seu localtário.

LUNs / Volumes

Qtrees

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 e outras tarefas

API do Data Infrastructure Insights

A API de informações de infraestrutura de dados permite que clientes da NetApp e fornecedores independentes de software (ISVs) integrem informações de infraestrutura de dados com outros aplicativos, como CMDB ou outros sistemas de emissão de tíquetes.

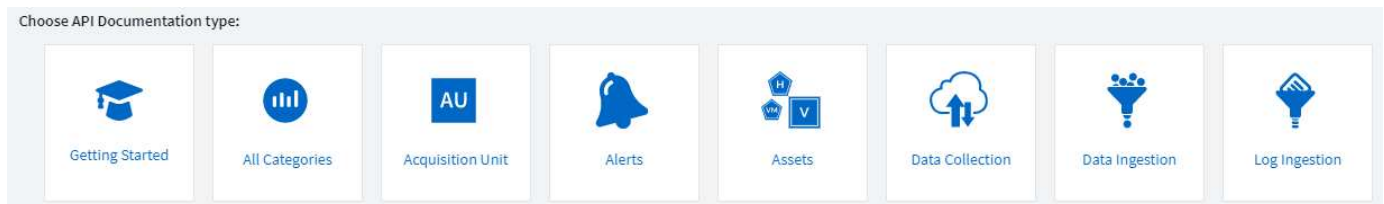
Seus insights de infraestrutura de dados "[função de conjunto de funcionalidades](#)" determinarão quais APIs você pode acessar. As funções de usuário e convidado têm menos Privileges do que a função de administrador. Por exemplo, se você tiver a função de Administrador no Monitor e Otimize, mas a função de Usuário no Relatório, poderá gerenciar todos os tipos de API, exceto o Data Warehouse.

Requisitos para acesso à API

- Um modelo de token de acesso à API é usado para conceder acesso.
- O gerenciamento de token de API é realizado por usuários do Data Infrastructure Insights com a função Administrador.

Documentação da API (Swagger)

As informações mais recentes da API são encontradas efetuando login no Data Infrastructure Insights e navegando para **Admin > API Access**. Clique no link **Documentação da API**.



A Documentação da API é baseada no Swagger, que fornece uma breve descrição e informações de uso para a API, e permite que você experimente isso em seu locatário. Dependendo da sua função de usuário e/ou edição do Data Infrastructure Insights, os tipos de API disponíveis podem variar.

POST

/assets/annotations Create annotation definition



Parameters

Try it out

No parameters

Request body

application/json



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

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

Example Value | Schema

```
{}
```

Tokens de acesso à API

Antes de usar a API Data Infrastructure Insights, você deve criar um ou mais **tokens de acesso à API**. Os tokens de acesso são usados para tipos de API especificados e podem conceder permissões de leitura e/ou gravação. Você também pode definir a expiração para cada token de acesso. Todas as APIs sob os tipos especificados são válidas para o token de acesso. Cada token é nulo de um nome de usuário ou senha.

Para criar um token de acesso:

- Clique em **Admin > API Access**
- Clique em * API Access Token*
 - Introduza o Nome do Token
 - Selecione tipos de API
 - Especifique as permissões concedidas para esse acesso à API
 - Especifique a expiração do token



Seu token só estará disponível para copiar para a área de transferência e salvar durante o processo de criação. Os tokens não podem ser recuperados depois que são criados, por isso é altamente recomendável copiar o token e salvá-lo em um local seguro. Você será solicitado a clicar no botão **Copiar token de acesso à API** antes de fechar a tela de criação de token.

Você pode desativar, ativar e revogar tokens. Os tokens que estão desativados podem ser ativados.

Os tokens concedem acesso de propósito geral às APIs da perspectiva do cliente, gerenciando o acesso às APIs no escopo de seu próprio locatário. Os administradores do cliente podem conceder e revogar esses tokens sem envolvimento direto do pessoal de back-end do Data Infrastructure Insights.

O aplicativo recebe um token de acesso depois que um usuário autentica e autoriza o acesso com êxito e passa o token de acesso como uma credencial quando chama a API de destino. O token passado informa à API que o portador do token foi autorizado a acessar a API e executar ações específicas especificadas pelo escopo que foi concedido durante a autorização.

O cabeçalho HTTP onde o token de acesso é passado é **X-CloudInsights-ApiKey**:

Por exemplo, use o seguinte para recuperar ativos de armazenamento:

```
curl https://<tenant_host_name>/rest/v1/assets/storages -H 'X-CloudInsights-ApiKey:<API_Access-Token>'
```

Onde `<API_Access-Token>` é o token que você salvou durante a criação do acesso à API.

Consulte as páginas de swagger para obter exemplos específicos da API que você deseja usar.

Tipo API

A API Data Infrastructure Insights é baseada em categoria e atualmente contém os seguintes tipos:

- O tipo DE ATIVOS contém APIs de ativo, consulta e pesquisa.
 - Assets: Enumerar objetos de nível superior e recuperar um objeto específico ou uma hierarquia de objetos.
 - Consulta: Recupere e gerencie consultas do Data Infrastructure Insights.
 - Importar: Importe anotações ou aplicativos e atribua-os a objetos
 - Pesquisa: Localize um objeto específico sem saber a ID exclusiva ou o nome completo do objeto.
- O tipo DE COLETA DE DADOS é usado para recuperar e gerenciar coletores de dados.
- O tipo de INGESTÃO DE DADOS é usado para recuperar e gerenciar dados de ingestão e métricas personalizadas, como de agentes Telegraf
- A INGESTÃO DE LOG é usada para recuperar e gerenciar dados de log

Tipos e/ou APIs adicionais podem ficar disponíveis ao longo do tempo. Você pode encontrar as informações mais recentes da API no "[Documentação do Swagger API](#)".

Observe que os tipos de API aos quais um usuário tem acesso dependem também dos "[Função de utilizador](#)" que eles têm em cada conjunto de recursos do Data Infrastructure Insights (monitoramento, segurança de workload, relatórios).

Travessia de inventário

Esta seção descreve como atravessar uma hierarquia de objetos do Data Infrastructure Insights.

Objetos de nível superior

Objetos individuais são identificados em solicitações por URL exclusiva (chamado "self" em JSON) e exigem conhecimento do tipo de objeto e ID interno. Para alguns dos objetos de nível superior (hosts, storages, etc.), a API REST fornece acesso à coleção completa.

O formato geral de uma URL da API é:

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

Por exemplo, para recuperar todos os armazenamentos de um locatário chamado `_mysite.C01.cloudinsights.NetApp.com_`, o URL de solicitação é:

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

Crianças e objetos relacionados

Objetos de nível superior, como armazenamento, podem ser usados para atravessar para outras crianças e objetos relacionados. Por exemplo, para recuperar todos os discos para um armazenamento específico, concatenar o URL "self" de armazenamento com `/disks`, por exemplo:

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

Expande

Muitos comandos API suportam o parâmetro **expand**, que fornece detalhes adicionais sobre o objeto ou URLs para objetos relacionados.

O único parâmetro de expansão comum é *expansions*. A resposta contém uma lista de todas as expansões específicas disponíveis para o objeto.

Por exemplo, quando você solicita o seguinte:

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

A API retorna todas as expansões disponíveis para o objeto da seguinte forma:

```

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

```

Cada expansão contém dados, um URL ou ambos. O parâmetro expandir suporta atributos múltiplos e aninhados, por exemplo:

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

Expandir permite que você traga muitos dados relacionados em uma resposta. A NetApp aconselha que não solicite demasiada informação de uma só vez; isto pode causar degradação do desempenho.

Para desencorajar isso, as solicitações de coleções de nível superior não podem ser expandidas. Por exemplo, você não pode solicitar dados de expansão para todos os objetos de armazenamento de uma só vez. Os clientes são obrigados a recuperar a lista de objetos e, em seguida, escolher objetos específicos para expandir.

Dados de performance

Os dados de desempenho são coletados em vários dispositivos como amostras separadas. A cada hora (o padrão), o Data Infrastructure Insights agrega e resume amostras de desempenho.

A API permite o acesso a amostras e aos dados resumidos. Para um objeto com dados de desempenho, um resumo de desempenho está disponível como `_expand`. As séries temporais do histórico de desempenho estão disponíveis através de

Exemplos de objetos de dados de desempenho incluem:

- StoragePerformance
- StoragePoolPerformance
- PortPerformance
- DiskPerformance

Uma métrica de desempenho tem uma descrição e um tipo e contém uma coleção de resumos de desempenho. Por exemplo, latência, tráfego e taxa.

Um Resumo de desempenho tem uma descrição, unidade, hora de início da amostra, hora de fim da amostra e uma coleção de valores resumidos (corrente, min, máx, média, etc.) calculados a partir de um único contador de desempenho em um intervalo de tempo (1 hora, 24 horas, 3 dias, etc.).

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

Details

Response body

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

Self

Performance Metric

Response body

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

```

History

Timestamp

Counter Values

O dicionário de dados de desempenho resultante tem as seguintes chaves:

- "Self" é a URL exclusiva do objeto

- "histórico" é a lista de pares de timestamp e mapa de valores de contadores
- Cada outra chave do dicionário ("diskThroughput" e assim por diante) é o nome de uma métrica de desempenho.

Cada tipo de objeto de dados de desempenho tem um conjunto exclusivo de métricas de desempenho. Por exemplo, o objeto de desempenho da Máquina Virtual suporta "diskThroughput" como uma métrica de desempenho. Cada métrica de desempenho suportada é de uma certa "performanceCategory" apresentada no dicionário de métricas. O Data Infrastructure Insights oferece suporte a vários tipos de métricas de desempenho listados posteriormente neste documento. Cada dicionário de métrica de desempenho também terá o campo "descrição" que é uma descrição legível por humanos dessa métrica de desempenho e um conjunto de entradas de contador de resumo de desempenho.

O contador de Resumo de desempenho é o resumo dos contadores de desempenho. Apresenta valores agregados típicos como min, Max e avg para um contador e também o valor observado mais recente, intervalo de tempo para dados resumidos, tipo de unidade para contador e limiares para dados. Apenas os limites são opcionais; o resto dos atributos são obrigatórios.

Estão disponíveis resumos de desempenho para estes tipos de contadores:

- Leia – Resumo para operações de leitura
- Escrever – Resumo para operações de escrita
- Total – Resumo para todas as operações. Pode ser maior do que a soma simples de leitura e escrita; pode incluir outras operações.
- Total máximo – Resumo para todas as operações. Este é o valor total máximo no intervalo de tempo especificado.

Métricas de performance do objeto

A API pode retornar métricas detalhadas para objetos no seu localatário, por exemplo:

- Métricas de desempenho de storage como IOPS (número de solicitações de entrada/saída por segundo), latência ou taxa de transferência.
- Métricas de desempenho do switch, como utilização de tráfego, dados BB Credit Zero ou erros de porta.

Consulte o "[Documentação do Swagger API](#)" para obter informações sobre métricas para cada tipo de objeto.

Dados do histórico de performance

Os dados de histórico são apresentados em dados de desempenho como uma lista de pares de mapas de carimbo de data/hora e contador.

Os contadores de histórico são nomeados com base no nome do objeto da métrica de desempenho. Por exemplo, o objeto de desempenho da máquina virtual suporta "diskThroughput" para que o mapa de histórico contenha chaves chamadas "diskThroughput.read", "diskThroughput.write" e "diskThroughput.total".



Timestamp está no formato de hora UNIX.

A seguir está um exemplo de um JSON de dados de desempenho para um disco:

```

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

```

Objetos com atributos de capacidade

Objetos com atributos de capacidade usam tipos de dados básicos e o `CapacityItem` para representação.

CapacityItem

`CapacityItem` é uma única unidade lógica de capacidade. Ele tem "valor" e "highThreshold" em unidades definidas por seu objeto pai. Ele também suporta um mapa de divisão opcional que explica como o valor da capacidade é construído. Por exemplo, a capacidade total de um `storagePool` de 100 TB seria um `CapacityItem` com um valor de 100. O detalhamento pode mostrar 60 TB alocados para "dados" e 40 TB para "instantâneos".

Nota

"HighThreshold" representa limites definidos pelo sistema para as métricas correspondentes, que um cliente pode usar para gerar alertas ou dicas visuais sobre valores que estão fora dos intervalos configurados aceitáveis.

A seguir mostra a capacidade dos `StoragePools` com vários contadores de capacidade:

StoragePoolCapacity

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

close

Usando a Pesquisa para procurar objetos

A API de pesquisa é um ponto de entrada simples para o sistema. O único parâmetro de entrada para a API é uma string de forma livre e o JSON resultante contém uma lista categorizada de resultados. Os tipos são tipos de ativos diferentes do Inventário, como armazenamentos, hosts, datastores e assim por diante. Cada tipo conterá uma lista de objetos do tipo que correspondem aos critérios de pesquisa.


O Data Infrastructure Insights é uma solução extensível (aberta) que permite integrações com sistemas de orquestração, gerenciamento de negócios, controle de alterações e emissão de tíquetes, bem como integrações personalizadas de CMDB.

A API RESTful do Cloud Insight é um ponto de integração principal que permite a movimentação simples e eficaz de dados, além de permitir que os usuários obtenham acesso otimizado aos dados.

Desativando ou revogando um token de API

Para desativar temporariamente um token de API, na página de lista de token de API, clique no menu "três pontos" da API e selecione *Desativar*. Você pode reativar o token a qualquer momento usando o mesmo menu e selecionando *enable*.

Para remover permanentemente um token de API, no menu, selecione "revogar". Não é possível reativar um token revogado; você deve criar um novo token.

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

Disable
Edit Description
Revoke

Girando tokens de acesso à API expirados

Os tokens de acesso à API têm uma data de validade. Quando um token de acesso à API expira, os usuários precisam gerar um novo token (do tipo *ingestão de dados* com permissões de leitura/gravação) e reconfigurar o Telegraf para usar o token recém-gerado em vez do token expirado. As etapas abaixo detalham como fazer isso.

Kubernetes

Observe que esses comandos estão usando o namespace padrão "NetApp-monitoring". Se você tiver definido seu próprio namespace, substitua esse namespace nesses e todos os comandos e arquivos subsequentes.

Observação: Se você tiver o operador de monitoramento mais recente do NetApp Kubernetes instalado e usar um token de acesso à API renovável, os tokens expirados serão automaticamente substituídos por tokens de acesso à API novos/atualizados. Não é necessário executar as etapas manuais listadas abaixo.

- Edite o Operador de Monitoramento do Kubernetes do NetApp.

```
kubectl -n netapp-monitoring edit agent agent-monitoring-netapp  
* Modifique o valor _spec.output-sink.api-key_, substituindo o antigo token de API pelo novo token de API.
```

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

RHEL/CentOS e Debian/Ubuntu

- Edite os arquivos de configuração do Telegraf e substitua todas as instâncias do token de API antigo pelo novo token de API.

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

```
sudo systemctl restart telegraf
```

Windows

- Para cada arquivo de configuração do Telegraf em _C: Arquivos de programas, substitua todas as instâncias do token API antigo pelo novo token da API.

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

- Reinicie o Telegraf.

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

Monitoramento do seu ambiente

Auditoria

Para identificar as alterações esperadas (para rastreamento) ou inesperadas (para solução de problemas), você pode visualizar uma trilha de auditoria dos eventos do sistema Data Infrastructure Insights e das atividades do usuário.

Visualizar eventos auditados

Para visualizar a página Auditoria, clique em **Admin > Auditoria** no menu. A página Auditoria é exibida, fornecendo os seguintes detalhes para cada entrada de auditoria:

- **Hora** - Data e hora do evento ou atividade
- **Usuário** - o Usuário que iniciou a atividade
- **Função** - a função do usuário no Data Infrastructure Insights (convidado, usuário, administrador)
- **IP** - o endereço IP associado ao evento
- **Ação** - tipo de atividade, por exemplo Login, criar, Atualizar
- **Categoria** - a categoria de atividade
- **Detalhes** - Detalhes da atividade

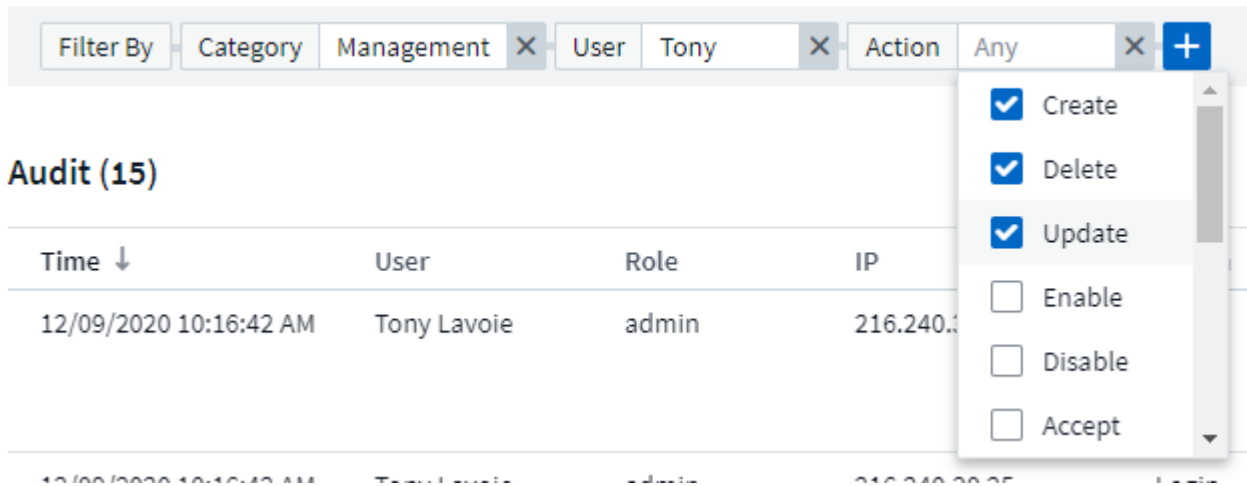
Exibindo entradas de auditoria

Existem várias formas diferentes de ver entradas de auditoria:

- Você pode exibir entradas de auditoria escolhendo um período de tempo específico (1 hora, 24 horas, 3 dias, etc.).
- Você pode alterar a ordem de classificação das entradas para ascendente (seta para cima) ou descendente (seta para baixo) clicando na seta no cabeçalho da coluna.

Por padrão, a tabela exibe as entradas em ordem decrescente de tempo.

- Você pode usar os campos de filtro para mostrar apenas as entradas desejadas na tabela. Clique no botão para adicionar filtros adicionais.



Mais sobre filtragem

Você pode usar qualquer um dos seguintes para refinar seu filtro:

Filtro	O que faz	Exemplo	Resultado
* (Asterisco)	permite-lhe procurar tudo	vol*rhel	retorna todos os recursos que começam com "vol" e terminam com "rhel"
? (ponto de interrogação)	permite-lhe procurar um número específico de caracteres	BOS-PRD??-S12	Retorna BOS-PRD 12 _S12, BOS-PRD 23 _S12, e assim por diante
OU	permite especificar várias entidades	FAS2240 OU CX600 OU FAS3270	Retorna qualquer um de FAS2440, CX600 ou FAS3270
NÃO	permite excluir texto dos resultados da pesquisa	NÃO EMC*	Retorna tudo o que não começa com "EMC"
<i>Nenhum</i>	Procura em branco/NULL/None em qualquer campo selecionado	<i>Nenhum</i>	retorna resultados em que o campo de destino não está vazio
Não *	Como em <i>None</i> acima, mas você também pode usar este formulário para procurar valores NULL em campos <i>text-only</i>	Não *	retorna resultados em que o campo de destino não está vazio.
""	procura uma correspondência exata	"NetApp"	Retorna resultados contendo a string literal exata <i>NetApp</i> *

Se você incluir uma string de filtro em aspas duplas, o Insight trata tudo entre a primeira e a última citação como uma correspondência exata. Quaisquer caracteres especiais ou operadores dentro das aspas serão

tratados como literais. Por exemplo, a filtragem para "*" retornará resultados que são um asterisco literal; o asterisco não será Tratado como um curinga neste caso. Os operadores OU E NÃO também serão tratados como strings literais quando incluídos em aspas duplas.

Eventos e ações auditadas

Os eventos e ações auditados pelo Data Infrastructure Insights podem ser categorizados nas seguintes áreas amplas:

- **Conta de usuário:** Login, logout, mudança de função, etc.

Exemplo: *Usuário **Tony Lavoie** logado a partir de **10,1.120,15**, agente de usuário **Mozilla/5,0 (Windows NT 10,0; Win64; x64) AppleWebKit/537,36 (KHTML, como Gecko) Chrome/85.0.4183.121 Safari/537,36**, método(s) de login **Início de sessão do Portal BlueXP***

- **Unidade de aquisição:** Criar, excluir, etc.

Exemplo: *Unidade de aquisição **AU-Boston-1** removida.*

- **Coletor de dados:** Adicionar, remover, modificar, adiar/retomar, alterar unidade de aquisição, iniciar/parar, etc.

Exemplo: *Datasource **Laboratório FlexPod** removido, fornecedor **NetApp**, modelo **Software de gerenciamento de dados ONTAP**, ip **192.168.106.5**.*

- *** Aplicação*:** Adicionar, atribuir a objeto, remover, etc.

Exemplo: *Volume interno **ocisedev:t1appSVM01:t1appFlexVol01** adicionado ao aplicativo **Test App**.*

- **Anotação:** Adicionar, atribuir, remover, ações de regra de anotação, alterações de valor de anotação, etc.

Exemplo: *Valor de anotação **Boston** adicionado ao tipo de anotação **SalesOffice**.*

- **Consulta:** Adicionar, remover, etc.

Exemplo: *Query **TL Sales Query** é adicionado.*

- **Monitor:** Adicionar, remover, etc.

Exemplo: *Monitor **tamanho do Aggr - CI Alertas notificações Dev** atualizado*

- **Notificação:** Alterar e-mail, etc.


Exemplo: *Destinatário **CI-alerts-notifications-dl** criado*

Exportar eventos de auditoria

Você pode exportar os resultados da exibição Auditoria para um arquivo .CSV, que permitirá analisar os dados ou importá-los para outro aplicativo.

Passos

1. Na página Auditoria, defina o intervalo de tempo desejado e os filtros desejados. O Data Infrastructure Insights exportará apenas as entradas de Auditoria que correspondem à filtragem e ao intervalo de tempo que você definiu.

2. Clique no botão *Export*  no canto superior direito da tabela.

Os eventos de auditoria exibidos serão exportados para um arquivo .CSV, até um máximo de 10.000 linhas.

Retenção de dados de auditoria

O período de tempo que o Data Infrastructure Insights retém os dados de auditoria é baseado na sua Edição:

- Edição básica: Os dados de auditoria são mantidos por 30 dias
- Edições Standard e Premium: Os dados de auditoria são retidos por 1 ano mais 1 dia

As entradas de auditoria mais antigas do que o tempo de retenção são automaticamente eliminadas. Nenhuma interação do usuário é necessária.

Solução de problemas

Aqui você encontrará sugestões para solucionar problemas com a Auditoria.

Problema:	Tente isto:
Vejo mensagens de auditoria me informando que um monitor foi exportado.	A exportação de uma configuração de monitor personalizada geralmente é usada por engenheiros da NetApp durante o desenvolvimento e teste de novos recursos. Se você não esperava ver essa mensagem, considere explorar as ações do usuário nomeado na ação auditada ou entre em Contato com o suporte.

Active IQ

O NetApp "Active IQ" fornece uma série de visualizações, análises e outros serviços relacionados ao suporte aos clientes da NetApp para seus sistemas de hardware/software. Os dados reportados pela Active IQ podem melhorar a solução de problemas do sistema e também fornecer informações sobre otimização e análise preditiva relacionadas aos seus dispositivos.

O Insights de infraestrutura de dados coleta os **riscos** para qualquer sistema de storage NetApp Clustered Data ONTAP que é monitorado e reportado pela Active IQ. Os riscos relatados para os sistemas de storage são coletados automaticamente pelo Data Infrastructure Insights como parte de sua coleta de dados desses dispositivos. Você deve adicionar o coletor de dados apropriado ao Insights de infraestrutura de dados para coletar informações de risco do Active IQ.

Os insights de infraestrutura de dados não mostrarão dados de risco para sistemas ONTAP que não sejam monitorados e relatados pela Active IQ.

Os riscos relatados são mostrados em Data Infrastructure Insights nas páginas de destino de ativos *storage* e *storage node*, na tabela "riscos". A tabela mostra Detalhes do risco, Categoria de risco e impacto potencial do risco e também fornece um link para a página Active IQ resumindo todos os riscos para o nó de armazenamento (logon da conta de suporte da NetApp necessário).

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

Uma contagem de riscos relatados também é mostrada no widget Resumo da página de destino, com um link para a página Active IQ apropriada. Em uma Landing page *storage*, a contagem é uma soma de riscos de todos os nós de storage subjacentes.

Storage Summary

Model: FAS6210 Vendor: NetApp Family: FAS6200 Serial Number: 1-80-000013 IP: 10.197.143.25	Microcode Version: 8.3.2 clustered Data ONTAP Raw Capacity: 80,024.3 GB Latency - Total: 0.77 ms IOPS - Total: 1,819.19 IO/s Throughput - Total: 41.69 MB/s	Management: HTTPS://10.197.143.25:443 FC Fabrics Connected: 0 Performance Policies: <div style="border: 2px solid blue; border-radius: 10px; padding: 5px; display: inline-block;"> Risks: 108 risks detected by Active IQ ↗ </div>
--	---	--

Abrindo a página Active IQ

Ao clicar no link para uma página do Active IQ, se você não estiver conectado atualmente à sua conta do Active IQ, execute as etapas a seguir para exibir a página Active IQ do nó de armazenamento.

1. Na tabela Resumo de informações de infraestrutura de dados ou riscos, clique no link "Active IQ".
2. Inicie sessão na sua conta de suporte da NetApp. Você é direcionado diretamente para a página do nó de storage no Active IQ.

Buscando riscos

No Data Infrastructure Insights, você pode adicionar a coluna **Monitoring.count** a uma consulta de nó de armazenamento ou armazenamento. Se o resultado retornado incluir sistemas de storage monitorados por Active IQ, a coluna Monitoring.count exibirá o número de riscos para o sistema de storage ou nó.

Dashboards

Você pode criar widgets (por exemplo, gráfico de pizza, widget de tabela, barra, coluna, gráfico de dispersão e widgets de valor único) para visualizar riscos de objetos para nós de armazenamento e armazenamento para sistemas NetApp Clustered Data ONTAP monitorados pelo Active IQ. Os "riscos do objeto" podem ser selecionados como uma coluna ou métrica nestes widgets onde Storage ou Storage Node é o objeto de foco.

Object Risks by Array

12 items found

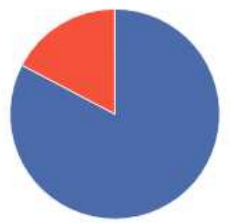
Name	Object Risks ↓
tawny	110
rtp-sa-select01	23
rtp-sa-cl02	N/A
rtp-sa-cl07	N/A
oci-phonehome	N/A
durlabprdfs01	N/A
oci-3070-01	N/A

Object Risks by Node

25 items found

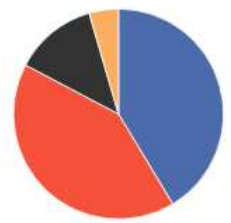
Name	Object Risks ↓
tawny02	55
tawny01	55
rtp-sa-select01-1	17
rtp-sa-select01-2	6
tnode02	N/A
rtp-sa-cl06-01	N/A
rtp-sa-cl06-02	N/A

Object Risks by Storage



■ tawny ■ rtp-sa-select01

Object Risks by Storage Node



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

Total Storage Risks

133.00
Object Risks

Segurança da carga de trabalho

Sobre o Storage Workload Security

A segurança de workload de storage (anteriormente Cloud Secure) ajuda a proteger seus dados com inteligência acionável sobre ameaças internas. Ele fornece visibilidade e controle centralizados de todos os acessos a dados corporativos em ambientes de nuvem híbrida para garantir que as metas de segurança e conformidade sejam atingidas.

Visibilidade

Obtenha visibilidade centralizada e controle do acesso do usuário aos dados corporativos essenciais armazenados no local ou na nuvem.

Substitua as ferramentas e os processos manuais que não fornecem visibilidade atempada e precisa do acesso e controle dos dados. O Workload Security opera exclusivamente em sistemas de storage na nuvem e no local para fornecer alertas em tempo real de comportamento mal-intencionado do usuário.

Proteção

Proteja os dados organizacionais contra a utilização indevida por parte de usuários mal-intencionados ou comprometidos por meio do aprendizado de máquina avançado e da detecção de anomalias.

Alerta você para acesso anormal aos dados por meio do aprendizado de máquina avançado e da detecção de anomalias de comportamento do usuário.

Conformidade

Garanta a conformidade empresarial auditando o acesso aos dados dos usuários aos dados corporativos essenciais armazenados no local ou na nuvem.

Como começar

Introdução ao Workload Security

Há tarefas de configuração que precisam ser concluídas antes de começar a usar o Workload Security para monitorar a atividade do usuário.

O sistema de segurança de carga de trabalho usa um agente para coletar dados de acesso de sistemas de armazenamento e informações de usuários de servidores de Serviços de diretório.

Você precisa configurar o seguinte antes de começar a coletar dados:

Tarefa	Informações relacionadas
--------	--------------------------

Configurar um agente	"Requisitos do agente" "Adicionar agente" " Vídeo: Implantação de agentes"
Configure um conector do diretório de usuários	"Adicionar conector do diretório do utilizador" " Vídeo: Conexão do ativo Directory"
Configurar coletores de dados	Clique em Workload Security > Collectors clique no coletor de dados que deseja configurar. Consulte a seção Referência do fornecedor do coletor de dados da documentação. " Vídeo: Conexão ONTAP SVM"
Crie contas de usuários	"Gerir contas de utilizador"
Solução de problemas	" Vídeo: Resolução de problemas"

O Workload Security também pode ser integrado a outras ferramentas. Por exemplo, ["consulte este guia"](#) na integração com o Splunk.

Requisitos do Agente de Segurança de carga de trabalho

Você deve ["Instale um agente"](#), a fim de adquirir informações de seus coletores de dados. Antes de instalar o agente, você deve garantir que seu ambiente atenda aos requisitos do sistema operacional, CPU, memória e espaço em disco.

Componente	Requisito Linux
Sistema operacional	Um computador executando uma versão licenciada de um dos seguintes: * CentOS 64 64 64 24,04 11 9,4 Stream (9,2 15 SP3 20,04 64 64 64-bit), CentOS 9 9,4 15 SP5 22,04 10 9,3 Stream, SELinux * OpenSUSE Leap 8,8 a 15,5 (64-bit) * Oracle Linux 8,6 - 64, 9,1 a 9,4 (8,8-bit) * Red Hat Enterprise Linux 8,6 a 15,3, 9,1 a 9,4 (8-bit), SELinux * Rocky 64 Recomenda-se um servidor dedicado.
Comandos	'unzip' é necessário para a instalação. Além disso, o comando 'sudo su -' é necessário para instalação, execução de scripts e desinstalação.
CPU	4 núcleos de CPU
Memória	16 GB DE RAM

Componente	Requisito Linux
Espaço disponível em disco	O espaço em disco deve ser alocado desta maneira: /Opt/NetApp 36 GB (mínimo de 35 GB de espaço livre após a criação do sistema de arquivos) Nota: Recomenda-se alocar um pouco de espaço em disco extra para permitir a criação do sistema de arquivos. Certifique-se de que haja pelo menos 35 GB de espaço livre no sistema de arquivos. Se /opt for uma pasta montada a partir de um armazenamento nas, certifique-se de que os utilizadores locais têm acesso a esta pasta. O Agent ou Data Collector pode falhar na instalação se os usuários locais não tiverem permissão para essa pasta. Consulte " solução de problemas " a seção para obter mais detalhes.
Rede	Conexão Ethernet de 100 Mbps a 1 Gbps, endereço IP estático, conectividade IP a todos os dispositivos e uma porta necessária para a instância de segurança de carga de trabalho (80 ou 443).

Observação: O agente Workload Security pode ser instalado na mesma máquina que uma unidade de aquisição e/ou agente do Data Infrastructure Insights. No entanto, é uma prática recomendada instalá-los em máquinas separadas. No caso de estes estarem instalados na mesma máquina, atribua espaço em disco, conforme ilustrado abaixo:

Espaço disponível em disco	50-55 GB para Linux, o espaço em disco deve ser alocado desta maneira: /Opt/NetApp 25-30 GB /var/log/NetApp 25 GB
----------------------------	--

Recomendações adicionais

- É altamente recomendável sincronizar a hora no sistema ONTAP e na máquina do agente usando **Protocolo de tempo de rede (NTP)** ou **Protocolo de tempo de rede simples (SNTP)**.

Regras de acesso à rede na nuvem

Para ambientes de segurança de carga de trabalho **baseados nos EUA**:

Protocolo	Porta	Fonte	Destino	Descrição
TCP	443	Agente de segurança de carga de trabalho	<site_name>.cs01.cloudinsights.NetApp.com <site_name>.c01.cloudinsights.NetApp.com <site_name>.c02.cloudinsights.NetApp.com	Acesso ao Data Infrastructure Insights
TCP	443	Agente de segurança de carga de trabalho	gateway.c01.cloudinsights.netapp.com agentlogin.cs01.cloudinsights.netapp.com	Acesso aos serviços de autenticação

Para ambientes de segurança de carga de trabalho **baseados na Europa**:

Protocolo	Porta	Fonte	Destino	Descrição
TCP	443	Agente de segurança de carga de trabalho	<site_name>.cs01-eu-1.cloudinsights.NetApp.com <site_name>.c01-eu-1.cloudinsights.NetApp.com <site_name>.c02-eu-1.cloudinsights.NetApp.com	Acesso ao Data Infrastructure Insights
TCP	443	Agente de segurança de carga de trabalho	gateway.c01.cloudinsights.NetApp.com agentlogin.cs01-eu-1.cloudinsights.NetApp.com	Acesso aos serviços de autenticação

Para ambientes de segurança de workload **baseados na APAC**:

Protocolo	Porta	Fonte	Destino	Descrição
TCP	443	Agente de segurança de carga de trabalho	<site_name>.cs01-ap-1.cloudinsights.NetApp.com <site_name>.c01-ap-1.cloudinsights.NetApp.com <site_name>.c02-ap-1.cloudinsights.NetApp.com	Acesso ao Data Infrastructure Insights
TCP	443	Agente de segurança de carga de trabalho	gateway.c01.cloudinsights.NetApp.com agentlogin.cs01-ap-1.cloudinsights.NetApp.com	Acesso aos serviços de autenticação

Regras na rede

Protocolo	Porta	Fonte	Destino	Descrição
TCP	389 (LDAP) 636 (LDAPS/start-tls)	Agente de segurança de carga de trabalho	URL do servidor LDAP	Ligar ao LDAP

Protocolo	Porta	Fonte	Destino	Descrição
TCP	443	Agente de segurança de carga de trabalho	Endereço IP do gerenciamento do cluster ou SVM (dependendo da configuração do coletor do SVM)	Comunicação de API com o ONTAP
TCP	35000 - 55000	Endereços IP de LIF de dados SVM	Agente de segurança de carga de trabalho	Comunicação do ONTAP para o agente de segurança de carga de trabalho para eventos Fpolicy. Essas portas devem ser abertas para o Agente de Segurança de carga de trabalho para que o ONTAP envie eventos para ele, incluindo qualquer firewall no próprio Agente de Segurança de carga de trabalho (se presente). OBSERVE que você não precisa reservar todos dessas portas, mas as portas que você reserva para isso devem estar dentro desse intervalo. Recomenda-se começar reservando cerca de 100 portas e aumentando, se necessário.
TCP	7	Agente de segurança de carga de trabalho	Endereços IP de LIF de dados SVM	ECHO de LIFs de dados de agente para SVM
SSH	22	Agente de segurança de carga de trabalho	Gerenciamento de clusters	Necessário para bloqueio de usuários CIFS/SMB.

Dimensionamento do sistema

Consulte "[Verificador de taxa de eventos](#)" a documentação para obter informações sobre dimensionamento.

Instalação do Agente de Segurança de carga de trabalho

A Segurança da carga de trabalho (anteriormente Cloud Secure) coleta dados de atividade do usuário usando um ou mais agentes. Os agentes se conectam a dispositivos no local e coletam dados que são enviados para a camada SaaS de segurança do workload para análise. ["Requisitos do agente"](#) Consulte para configurar uma VM de agente.

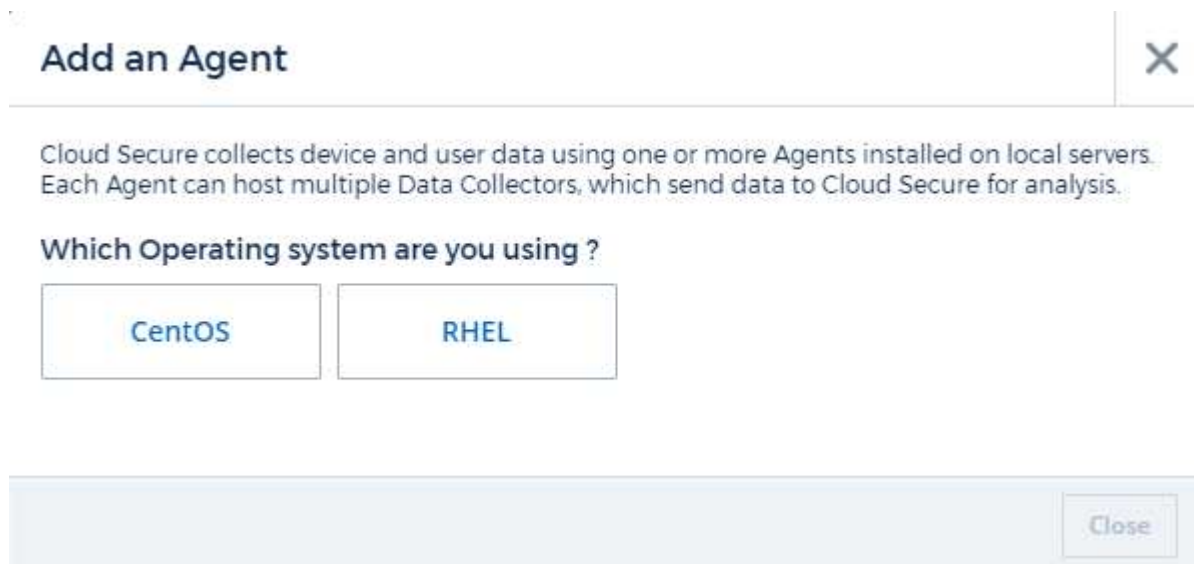
Antes de começar

- O privilégio sudo é necessário para instalação, execução de scripts e desinstalação.
- Durante a instalação do agente, um usuário local `cssys` e um grupo local `cssys` são criados na máquina. Se as configurações de permissão não permitirem a criação de um usuário local e, em vez disso, exigirem o Active Directory, um usuário com o nome de usuário `cssys` deve ser criado no servidor do Active Directory.
- Você pode ler sobre a segurança do Data Infrastructure Insights ["aqui"](#).

Etapas para instalar o agente

1. Inicie sessão como Administrador ou proprietário de conta no ambiente de Segurança de carga de trabalho.
2. Selecione **Collectors > Agents > Agent**

O sistema exibe a página Adicionar um agente:



3. Verifique se o servidor do agente atende aos requisitos mínimos do sistema.
4. Para verificar se o servidor de agente está executando uma versão suportada do Linux, clique em *versões suportadas (i)*.
5. Se a rede estiver usando o servidor proxy, defina os detalhes do servidor proxy seguindo as instruções na seção Proxy.

Configuração de rede

Execute os seguintes comandos no sistema local para abrir portas que serão usadas pelo Workload Security. Se houver um problema de segurança em relação ao intervalo de portas, você pode usar um intervalo de portas menor, por exemplo `35000:35100`. Cada SVM usa duas portas.

Passos

1. `sudo firewall-cmd --permanent --zone=public --add-port=35000-55000/tcp`
2. `sudo firewall-cmd --reload`

Siga os próximos passos de acordo com a sua plataforma:

- CentOS 7.x / RHEL 7.x*:

1. `sudo iptables-save | grep 35000`

Saída da amostra:

```
-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` (Para CentOS 8)

Saída da amostra:

```
35000-55000/tcp
```

"Fixar" um agente na versão atual

Por padrão, o Data Infrastructure Insights Workload Security atualiza os agentes automaticamente. Alguns clientes podem desejar pausar a atualização automática, o que deixa um Agente em sua versão atual até que uma das seguintes situações ocorra:

- O cliente retoma atualizações automáticas do agente.
- 30 dias se passaram. Observe que os 30 dias começam no dia da atualização mais recente do agente, e não no dia em que o agente é pausado.

Em cada um desses casos, o agente será atualizado na próxima atualização de Segurança de carga de trabalho.

Para pausar ou retomar atualizações automáticas de agentes, use as APIs `cloudsecure_config.agents`:

cloudsecure_config.agents



GET	/v1/cloudsecure/agents	Retrieve all agents.	🔒
POST	/v1/cloudsecure/agents/configuration	Pin all agents under tenant	🔒
DELETE	/v1/cloudsecure/agents/configuration	Unpin all agents under tenant	🔒
POST	/v1/cloudsecure/agents/{agentId}/configuration	Pin an agent under tenant	🔒
DELETE	/v1/cloudsecure/agents/{agentId}/configuration	Unpin an agent under tenant	🔒
GET	/v1/cloudsecure/agents/{agentUuid}	Retrieve an agent by agentUuid.	🔒

Observe que pode levar até cinco minutos para que a ação de pausa ou retomada entre em vigor.

Você pode exibir suas versões atuais do Agente na página **Segurança de carga de trabalho > coletores**, na guia **agentes**.

Installed Agents (15)

Name ↑	IP Address	Version	Status
agent-1396	10.128.218.124	1.625.0	Connected

Solução de problemas de erros do agente

Problemas conhecidos e suas resoluções são descritos na tabela a seguir.

Problema:	Resolução:
A instalação do agente falha ao criar a pasta /opt/NetApp/cloudsecure/Agent/logs/agent.log e o arquivo install.log não fornece informações relevantes.	Esse erro ocorre durante o bootstrapping do agente. O erro não é registrado em arquivos de log porque ocorre antes que o logger seja inicializado. O erro é redirecionado para a saída padrão e é visível no log de serviço usando o <code>journalctl -u cloudsecure-agent.service</code> comando. Este comando pode ser usado para solucionar o problema ainda mais. est
A instalação do agente falha com 'esta distribuição linux não é suportada. Sair da instalação'.	Esse erro aparece quando você tenta instalar o Agente em um sistema não suportado. "Requisitos do agente" Consulte .
Falha na instalação do agente com o erro: "-bash: Unzip: Comando not found"	Instale o descompacte e execute o comando de instalação novamente. Se o Yum estiver instalado na máquina, tente "yum install unzip" para instalar o software deszip. Depois disso, copie novamente o comando da IU de instalação do agente e cole-o na CLI para executar a instalação novamente.

Problema:	Resolução:
<p>O agente foi instalado e estava em execução. No entanto, o agente parou de repente.</p>	<p>SSH para a máquina Agent. Verifique o status do serviço do agente através <code>sudo systemctl status cloudsecure-agent.service`do .</code> 1. Verifique se os logs mostram uma mensagem "Falha ao iniciar o serviço daemon de Segurança do Workload" . 2. Verifique se o usuário <code>cssys</code> existe ou não na máquina Agente. Execute os seguintes comandos um por um com permissão <code>root</code> e verifique se o usuário e o grupo <code>cssys</code> existem.</p> <pre> `sudo id cssys sudo groups cssys </pre> <p>3. Se nenhuma existir, uma política de monitorização centralizada pode ter eliminado o utilizador <code>cssys</code>. 4. Crie o usuário e o grupo <code>cssys</code> manualmente executando os seguintes comandos.</p> <pre> sudo useradd cssys sudo groupadd cssys </pre> <p>5. Reinicie o serviço do agente depois disso executando o seguinte comando:</p> <pre> sudo systemctl restart cloudsecure-agent.service </pre> <p>6. Se ainda não estiver em execução, verifique as outras opções de resolução de problemas.</p>
<p>Não é possível adicionar mais de 50 coletores de dados a um agente.</p>	<p>Apenas 50 coletores de dados podem ser adicionados a um Agente. Isso pode ser uma combinação de todos os tipos de coletor, por exemplo, ative Directory, SVM e outros coletores.</p>
<p>A IU mostra que o Agente está no estado NÃO LIGADO.</p>	<p>Etapas para reiniciar o Agente. 1. SSH para a máquina Agent. 2. Reinicie o serviço do agente depois disso executando o seguinte comando:</p> <pre> sudo systemctl restart cloudsecure-agent.service </pre> <p>3. Verifique o status do serviço do agente através <code>`sudo systemctl status cloudsecure-agent.service`do .</code> 4. O agente deve ir para o estado CONETADO.</p>
<p>A VM do agente está atrás do proxy Zscaler e a instalação do agente está falhando. Devido à inspeção SSL do proxy Zscaler, os certificados de Segurança da carga de trabalho são apresentados à medida que são assinados pela Zscaler CA para que o agente não confie na comunicação.</p>	<p>Desative a inspeção SSL no proxy Zscaler para o url <code>*.cloudinsights.NetApp.com</code>. Se o Zscaler fizer a inspeção SSL e substituir os certificados, o Workload Security não funcionará.</p>

Problema:	Resolução:
<p>Durante a instalação do agente, a instalação trava após o desbloqueio.</p>	<p>O comando "chmod 755 -RF" está falhando. O comando falha quando o comando de instalação do agente está sendo executado por um usuário sudo não-root que tem arquivos no diretório de trabalho, pertencentes a outro usuário, e as permissões desses arquivos não podem ser alteradas. Devido ao comando chmod com falha, o resto da instalação não é executado. 1. Crie um novo diretório chamado "cloudsecure". 2. Vá para esse diretório. 3. Copie e cole o comando completo de instalação "token....." e pressione ENTER. 4. A instalação deve ser capaz de prosseguir.</p>
<p>Se o agente ainda não conseguir se conectar ao SaaS, abra um caso com o suporte da NetApp. Forneça o número de série do Data Infrastructure Insights para abrir um caso e anexe logs ao caso, conforme observado.</p>	<p>Para anexar logs ao caso: 1. Execute o seguinte script com permissão root e compartilhe o arquivo de saída (cloudsecure-Agent-sympats.zip). A. /opt/NetApp/cloudsecure/Agent/bin/cloudsecure-agent-symptom-collector.sh 2. Execute os seguintes comandos um a um com permissão root e compartilhe a saída. a. id cssys b. Groups cssys c. Cat /etc/os-release</p>
<p>O script cloudsecure-agent-symptom-collector.sh falha com o seguinte erro. /Opt/NetApp/cloudsecure/Agent/bin/cloudsecure-agent-symptom-collector.sh coletando log de serviço coletando logs de aplicativos coletando configurações de agentes tomando snapshot de status de serviço tomando snapshot da estrutura de diretórios de agentes..... /Opt/NetApp/cloudsecure/Agent/bin/cloudsecure-Agent-sintoma-Collector.sh: Linha 52: Zip: ERRO de comando não encontrado: Falha ao criar /tmp/cloudsecure-agent-symptoms.zip</p>	<p>A ferramenta zip não está instalada. Instale a ferramenta zip executando o comando "yum install zip". Em seguida, execute o cloudsecure-agent-symptom-collector.sh novamente.</p>
<p>Falha na instalação do agente com useradd: Não é possível criar diretório /home/cssys</p>	<p>Esse erro pode ocorrer se o diretório de login do usuário não puder ser criado em /home, devido à falta de permissões. A solução alternativa seria criar o usuário cssys e adicionar seu diretório de login manualmente usando o seguinte comando: <i>Sudo useradd user_name -m -d home_DIR -m</i> :criar o diretório home do usuário se ele não existir. -D : o novo usuário é criado usando home_DIR como o valor para o diretório de login do usuário. Por exemplo, <i>sudo useradd cssys -m -d /cssys</i>, adiciona um usuário cssys e cria seu diretório de login sob root.</p>

Problema:	Resolução:
<p>O agente não está em execução após a instalação. <code>Systemctl status cloudsecure-agent.service</code> NetApp 25889 12:26 126 1 mostra o seguinte: [Root at demo] no. <code>Systemctl status cloudsecure-agent.service agent.service 25889 126 1 03 21 cloudsecure-agent.service – Workload Agente de Segurança Serviço Daemon carregado: Carregado (/usr/lib/systemd/system/cloudsecure-agent.service; 126 03 21 cloudsecure-agent.service: 12:26 ativado; predefinição do fornecedor: Desativado) Ativo: Ativando (auto-restart) (resultado: Exit-code) desde Tue 2s-08-03 21:12:26 PDT; 2021 Aug 03 21:12:26 demo systemd[1]: cloudsecure-agent.service falhou.</code></p>	<p>Isso pode estar falhando porque o usuário <code>cssys</code> pode não ter permissão para instalar. Se <code>/opt/NetApp</code> for uma montagem NFS e se o usuário <code>cssys</code> não tiver acesso a essa pasta, a instalação falhará. <code>Cssys</code> é um usuário local criado pelo instalador do Workload Security que pode não ter permissão para acessar o compartilhamento montado. Você pode verificar isso tentando acessar <code>/opt/NetApp/cloudsecure/Agent/bin/cloudsecure-Agent</code> usando <code>cssys</code> usuário. Se retornar "permissão negada", a permissão de instalação não está presente. Em vez de uma pasta montada, instale em um diretório local para a máquina.</p>
<p>O agente foi inicialmente conetado através de um servidor proxy e o proxy foi definido durante a instalação do Agente. Agora, o servidor proxy mudou. Como a configuração do proxy do Agente pode ser alterada?</p>	<p>Você pode editar o <code>agent.properties</code> para adicionar os detalhes do proxy. Siga estes passos: 1. Mude para a pasta que contém o arquivo de propriedades: <code>cd /opt/NetApp/cloudsecure/conf</code> 2. Usando seu editor de texto favorito, abra o arquivo <code>agent.properties</code> para edição. 3. Adicione ou modifique as seguintes linhas: <code>AGENT_PROXY_HOST scspa1950329001.vm.NetApp.com</code> <code>AGENT_PROXY_PORT 80</code> <code>AGENT_PROXY_USER pass1234</code> 4. Salve o arquivo. 5. Reinicie o agente: <code>Sudo systemctl restart cloudsecure-agent.service</code></p>

Excluindo um agente de segurança de carga de trabalho

Quando você exclui um agente de segurança de carga de trabalho, todos os coletores de dados associados ao agente devem ser excluídos primeiro.

Excluindo um agente



A exclusão de um agente exclui todos os coletores de dados associados ao agente. Se você pretende configurar os coletores de dados com um agente diferente, você deve criar um backup das configurações do Data Collector antes de excluir o Agente.

Antes de começar

1. Certifique-se de que todos os coletores de dados associados ao agente sejam excluídos do portal Workload Security.

Nota: Ignore esta etapa se todos os coletores associados estiverem no estado PARADO.

Etapas para excluir um agente:

1. SSH na VM do agente e execute o seguinte comando. Quando solicitado, digite "y" para continuar.

```
sudo /opt/netapp/cloudsecure/agent/install/cloudsecure-agent-
uninstall.sh
Uninstall CloudSecure Agent? [y|N]:
```

2. Clique em **Workload Security > Collectors > Agents**

O sistema exibe a lista de agentes configurados.

3. Clique no menu de opções para o agente que você está excluindo.

4. Clique em **Excluir**.

O sistema exibe a página **Excluir agente**.

5. Clique em **Excluir** para confirmar a exclusão.

Configurando um Coletor de diretório de usuários do ativo Directory (AD)

A Segurança da carga de trabalho pode ser configurada para coletar atributos de usuário de servidores do ativo Directory.

Antes de começar

- Você deve ser um Administrador do Data Infrastructure Insights ou um proprietário de conta para executar esta tarefa.
- Você deve ter o endereço IP do servidor que hospeda o servidor ativo Directory.
- Um agente deve ser configurado antes de configurar um conector do diretório de usuários.

Passos para configurar um Coletor de diretório de usuários

1. No menu Workload Security, clique em: **Collectors > User Directory Collectors > User Directory Collector** e selecione **ativo Directory**

O sistema exibe a tela Adicionar diretório do usuário.

Configure o Coletor de diretório de usuários inserindo os dados necessários nas seguintes tabelas:

Nome	Descrição
Nome	Nome exclusivo para o diretório do usuário. Por exemplo <i>GlobalADCollector</i>
Agente	Selecione um agente configurado na lista
Nome de domínio/IP do servidor	Endereço IP ou nome de domínio totalmente qualificado (FQDN) do servidor que hospeda o diretório ativo
Nome da floresta	Nível de floresta da estrutura do diretório. O nome da floresta permite ambos os seguintes formatos: <i>X.y.z</i> > nome de domínio direto como você o tem no SVM. [Exemplo: <i>hq.companyname.com</i>] <i>_DC,DC_DC_com</i>] ou você pode especificar como o seguinte: <i>_Ou NetApp <username> <engineering></i>

Vincular DN	Usuário autorizado a pesquisar o diretório. Por exemplo: <i>username@companyname.com</i> ou <i>username@domainname.com</i> além disso, a permissão de domínio somente leitura é necessária. O usuário deve ser um membro do grupo <i>Segurança Controladores de domínio somente leitura</i> .
Palavra-passe BIND	Senha do servidor de diretório (ou seja, senha para nome de usuário usado no DN de vinculação)
Protocolo	ldap, ldaps, ldap-start-tls
Portas	Selecione a porta

Insira os seguintes atributos necessários do Directory Server se os nomes de atributo padrão tiverem sido modificados no active Directory. Na maioria das vezes, esses nomes de atributos são *not* modificados no active Directory, caso em que você pode simplesmente prosseguir com o nome do atributo padrão.

Atributos	Nome do atributo no Directory Server
Nome de exibição	nome
SID	objectsid
Nome de utilizador	SAMAccountName

Clique em incluir atributos opcionais para adicionar qualquer um dos seguintes atributos:

Atributos	Nome do atributo no servidor de diretório
Endereço de e-mail	e-mail
Número de telefone	número de telefone
Função	título
País	co
Estado	estado
Departamento	departamento
Foto	thumbnailphoto
ManagerDN	gerente
Grupos	Membro Of

Testando a configuração do coletor do diretório de usuários

Você pode validar permissões de Usuário LDAP e Definições de Atributo usando os seguintes procedimentos:

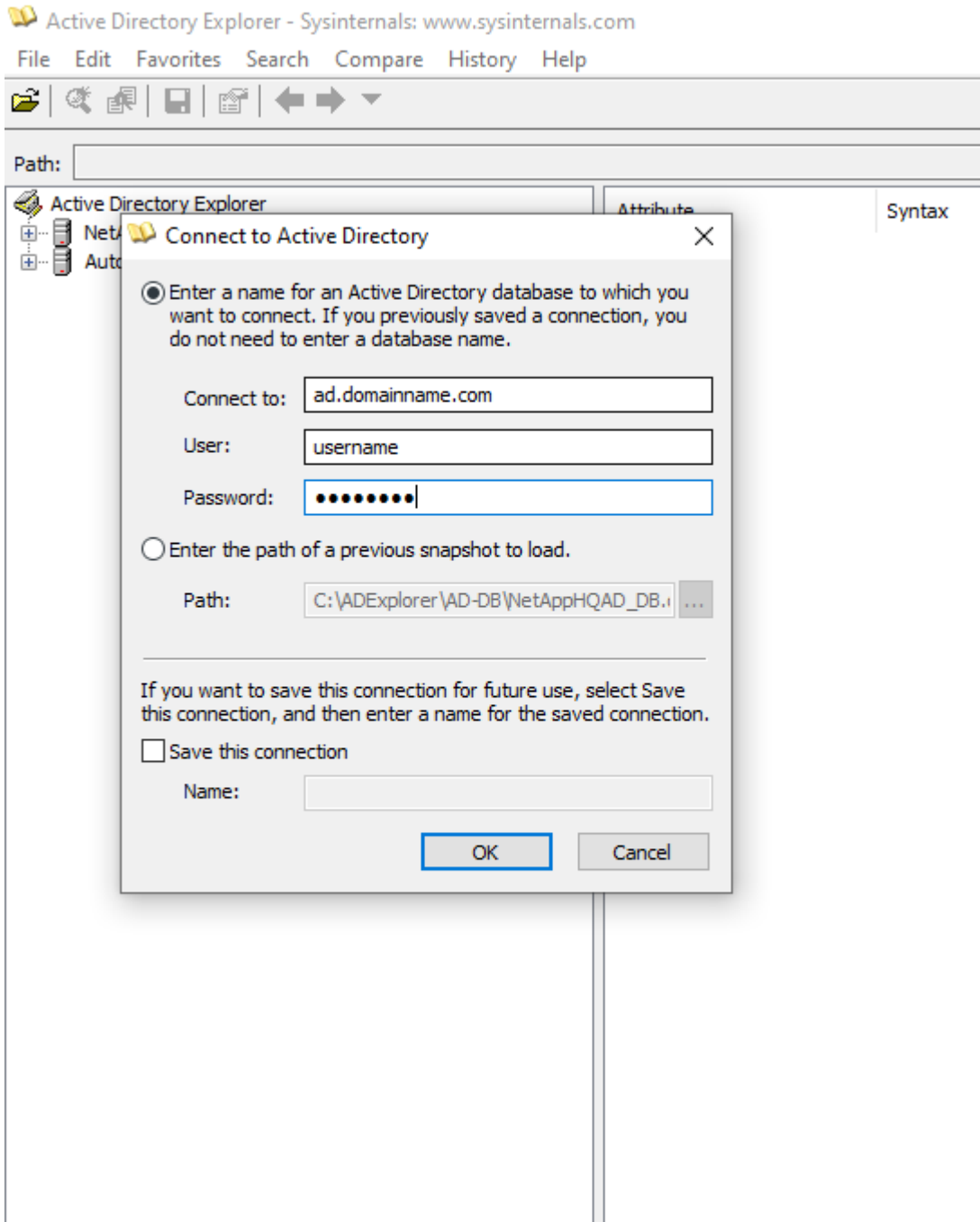
- Use o seguinte comando para validar a permissão de usuário LDAP de segurança de workload:

```
ldapsearch -o ldif-wrap=no -LLL -x -b "dc=netapp,dc=com" -h 10.235.40.29 -p 389 -D Administrator@netapp.com -W
```

- Use o AD Explorer para navegar em um banco de dados do AD, exibir propriedades e atributos de objetos, exibir permissões, exibir o esquema de um objeto, executar pesquisas sofisticadas que você pode

salvar e executar novamente.

- Instale "Explorador de ANÚNCIOS" em qualquer máquina Windows que possa se conectar ao servidor AD.
- Conecte-se ao servidor AD usando o nome de usuário/senha do servidor de diretório AD.



Solução de problemas de erros de configuração do coletor do diretório do usuário

A tabela a seguir descreve problemas conhecidos e resoluções que podem ocorrer durante a configuração do coletor:

Problema:	Resolução:
Adicionar um conector do diretório de usuários resulta no estado "erro". O erro diz: "Credenciais inválidas fornecidas para o servidor LDAP".	Nome de utilizador ou palavra-passe incorretos fornecidos. Edite e forneça o nome de usuário e a senha corretos.
Adicionar um conector do diretório de usuários resulta no estado "erro". Erro diz: "Falha ao obter o objeto correspondente a DN"	Nome da floresta incorreto fornecido. Edite e forneça o nome correto da floresta.
Os atributos opcionais do usuário de domínio não estão aparecendo na página Perfil de usuário de Segurança de carga de trabalho.	Isso provavelmente se deve a uma incompatibilidade entre os nomes de atributos opcionais adicionados no CloudSecure e os nomes de atributos reais no ative Directory. Edite e forneça o(s) nome(s) do atributo opcional correto(s).
Coletor de dados no estado de erro com "Falha ao recuperar usuários LDAP. Motivo da falha: Não é possível conectar no servidor, a conexão é nula"	Reinicie o coletor clicando no botão <i>Restart</i> .
Adicionar um conector do diretório de usuários resulta no estado "erro".	Certifique-se de que forneceu valores válidos para os campos obrigatórios (servidor, nome da floresta, bind-DN, bind-Password). Certifique-se de que a entrada BIND-DN é sempre fornecida como "Administrador <domain_forest_name>" ou como uma conta de usuário com Privileges de administrador de domínio.
Adicionar um conector do diretório de usuários resulta no estado "TENTAR NOVAMENTE". Mostra o erro "não é possível definir o estado do comando Collector,Reason TCP [Connect(localhost:35012,None,List(),some(,seconds),true)] falhou por causa de java.net.ConnectionException:Connection recusado."	IP ou FQDN incorreto fornecido para o servidor AD. Edite e forneça o endereço IP ou FQDN correto.
Adicionar um conector do diretório de usuários resulta no estado "erro". O erro diz: "Falha ao estabelecer a conexão LDAP".	IP ou FQDN incorreto fornecido para o servidor AD. Edite e forneça o endereço IP ou FQDN correto.
Adicionar um conector do diretório de usuários resulta no estado "erro". O erro diz: "Falha ao carregar as configurações. Motivo: A configuração da fonte de dados tem um erro. Razão específica: /Connector/conf/application.conf: 70: LDAP.Idap-port tem STRING de tipo em vez DE NÚMERO"	Valor incorreto para a porta fornecida. Tente usar os valores de porta padrão ou o número de porta correto para o servidor AD.
Comecei com os atributos obrigatórios, e funcionou. Depois de adicionar os opcionais, os dados de atributos opcionais não são obtidos do AD.	Isso provavelmente se deve a uma incompatibilidade entre os atributos opcionais adicionados no CloudSecure e os nomes de atributos reais no ative Directory. Edite e forneça o nome do atributo obrigatório ou opcional correto.
Depois de reiniciar o coletor, quando acontecerá a sincronização AD?	A sincronização DE ANÚNCIOS ocorrerá imediatamente após o coletor ser reiniciado. Levará aproximadamente 15 minutos para obter dados do usuário de aproximadamente 300K usuários e é atualizado a cada 12 horas automaticamente.

Problema:	Resolução:
Os dados do usuário são sincronizados do AD para o CloudSecure. Quando os dados serão excluídos?	Os dados do usuário são mantidos para 13months em caso de não atualização. Se o locatário for excluído, os dados serão excluídos.
O conector do diretório do usuário resulta no estado "erro". "O conector está no estado de erro. Nome do serviço: UsersLdap. Motivo da falha: Falha ao recuperar usuários LDAP. Motivo da falha: 80090308: LdapErr: DSID-0C090453, comentário: AcceptSecurityContext error, data 52e, v3839"	Nome da floresta incorreto fornecido. Veja acima como fornecer o nome correto da floresta.
O número de telefone não está a ser preenchido na página de perfil de utilizador.	Isso é provavelmente devido a um problema de mapeamento de atributos com o ativo Directory. 1. Edite o coletor específico do ativo Directory que está obtendo as informações do usuário do ativo Directory. 2. Em atributos opcionais, há um nome de campo "número de telefone" mapeado para o atributo do ativo Directory 'número de telefone'. 4. Agora, use a ferramenta Explorador do ativo Directory conforme descrito acima para navegar no ativo Directory e ver o nome do atributo correto. 3. Certifique-se de que, no ativo Directory, existe um atributo chamado "número de telefone" que tem, de fato, o número de telefone do usuário. 5. Digamos que no ativo Directory foi modificado para "número de telefone". 6. Em seguida, edite o coletor CloudSecure User Directory. Na seção de atributo opcional, substitua 'número de telefone' por 'número de telefone'. 7. Salve o coletor do ativo Directory, o coletor reiniciará e obterá o número de telefone do usuário e exibirá o mesmo na página do perfil do usuário.
Se o certificado de encriptação (SSL) estiver ativado no servidor AD (ativo Directory), o Coletor do diretório de utilizadores de Segurança de carga de trabalho não pode ligar-se ao servidor AD.	Desative a criptografia do AD Server antes de configurar um coletor de diretório de usuários. Uma vez que os detalhes do usuário são obtidos, ele estará lá por 13 meses. Se o servidor AD for desconectado após buscar os detalhes do usuário, os usuários recém-adicionados no AD não serão obtidos. Para buscar novamente, o coletor de diretório do usuário precisa ser conectado ao AD.
Os dados do ativo Directory estão presentes no CloudInsights Security. Deseja excluir todas as informações do usuário do CloudInsights.	Não é possível excluir APENAS as informações do usuário do ativo Directory do CloudInsights Security. Para excluir o usuário, o locatário completo precisa ser excluído.

Configurando um LDAP Directory Server Collector

Você configura o Workload Security para coletar atributos de usuário de servidores LDAP Directory.

Antes de começar

- Você deve ser um Administrador do Data Infrastructure Insights ou um proprietário de conta para executar

Nome de utilizador	uid
--------------------	-----

Clique em incluir atributos opcionais para adicionar qualquer um dos seguintes atributos:

Atributos	Nome do atributo no servidor de diretório
Endereço de e-mail	e-mail
Número de telefone	número de telefone
Função	título
País	co
Estado	estado
Departamento	número de peça
Foto	foto
ManagerDN	gerente
Grupos	Membro Of

Testando a configuração do coletor do diretório de usuários

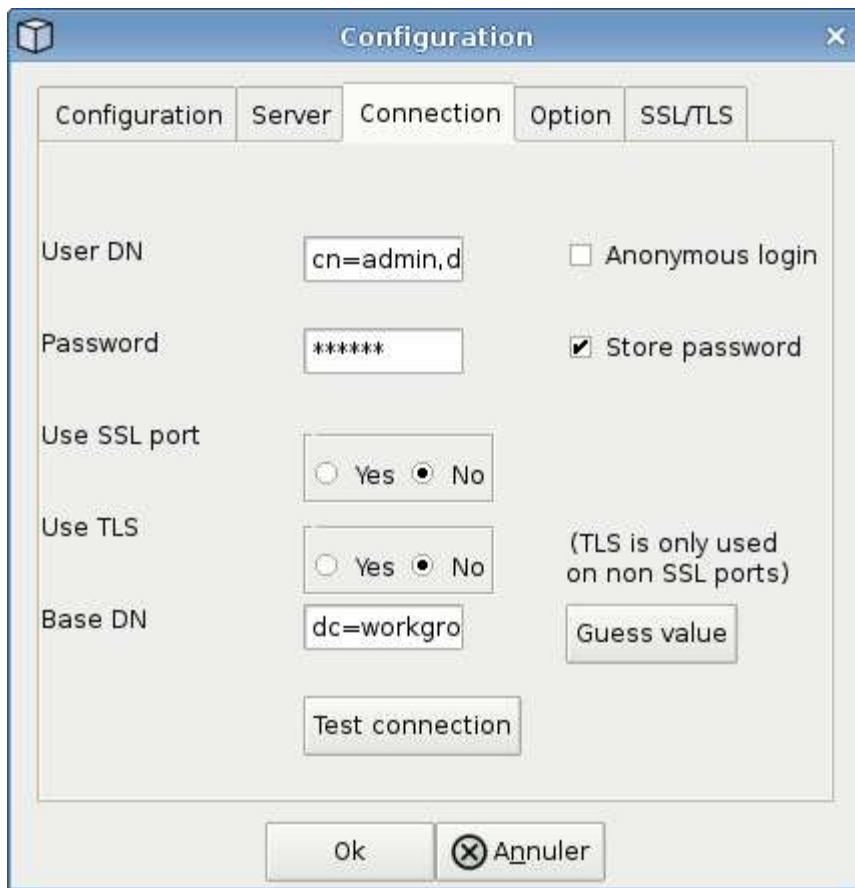
Você pode validar permissões de Usuário LDAP e Definições de Atributo usando os seguintes procedimentos:

- Use o seguinte comando para validar a permissão de usuário LDAP de segurança de workload:

```
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
```

* Use o LDAP Explorer para navegar em um banco de dados LDAP, exibir propriedades e atributos de objetos, exibir permissões, exibir o esquema de um objeto, executar pesquisas sofisticadas que você pode salvar e executar novamente.

- Instale o LDAP Explorer (<http://daptool.sourceforge.net/>) ou o Java LDAP (<http://jxplorer.org/Explorer>) em qualquer máquina Windows que possa se conectar ao servidor LDAP.
- Conecte-se ao servidor LDAP usando o nome de usuário/senha do servidor de diretório LDAP.



Solução de problemas de erros de configuração do coletor de diretório LDAP

A tabela a seguir descreve problemas conhecidos e resoluções que podem ocorrer durante a configuração do coletor:

Problema:	Resolução:
Adicionar um conector de diretório LDAP resulta no estado "erro". O erro diz: "Credenciais inválidas fornecidas para o servidor LDAP".	DN de vinculação ou Senha de vinculação incorreta ou base de pesquisa fornecida. Edite e forneça as informações corretas.
Adicionar um conector de diretório LDAP resulta no estado "erro". Erro diz: "Falha ao obter o objeto correspondente a DN"	Base de pesquisa incorreta fornecida. Edite e forneça o nome correto da floresta.
Os atributos opcionais do usuário de domínio não estão aparecendo na página Perfil de usuário de Segurança de carga de trabalho.	Isso provavelmente se deve a uma incompatibilidade entre os nomes de atributos opcionais adicionados no CloudSecure e os nomes de atributos reais no Active Directory. Os campos são sensíveis a maiúsculas e minúsculas. Edite e forneça o(s) nome(s) do atributo opcional correto(s).
Coletor de dados no estado de erro com "Falha ao recuperar usuários LDAP. Motivo da falha: Não é possível conectar no servidor, a conexão é nula"	Reinicie o coletor clicando no botão <i>Restart</i> .

Problema:	Resolução:
Adicionar um conector de diretório LDAP resulta no estado "erro".	Certifique-se de que forneceu valores válidos para os campos obrigatórios (servidor, nome da floresta, bind-DN, bind-Password). Certifique-se de que a entrada bind-DN é sempre fornecida como
Adicionar um conector de diretório LDAP resulta no estado "TENTAR NOVAMENTE". Mostra o erro "Falha ao determinar a integridade do coletor, portanto, tentar novamente"	Certifique-se de que o IP do servidor e a base de pesquisa estão corretos ///
Ao adicionar o diretório LDAP, o seguinte erro é mostrado: "Falha ao determinar a integridade do coletor dentro de 2 tentativas, tente reiniciar o coletor novamente (Código de erro: AGENT008)"	Certifique-se de que o IP do servidor e a base de pesquisa estão corretos
Adicionar um conector de diretório LDAP resulta no estado "TENTAR NOVAMENTE". Mostra o erro "não é possível definir o estado do comando Collector,Reason TCP [Connect(localhost:35012,None,List(),some(,seconds),true)] falhou por causa de java.net.ConnectionException:Connection recusado."	IP ou FQDN incorreto fornecido para o servidor AD. Edite e forneça o endereço IP ou FQDN correto. ///
Adicionar um conector de diretório LDAP resulta no estado "erro". O erro diz: "Falha ao estabelecer a conexão LDAP".	IP ou FQDN incorreto fornecido para o servidor LDAP. Edite e forneça o endereço IP ou FQDN correto. Ou valor incorreto para a porta fornecida. Tente usar os valores de porta padrão ou o número de porta correto para o servidor LDAP.
Adicionar um conector de diretório LDAP resulta no estado "erro". O erro diz: "Falha ao carregar as configurações. Motivo: A configuração da fonte de dados tem um erro. Razão específica: /Connector/conf/application.conf: 70: LDAP.ldap-port tem STRING de tipo em vez DE NÚMERO"	Valor incorreto para a porta fornecida. Tente usar os valores de porta padrão ou o número de porta correto para o servidor AD.
Comecei com os atributos obrigatórios, e funcionou. Depois de adicionar os opcionais, os dados de atributos opcionais não são obtidos do AD.	Isso provavelmente se deve a uma incompatibilidade entre os atributos opcionais adicionados no CloudSecure e os nomes de atributos reais no ative Directory. Edite e forneça o nome do atributo obrigatório ou opcional correto.
Depois de reiniciar o coletor, quando acontecerá a sincronização LDAP?	A sincronização LDAP ocorrerá imediatamente após o coletor ser reiniciado. Levará aproximadamente 15 minutos para obter dados do usuário de aproximadamente 300K usuários e é atualizado a cada 12 horas automaticamente.
Os dados do usuário são sincronizados do LDAP para o CloudSecure. Quando os dados serão excluídos?	Os dados do usuário são mantidos para 13months em caso de não atualização. Se o locatário for excluído, os dados serão excluídos.

Problema:	Resolução:
O conector de diretório LDAP resulta no estado "erro". "O conector está no estado de erro. Nome do serviço: UsersLdap. Motivo da falha: Falha ao recuperar usuários LDAP. Motivo da falha: 80090308: LdapErr: DSID-0C090453, comentário: AcceptSecurityContext error, data 52e, v3839"	Nome da floresta incorreto fornecido. Veja acima como fornecer o nome correto da floresta.
O número de telefone não está a ser preenchido na página de perfil de utilizador.	Isso é provavelmente devido a um problema de mapeamento de atributos com o Active Directory. 1. Edite o coletor específico do Active Directory que está obtendo as informações do usuário do Active Directory. 2. Em atributos opcionais, há um nome de campo "número de telefone" mapeado para o atributo do Active Directory 'número de telefone'. 4. Agora, utilize a ferramenta Explorador do Active Directory conforme descrito acima para navegar no servidor LDAP Directory e ver o nome do atributo correto. 3. Certifique-se de que no diretório LDAP existe um atributo chamado "número de telefone" que tem realmente o número de telefone do usuário. 5. Digamos que no diretório LDAP ele foi modificado para "número de telefone". 6. Em seguida, edite o coletor CloudSecure User Directory. Na seção de atributo opcional, substitua 'número de telefone' por 'número de telefone'. 7. Salve o coletor do Active Directory, o coletor reiniciará e obterá o número de telefone do usuário e exibirá o mesmo na página do perfil do usuário.
Se o certificado de encriptação (SSL) estiver ativado no servidor AD (Active Directory), o Coletor do diretório de utilizadores de Segurança de carga de trabalho não pode ligar-se ao servidor AD.	Desative a criptografia do AD Server antes de configurar um coletor de diretório de usuários. Uma vez que os detalhes do usuário são obtidos, ele estará lá por 13 meses. Se o servidor AD for desconectado após buscar os detalhes do usuário, os usuários recém-adicionados no AD não serão obtidos. Para buscar novamente, o coletor de diretório do usuário precisa ser conectado ao AD.

Configurando o coletor de dados SVM do ONTAP

O Workload Security usa coletores de dados para coletar dados de acesso de arquivos e usuários de dispositivos.

Antes de começar

- Este coletor de dados é suportado com o seguinte:
 - Data ONTAP 9,2 e versões posteriores. Para obter o melhor desempenho, use uma versão do Data ONTAP superior a 9.13.1.
 - Protocolo SMB versão 3,1 e anterior.
 - Versões NFS até NFS 4,1 com ONTAP 9.15,1 ou posterior, inclusive.

- O FlexGroup é suportado a partir do ONTAP 9 .4 e versões posteriores
- O ONTAP Select é suportado
- Somente SVMs do tipo de dados são compatíveis. SVMs com volumes infinitos não são compatíveis.
- O SVM tem vários subtipos. Destes, apenas *default*, *Sync_source* e *Sync_destination* são suportados.
- Um agente "[tem de ser configurado](#)" antes de poder configurar coletores de dados.
- Certifique-se de ter um conector do diretório de usuário configurado corretamente, caso contrário, os eventos mostrarão nomes de usuário codificados e não o nome real do usuário (como armazenado no ativo Directory) na página "Activity Forensics".
- O ONTAP Persistent Store é suportado a partir de 9.14.1.
- Para um desempenho ideal, você deve configurar o servidor FPolicy para estar na mesma sub-rede que o sistema de armazenamento.
- É necessário adicionar um SVM usando um dos dois métodos a seguir:
 - Usando o IP do cluster, o nome do SVM e o nome de usuário e a senha do gerenciamento de cluster. **este é o método recomendado.**
 - O nome da SVM deve ser exatamente como mostrado no ONTAP e diferencia maiúsculas de minúsculas.
 - Usando o SVM Management IP, Nome de usuário e Senha
 - Se você não puder ou não estiver disposto a usar o nome de usuário e senha completos do gerenciamento do cluster do administrador/SVM, você poderá criar um usuário personalizado com Privileges menor, conforme mencionado na "[Uma nota sobre permissões](#)" seção abaixo. É possível criar esse usuário personalizado para SVM ou acesso a cluster.
 - O você também pode usar um usuário do AD com uma função que tenha pelo menos as permissões de csrole como mencionado na seção "Uma nota sobre permissões" abaixo. Consulte também a "[Documentação do ONTAP](#)".
- Verifique se os aplicativos corretos estão definidos para o SVM executando o seguinte comando:

```
clustershell::> security login show -vserver <vservname> -user-or
-group-name <username>
```

Exemplo de saída:

```
Vserver: svmname
-----
User/Group          Authentication          Acct   Second
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.
```

- Certifique-se de que o SVM tenha um servidor CIFS configurado: Clustershell::> vserver cifs show
O sistema retorna o nome do SVM, o nome do servidor CIFS e os campos adicionais.
- Defina uma senha para o usuário SVM vsadmin. Se estiver usando usuário personalizado ou usuário de

administrador de cluster, pule esta etapa. Clustershell::> security login password -username vsadmin -vserver svmname

- Desbloqueie o usuário do SVM vsadmin para acesso externo. Se estiver usando usuário personalizado ou usuário de administrador de cluster, pule esta etapa. Clustershell::> security login unlock -username vsadmin -vserver svmname
- Certifique-se de que a política de firewall do LIF de dados está definida como 'mgmt' (não 'dados'). Ignore esta etapa se estiver usando um lif de gerenciamento dedicado para adicionar o SVM. Clustershell::> network interface modify -lif <SVM_data_LIF_name> -firewall-policy mgmt
- Quando um firewall está ativado, você deve ter uma exceção definida para permitir tráfego TCP para a porta usando o coletor de dados Data ONTAP.

"Requisitos do agente" Consulte para obter informações de configuração. Isso se aplica a agentes locais e agentes instalados na nuvem.

- Quando um agente é instalado em uma instância do AWS EC2 para monitorar um SVM do Cloud ONTAP, o agente e o storage devem estar na mesma VPC. Se estiverem em VPCs separados, deve haver uma rota válida entre as VPC.

Pré-requisitos para bloqueio de acesso do usuário

Tenha em mente o seguinte durante **"Bloqueio de acesso do usuário"**:

Credenciais de nível de cluster são necessárias para que esse recurso funcione.

Se você estiver usando credenciais de administração de cluster, não serão necessárias novas permissões.

Se você estiver usando um usuário personalizado (por exemplo, *csuser*) com permissões dadas ao usuário, siga as etapas abaixo para conceder permissões ao Workload Security para bloquear o usuário.

Para *csuser* com credenciais de cluster, faça o seguinte na linha de comando ONTAP:

```
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
```

Uma Nota sobre permissões

Permissões ao adicionar via Cluster Management IP:

Se você não puder usar o usuário administrador de gerenciamento de cluster para permitir que a Segurança de carga de trabalho acesse o coletor de dados ONTAP SVM, você poderá criar um novo usuário chamado "csuser" com as funções como mostrado nos comandos abaixo. Use o nome de usuário "csuser" e a senha para "csuser" ao configurar o coletor de dados do Workload Security para usar o Cluster Management IP.

Para criar o novo usuário, faça login no ONTAP com o nome de usuário/senha do administrador de gerenciamento de cluster e execute os seguintes comandos no servidor ONTAP:

```
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 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
```

Permissões ao adicionar via SVM Management IP:

Se você não puder usar o usuário administrador de gerenciamento de cluster para permitir que a Segurança de carga de trabalho acesse o coletor de dados ONTAP SVM, você poderá criar um novo usuário chamado "csuser" com as funções como mostrado nos comandos abaixo. Use o nome de usuário "csuser" e a senha para "csuser" ao configurar o coletor de dados do Workload Security para usar o SVM Management IP.

Para criar o novo usuário, faça login no ONTAP com o nome de usuário/senha do administrador de gerenciamento de cluster e execute os seguintes comandos no servidor ONTAP. Para facilitar, copie esses comandos para um editor de texto e substitua o <vservername> pelo nome do SVM antes e execute esses comandos no ONTAP:

```
security login role create -vserver <vservername> -role csrole -cmddirname
DEFAULT -access none
```



```
security login role create -vserver <vservname> -role csrole -cmddirname
"network interface" -access readonly
security login role create -vserver <vservname> -role csrole -cmddirname
version -access readonly
security login role create -vserver <vservname> -role csrole -cmddirname
volume -access readonly
security login role create -vserver <vservname> -role csrole -cmddirname
vserver -access readonly
```

```
security login role create -vserver <vservname> -role csrole -cmddirname
"vserver fpolicy" -access all
security login role create -vserver <vservname> -role csrole -cmddirname
"volume snapshot" -access all
```

```
security login create -user-or-group-name csuser -application ontapi
-authmethod password -role csrole -vserver <vservname>
security login create -user-or-group-name csuser -application http
-authmethod password -role csrole -vserver <vservname>
```

Modo Protobuf

A Segurança da carga de trabalho configurará o mecanismo FPolicy no modo protobuf quando esta opção estiver ativada nas configurações *Advanced Configuration* do coletor. O modo Protobuf é suportado no ONTAP versão 9,15 e posterior.

Mais detalhes sobre esse recurso podem ser encontrados no ["Documentação do ONTAP"](#).

Permissões específicas são necessárias para o protobuf (algumas ou todas elas podem já existir):

Modo de cluster:

```
security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <cluster_name>
security login create -user-or-group-name csuser -application http
-authmethod password -role csrestrole
```

Modo SVM:

```
security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <svm_name>
security login create -user-or-group-name csuser -application http
-authmethod password -role csrestrole -vserver <svm_name>
```

Permissões para proteção autônoma contra ransomware do ONTAP e acesso à ONTAP negadas

Se você estiver usando credenciais de administração de cluster, não serão necessárias novas permissões.

Se você estiver usando um usuário personalizado (por exemplo, *csuser*) com permissões dadas ao usuário, siga as etapas abaixo para conceder permissões à Segurança de carga de trabalho para coletar informações relacionadas ao ARP do ONTAP.

Para obter mais informações, leia sobre ["Integração com o ONTAP Access negada"](#)

e ["Integração com a proteção autônoma contra ransomware do ONTAP"](#)

Configurar o coletor de dados

Passos para a configuração

1. Faça login como Administrador ou proprietário de conta no seu ambiente Data Infrastructure Insights.
2. Clique em **Workload Security > Collectors > Coletores de dados**

O sistema exibe os coletores de dados disponíveis.

3. Passe o Mouse sobre o bloco **NetApp SVM e clique em * Monitor**.

O sistema exibe a página de configuração do ONTAP SVM. Introduza os dados necessários para cada campo.

Campo	Descrição
Nome	Nome exclusivo para o Data Collector
Agente	Selecione um agente configurado na lista.
Ligar através de IP de gestão para:	Selecione Cluster IP ou SVM Management IP
Endereço IP do gerenciamento de cluster/SVM	O endereço IP do cluster ou do SVM, dependendo da sua seleção acima.
Nome SVM	O Nome do SVM (este campo é obrigatório ao se conectar via IP de cluster)
Nome de utilizador	Nome de usuário para acessar o SVM/cluster ao adicionar via IP de cluster as opções são: 1. Cluster-admin 2. 'csuser' 3. AD-user com papel semelhante ao csuser. Ao adicionar via SVM IP, as opções são: 4. Vsadmin 5. 'csuser' 6. AD-username com função semelhante ao csuser.
Palavra-passe	Senha para o nome de usuário acima
Filtre compartilhamentos/volumes	Escolha se deseja incluir ou excluir compartilhamentos / volumes da coleção de eventos
Introduza nomes de partilha completos para excluir/incluir	Lista de compartilhamentos separados por vírgulas para excluir ou incluir (conforme apropriado) da coleção de eventos
Introduza nomes de volume completos para excluir/incluir	Lista de volumes separados por vírgulas para excluir ou incluir (conforme apropriado) da coleção de eventos

Monitorar o acesso à pasta	Quando marcada, ativa eventos para monitoramento de acesso a pastas. Observe que a pasta criar/renomear e excluir será monitorada mesmo sem essa opção selecionada. Ativar isto aumentará o número de eventos monitorizados.
Definir o tamanho do buffer de envio do ONTAP	Define o tamanho do buffer de envio do Fpolicy do ONTAP. Se uma versão do ONTAP anterior a 9.8p7 for usada e um problema de desempenho for visto, o tamanho do buffer de envio do ONTAP pode ser alterado para obter um desempenho aprimorado do ONTAP. Entre em Contato com o suporte da NetApp se você não vir essa opção e deseja explorá-la.

Depois de terminar

- Na página coletores de dados instalados, use o menu de opções à direita de cada coletor para editar o coletor de dados. Você pode reiniciar o coletor de dados ou editar atributos de configuração do coletor de dados.

Configuração recomendada para MetroCluster

O seguinte é recomendado para o MetroCluster:

1. Conecte dois coletores de dados, um ao SVM de origem e outro ao SVM de destino.
2. Os coletores de dados devem ser conectados por *Cluster IP*.
3. A qualquer momento, um coletor de dados deve estar em execução, outro estará em erro.

O coletor de dados do SVM atual será exibido como *Running*. O coletor de dados do SVM 'parado' atual será exibido como *Error*.

4. Sempre que houver um switchover, o estado do coletor de dados mudará de "execução" para "erro" e vice-versa.
5. Levará até dois minutos para que o coletor de dados se mova do estado de erro para o estado de execução.

Política de Serviço

Se estiver usando a política de serviço com o ONTAP **versão 9.9.1 ou mais recente**, a fim de se conectar ao coletor de origem de dados, o serviço *data-fpolicy-client* será necessário junto com o serviço de dados *data-nfs* e/ou *data-cifs*.

Exemplo:

```
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)
```

Em versões do ONTAP anteriores a 9,9.1, *data-fpolicy-client* não precisam ser definidas.

Play-Pause Data Collector

2 novas operações são agora mostradas no menu kebab do coletor (PAUSA e RETOMADA).

Se o Coletor de dados estiver no estado *Running*, você pode pausar a coleta. Abra o menu "três pontos" para o coletor e SELECIONE PAUSE. Enquanto o coletor está em pausa, nenhum dado é coletado do ONTAP e nenhum dado é enviado do coletor para o ONTAP. Isso significa que nenhum evento do Fpolicy fluirá do ONTAP para o coletor de dados e dali para Insights de infraestrutura de dados.

Observe que se novos volumes, etc. forem criados no ONTAP enquanto o coletor estiver em pausa, a Segurança de carga de trabalho não coletará os dados e esses volumes, etc., não serão refletidos em painéis ou tabelas.

Tenha em mente o seguinte:

- A limpeza de instantâneos não acontecerá de acordo com as configurações configuradas em um coletor pausado.
- Os eventos EMS (como ONTAP ARP) não serão processados em um coletor pausado. Isso significa que, se o ONTAP identificar um ataque de ransomware, a segurança de workloads da infraestrutura de dados não conseguirá adquirir esse evento.
- Os e-mails de notificações de saúde NÃO serão enviados para um coletor em pausa.
- Ações manuais ou automáticas (como captura Instantânea ou bloqueio do usuário) não serão suportadas em um coletor pausado.
- Nas atualizações do agente ou coletor, a VM do agente reinicia/reinicia ou a reinicialização do serviço do agente, um coletor pausado permanecerá no estado *Pausado*.
- Se o coletor de dados estiver no estado *Error*, o coletor não poderá ser alterado para o estado *Paused*. O botão Pausa será ativado somente se o estado do coletor for *Running*.
- Se o agente estiver desconetado, o coletor não poderá ser alterado para o estado *Pausado*. O coletor entrará no estado *stopped* e o botão Pausa será desativado.

Armazenamento persistente

O armazenamento persistente é suportado com o ONTAP 9.14,1 e posterior. Observe que as instruções de nome de volume variam de ONTAP 9.14 a 9,15.

O armazenamento persistente pode ser ativado selecionando a caixa de seleção na página de edição/adição do coletor. Depois de selecionar a caixa de verificação, é apresentado um campo de texto para aceitar o nome do volume. O nome do volume é um campo obrigatório para ativar o armazenamento persistente.

- Para ONTAP 9.14,1, você deve criar o volume antes de ativar o recurso e fornecer o mesmo nome no campo *Nome do volume*. O tamanho de volume recomendado é 16GB.
- Para ONTAP 9.15,1, o volume será criado automaticamente com tamanho 16GB pelo coletor, usando o nome fornecido no campo *Nome do volume*.

Permissões específicas são necessárias para o armazenamento persistente (algumas ou todas elas podem já existir):

Modo de cluster:

```
security login rest-role create -role csrestrole -api  
/api/protocols/fpolicy -access all -vserver <cluster-name>  
security login rest-role create -role csrestrole -api /api/cluster/jobs/  
-access readonly -vserver <cluster-name>
```

Modo SVM:

```
security login rest-role create -role csrestrole -api  
/api/protocols/fpolicy -access all -vserver <vserver-name>  
security login rest-role create -role csrestrole -api /api/cluster/jobs/  
-access readonly -vserver <vserver-name>
```

Solução de problemas

Consulte "[Solução de problemas do SVM Collector](#)" a página para obter dicas de solução de problemas.

Configurando o Cloud Volumes ONTAP e o Amazon FSX para NetApp ONTAP Collector

O Workload Security usa coletores de dados para coletar dados de acesso de arquivos e usuários de dispositivos.

Configuração de armazenamento Cloud Volumes ONTAP

Consulte a documentação do OnCommand Cloud Volumes ONTAP para configurar uma instância do AWS de nó único/HA para hospedar o agente de segurança de carga de trabalho: <https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/index.html>

Após a conclusão da configuração, siga as etapas para configurar o SVM: https://docs.netapp.com/us-en/cloudinsights/task_add_collector_svm.html

Plataformas compatíveis

- Cloud Volumes ONTAP, compatível com todos os fornecedores de serviços de nuvem disponíveis, onde disponível. Por exemplo: Amazon, Azure, Google Cloud.
- ONTAP no FSX

Configuração da Máquina do Agente

A máquina do agente deve ser configurada nas respectivas sub-redes dos provedores de serviços de nuvem. Leia mais sobre o acesso à rede em [requisitos do agente].

Abaixo estão as etapas para a instalação do agente na AWS. Etapas equivalentes, conforme aplicável ao provedor de serviços de nuvem, podem ser seguidas no Azure ou no Google Cloud para a instalação.

Na AWS, siga as etapas a seguir para configurar a máquina a ser usada como agente de segurança de carga de trabalho:

Siga as etapas a seguir para configurar a máquina a ser usada como agente de segurança de carga de

trabalho:

Passos

1. Faça login no console da AWS e navegue até a página de instâncias EC2 e selecione *Launch instance*.
2. Selecione uma AMI RHEL ou CentOS com a versão apropriada, conforme mencionado nesta página: https://docs.netapp.com/us-en/cloudinsights/concept_cs_agent_requirements.html
3. Selecione a VPC e a sub-rede em que a instância do Cloud ONTAP reside.
4. Selecione *T2.xlarge* (4 vcpus e 16 GB de RAM) como recursos alocados.
 - a. Crie a instância EC2.
5. Instale os pacotes Linux necessários usando o gerenciador de pacotes YUM:
 - a. Instale os pacotes Linux nativos *wget* e *unzip*.

Instale o agente de segurança de carga de trabalho

1. Faça login como Administrador ou proprietário de conta no seu ambiente Data Infrastructure Insights.
2. Navegue até Workload Security **Collectors** e clique na guia **Agents**.
3. Clique em *Agente* e especifique RHEL como a plataforma de destino.
4. Copie o comando Instalação do agente.
5. Cole o comando Agent Installation na instância RHEL EC2 na qual você está conectado. Isso instala o agente Workload Security, desde que todos os "Pré-requisitos do agente" sejam atendidos.

Para obter as etapas detalhadas, consulte este xref.:/ https://docs.NetApp.com/US-en/cloudinsights/task_cs_add_Agent.html

Solução de problemas

Problemas conhecidos e suas resoluções são descritos na tabela a seguir.

Problema	Resolução
"Segurança de carga de trabalho: Falha ao determinar o tipo de ONTAP para o coletor de dados do Amazon FxSN" é mostrado pelo coletor de dados. O cliente não consegue adicionar um novo coletor de dados Amazon FSxN ao Workload Security. A conexão com o cluster FSxN na porta 443 do agente está esgotando. Os grupos de segurança do firewall e da AWS têm as regras necessárias habilitadas para permitir a comunicação. Um agente já está implantado e também está na mesma conta da AWS. Esse mesmo agente é usado para conectar e monitorar os dispositivos NetApp restantes (e todos eles estão funcionando).	Resolva esse problema adicionando o segmento de rede fsxadmin LIF à regra de segurança do agente. Permitido todas as portas se você não tiver certeza sobre as portas.

Gerenciamento de usuários

As contas de usuário do Workload Security são gerenciadas por meio do Data Infrastructure Insights.

O Data Infrastructure Insights oferece quatro níveis de conta de usuário: Proprietário da conta, Administrador, Usuário e convidado. Cada conta recebe níveis de permissão específicos. Uma conta de usuário que tenha Privileges de administrador pode criar ou modificar usuários e atribuir a cada usuário uma das seguintes funções de segurança de carga de trabalho:

Função	Acesso à segurança do workload
Administrador	Pode executar todas as funções de Segurança de carga de trabalho, incluindo as de Alertas, Forensics, coletores de dados, políticas de resposta automatizadas e APIs para Segurança de carga de trabalho. Um administrador também pode convidar outros usuários, mas só pode atribuir funções de Segurança de carga de trabalho.
Utilizador	Pode visualizar e gerir Alertas e visualizar Forensics. A função de usuário pode alterar o status de alerta, adicionar uma nota, tirar snapshots manualmente e restringir o acesso do usuário.
Convidado	Pode visualizar Alertas e Forensics. A função convidado não pode alterar o status de alerta, adicionar uma nota, tirar snapshots manualmente ou restringir o acesso do usuário.

Passos

1. Faça login no Workload Security
2. No menu, clique em **Admin > User Management**

Você será encaminhado para a página Gerenciamento de usuários do Data Infrastructure Insights.

3. Selecione a função pretendida para cada utilizador.

Ao adicionar um novo usuário, basta selecionar a função desejada (geralmente Usuário ou convidado).

Mais informações sobre contas de usuário e funções podem ser encontradas na documentação do Data Infrastructure Insights "[Função de utilizador](#)".

Verificador de taxa de eventos SVM (Guia de dimensionamento de agentes)

O Verificador de taxa de eventos é usado para verificar a taxa de eventos combinados NFS/SMB no SVM antes de instalar um coletor de dados ONTAP SVM, para ver quantos SVMs uma máquina pode monitorar. Use o Event Rate Checker como um guia de dimensionamento para ajudar a Planejar seu ambiente de segurança.

Um agente pode suportar até um máximo de 50 coletores de dados.

Requisitos:

- IP do cluster
- Nome de usuário e senha do administrador do cluster



Ao executar esse script, nenhum coletor de dados SVM do ONTAP deve estar em execução para o SVM para o qual a taxa de eventos está sendo determinada.

Passos:

1. Instale o agente seguindo as instruções do CloudSecure.
2. Depois que o agente estiver instalado, execute o script *Server_data_rate_checker.sh* como um usuário sudo:

```
/opt/netapp/cloudsecure/agent/install/svm_event_rate_checker.sh
. Este script requer _sshpass_ para ser instalado na máquina linux. Há duas maneiras de instalá-lo:
```

- a. Execute o seguinte comando:

```
linux_prompt> yum install sshpass
.. Se isso não funcionar, baixe _sshpass_ para a máquina linux a partir da web e execute o seguinte comando:
```

```
linux_prompt> rpm -i sshpass
```

3. Forneça os valores corretos quando solicitado. Veja abaixo um exemplo.
4. O script levará aproximadamente 5 minutos para ser executado.
5. Após a conclusão da execução, o script imprimirá a taxa de eventos do SVM. Você pode verificar a taxa de eventos por SVM na saída do console:

```
"Svm svm_rate is generating 100 events/sec".
```

Cada coletor de dados do ONTAP SVM pode ser associado a um único SVM, ou seja, cada coletor de dados poderá receber o número de eventos gerados por um único SVM.

Tenha em mente o seguinte:

A) Use esta tabela como um guia geral de dimensionamento. Você pode aumentar o número de núcleos e/ou memória para aumentar o número de coletores de dados suportados, até um máximo de 50 coletores de dados:

Configuração da Máquina do Agente	Número de coletores de dados SVM	Taxa máxima de eventos que a máquina do agente pode lidar
4 núcleo, 16GB	10 coletores de dados	20k eventos/seg
4 núcleo, 32GB	20 coletores de dados	20k eventos/seg

B) para calcular o total de eventos, adicione os Eventos gerados para todos os SVMs para esse agente.

C) se o script não for executado durante as horas de pico ou se o tráfego de pico for difícil de prever, mantenha um buffer de taxa de eventos de 30%.

B o C deve ser inferior AA, caso contrário, a máquina do Agente falhará em monitorar.

Em outras palavras, o número de coletores de dados que podem ser adicionados a uma única máquina do agente deve cumprir a fórmula abaixo:

```
Sum of all Event rate of all Data Source Collectors + Buffer Event rate  
of 30% < 20000 events/second
```

Consulte

```
xref:{relative_path}concept_cs_agent_requirements.html["Requisitos do  
agente"]a página para obter pré-requisitos e requisitos adicionais.
```

Exemplo

Digamos que temos três SVMS gerando taxas de eventos de 100, 200 e 300 eventos por segundo, respectivamente.

Aplicamos a fórmula:

```
(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.
```

A saída do console está disponível na máquina Agente no nome do arquivo *fpolicy_stat_<SVM Name>.log* no diretório de trabalho atual.

O script pode dar resultados errôneos nos seguintes casos:

- Credenciais, IP ou nome do SVM incorretos são fornecidos.
- Um fpolicy já existente com o mesmo nome, número de sequência, etc. irá dar erro.
- O script é interrompido abruptamente durante a execução.

Um exemplo de execução de script é mostrado abaixo:

```
[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]#
```

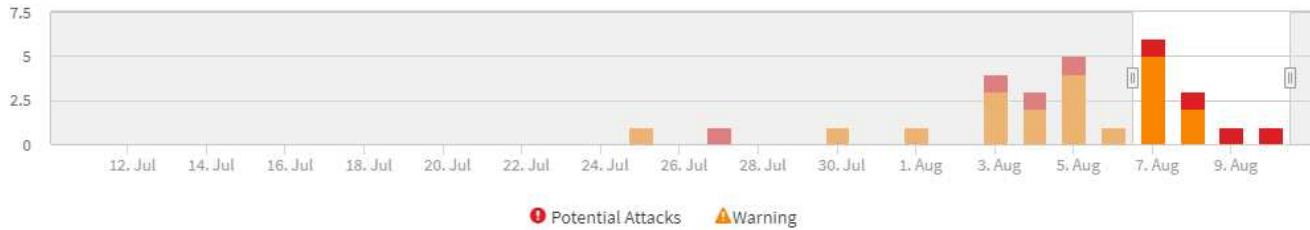
Solução de problemas

Pergunta	Resposta
----------	----------

Se eu executar esse script em um SVM que já esteja configurado para o Workload Security, ele só usará a configuração fpolicy existente no SVM ou configurará uma configuração temporária e executará o processo?	O Event Rate Checker pode ser executado corretamente mesmo para um SVM já configurado para Workload Security. Não deve haver impactos.
Posso aumentar o número de SVMs em que o script pode ser executado?	Sim. Basta editar o script e alterar o número máximo de SVMs de 5 para qualquer número desejável.
Se eu aumentar o número de SVMs, isso aumentará o tempo de execução do script?	Não. O script será executado por um máximo de 5 minutos, mesmo que o número de SVMs seja aumentado.
Posso aumentar o número de SVMs em que o script pode ser executado?	Sim. Você precisa editar o script e alterar o número máximo de SVMs de 5 para qualquer número desejável.
Se eu aumentar o número de SVMs, isso aumentará o tempo de execução do script?	Não. O script será executado por um máximo de 5mins, mesmo que o número de SVMs seja aumentado.
O que acontece se eu executar o Event Rate Checker com um agente existente?	A execução do Event Rate Checker em relação a um agente já existente pode causar um aumento na latência do SVM. Este aumento será temporário por natureza enquanto o verificador de taxa de eventos estiver em execução.

Alertas

A página Alertas de Segurança de carga de trabalho mostra uma linha do tempo de ataques e/ou avisos recentes e permite visualizar detalhes de cada problema.

Filter By Status New ✕ +**Potential Attacks** (3)

Potential Attacks	Detected ↓	Status	User	Evidence	Action Taken
Ransomware Attack	5 hours ago Aug 10, 2020 4:38 AM	New	Iris McIntosh	> 700 Files Encrypted	Snapshots Taken
Ransomware Attack	a day ago Aug 9, 2020 3:51 AM	New	Christy Santos	> 500 Files Encrypted	Snapshots Taken
Ransomware Attack	2 days ago Aug 8, 2020 4:29 AM	New	Safwan Langley	> 700 Files Encrypted	Snapshots Taken

Warnings (7)

Abnormal Behaviour	Detected ↓	Status	User	Change	Action Taken
User Activity Rate	2 days ago Aug 8, 2020 7:49 PM	New	Iris McIntosh	↑ 192.46%	None
User Activity Rate	2 days ago Aug 8, 2020 7:32 PM	New	Jenny Bryan	↑ 73.64%	None
User Activity Rate	3 days ago Aug 7, 2020 8:07 PM	New	Szymon Owen	↑ 189.88%	None

Alerta

A lista Alerta apresenta um gráfico que mostra o número total de potenciais ataques e/ou Avisos que foram levantados no intervalo de tempo selecionado, seguido de uma lista dos ataques e/ou avisos que ocorreram nesse intervalo de tempo. Você pode alterar o intervalo de tempo ajustando os controles deslizantes de hora de início e hora de fim no gráfico.

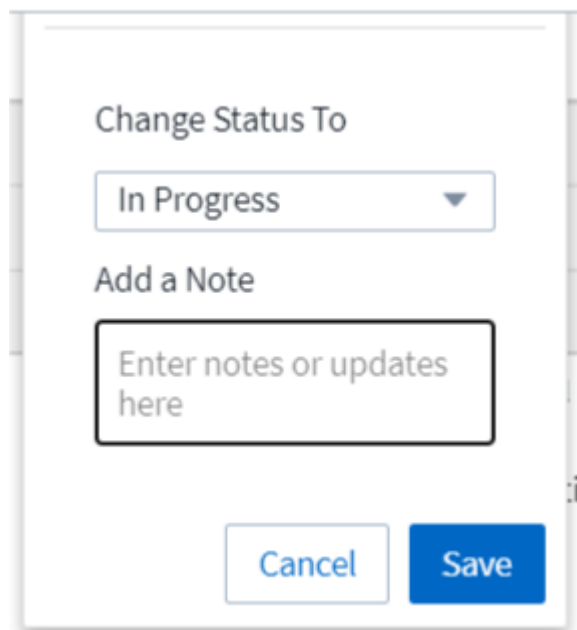
É apresentado o seguinte para cada alerta:

Potenciais ataques:

- O tipo *potential Attack* (por exemplo, ransomware ou Sabotage)
- A data e a hora em que o ataque potencial foi *detetado*
- O *Status* do alerta:
 - **Novo:** Este é o padrão para novos alertas.
 - **Em andamento:** O alerta está sob investigação por um membro da equipe ou membros.
 - **Resolvido:** O alerta foi marcado como resolvido por um membro da equipe.

- **Demitido:** O alerta foi rejeitado como comportamento falso positivo ou esperado.

Um administrador pode alterar o status do alerta e adicionar uma nota para ajudar na investigação.



The image shows a dialog box titled "Change Status To". It contains a dropdown menu with "In Progress" selected. Below the dropdown is a text input field with the placeholder text "Enter notes or updates here". At the bottom of the dialog are two buttons: "Cancel" and "Save".

- O *User* cujo comportamento acionou o alerta
- *Evidência* do ataque (por exemplo, um grande número de arquivos foi criptografado)
- A *Ação tomada* (por exemplo, um instantâneo foi tirado)

Avisos:

- O *comportamento anormal* que acionou o aviso
- A data e a hora em que o comportamento foi *detetado*
- O *Status* do alerta (novo, em andamento, etc.)
- O *User* cujo comportamento acionou o alerta
- Uma descrição do *change* (por exemplo, um aumento anormal no acesso ao arquivo)
- A *Ação tomada*

Opções de filtro

Você pode filtrar os alertas pelo seguinte:

- O *Status* do alerta
- Texto específico na *Nota*
- O tipo de *ataques/Avisos*
- O *User* cujas ações desencadearam o alerta/aviso

A página Detalhes do alerta

Você pode clicar em um link de alerta na página da lista Alertas para abrir uma página de detalhes para o alerta. Os detalhes do alerta podem variar de acordo com o tipo de ataque ou alerta. Por exemplo, uma

página de detalhes do ataque do ransomware pode mostrar as seguintes informações:

Secção de resumo:

- Tipo de ataque (ransomware, sabotagem) e ID de alerta (atribuído pela Workload Security)
- Data e hora em que o ataque foi detetado
- Ação tomada (por exemplo, um instantâneo automático foi feito. A hora do instantâneo é mostrada imediatamente abaixo da secção de resumo))
- Estado (novo, em curso, etc.)

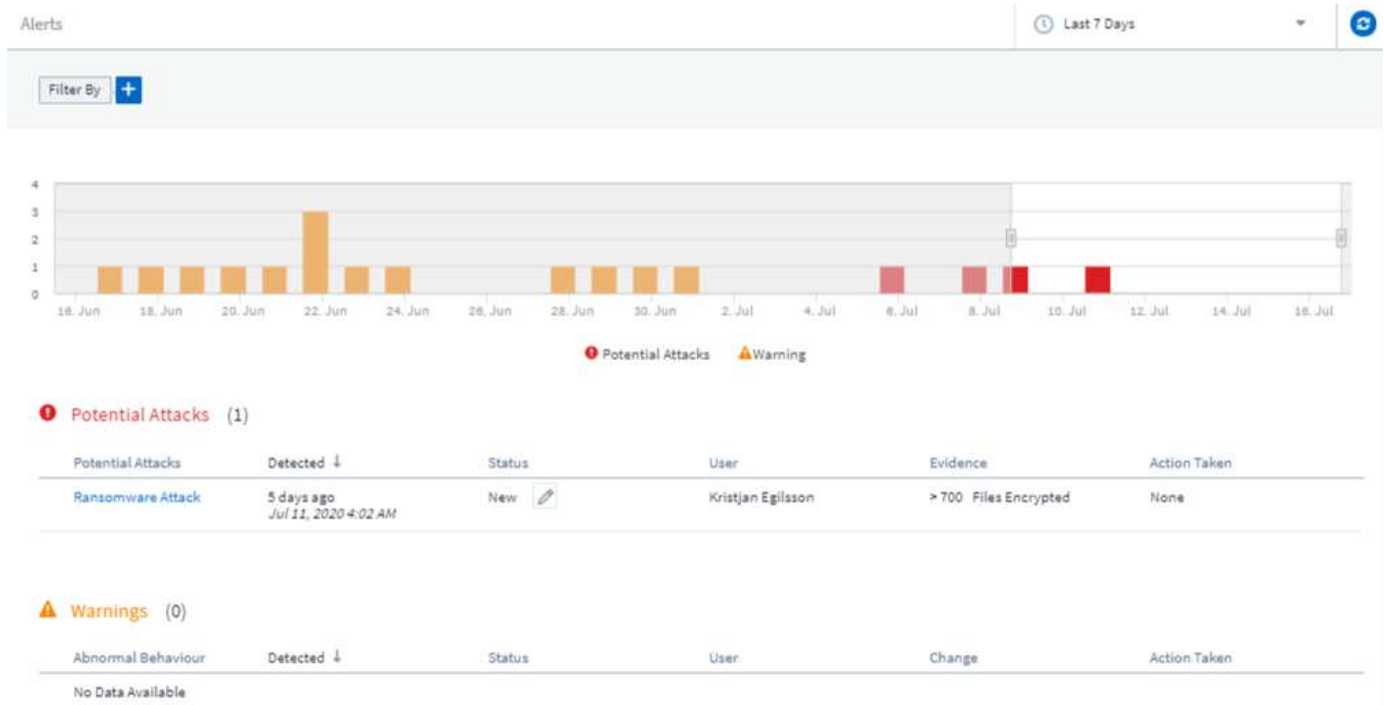
Secção de resultados do ataque:

- Contagens de volumes e arquivos afetados
- Um resumo que acompanha a deteção
- Um gráfico mostrando a atividade do arquivo durante o ataque

Secção utilizadores relacionados:

Esta secção mostra detalhes sobre o usuário envolvido no ataque potencial, incluindo um gráfico de atividade superior para o usuário.

Página de alertas (este exemplo mostra um possível ataque de ransomware):



Página de detalhes (este exemplo mostra um possível ataque de ransomware):



POTENTIAL ATTACK: AL_305
Ransomware Attack

Detected
5 days ago
Jul 11, 2020 4:02 AM

Action Taken
None

Status
New

Total Attack Results

1 Affected Volumes | 0 Deleted Files | 4173 Encrypted Files

4173 Files have been copied, deleted, and potentially encrypted by 1 user account.

This is potentially a sign of ransomware attack.
The extension ".crypt" was added to each file.

Encrypted Files

Activity per minute



Related Users



Kristjan Egilsson
Accountant
Finance

4173
Encrypted Files

Detected
5 days ago
Jul 11, 2020 4:02 AM

Action Taken
None



Username
us035

Email
Egilsson@netapp.com

Phone
387224312607

Department
Finance

Manager
Lyndsey Maddox

Top Activity Types

Activity per minute
Last access location: 10.197.144.115

[View Activity Detail](#)



Faça um instantâneo Ação

O Workload Security protege seus dados tirando automaticamente um snapshot quando uma atividade maliciosa é detetada, garantindo que seus dados sejam copiados com segurança.

Você pode definir "políticas de resposta automatizadas" essa captura instantânea quando um ataque de ransomware ou outra atividade anormal do usuário é detetada. Também pode tirar um instantâneo manualmente a partir da página de alerta.

Instantâneo automático captado:



POTENTIAL ATTACK: AL_307
Ransomware Attack

Detected
4 days ago
Jul 26, 2020 3:38 AM

Action Taken
Snapshots Taken

Status
In Progress

Last snapshots taken by
Amit Schwartz
Jul 30, 2020 2:54 PM

How To:
[Restore Entities](#)

[Re-Take Snapshots](#)

Total Attack Results

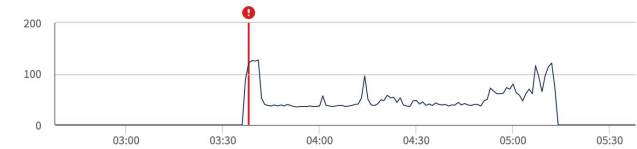
1 Affected Volumes | **0** Deleted Files | **5148** Encrypted Files

5148 Files have been copied, deleted, and potentially encrypted by 1 user account.

This is potentially a sign of ransomware attack. The extension "crypt" was added to each file.

Encrypted Files

Activity per minute



Related Users



Ewen Hall
Developer
Engineering

5148
Encrypted Files

Detected
4 days ago
Jul 26, 2020 3:38 AM

Action Taken
Snapshots Taken

Instantâneo manual:

☰ **Cloud Insights** Abhi Basu Thakur

MONITOR & OPTIMIZE Alerts / **Nabilah Howell had an abnormal change in activity rate** Jul 23, 2020 - Jul 26, 2020
1:44 AM 1:44 AM

Alert Detail

WARNING: AL_306
Nabilah Howell had an abnormal change in activity rate.

Detected
5 days ago
Jul 25, 2020 1:44 PM

Action Taken
None

Status
New

Recommendation: Setup an Automated Response Policy
An Automated Response Policy will trigger measures to contain the damage automatically when a future attack is detected. Try it now.

Take Snapshots
How To:
Restore Entities

Nabilah Howell's Activity Rate Change

Typical	Alert	
122.8 Activities Per Minute	210 Activities Per Minute	↑ 71%

Nabilah Howell's activity rate grew 71% over their typical average.

Activity Rate
Activity per 5 minutes

Notificações de alerta

As notificações por e-mail de alertas são enviadas para uma lista de destinatários de alerta para cada ação no alerta. Para configurar destinatários de alerta, clique em **Admin > notificações** e insira um endereço de e-mail para cada destinatário.

Política de retenção

Os alertas e avisos são mantidos por 13 meses. Os alertas e avisos com mais de 13 meses serão eliminados. Se o ambiente de Segurança de workload for excluído, todos os dados associados ao ambiente também

serão excluídos.

Solução de problemas

Problema:	Tente isto:
Há uma situação em que o ONTAP tira snapshots por hora por dia. Os snapshots do Workload Security (WS) afetarão isso? O instantâneo WS fará o instantâneo por hora local? O instantâneo por hora padrão será interrompido?	Os snapshots de segurança da carga de trabalho não afetarão os instantâneos por hora. Os instantâneos WS não tirarão o espaço instantâneo por hora e isso deverá continuar como antes. O instantâneo por hora padrão não será interrompido.
O que acontecerá se a contagem máxima de instantâneos for atingida no ONTAP?	Se a contagem máxima de instantâneos for atingida, a captura subsequente de instantâneos falhará e o Workload Security mostrará uma mensagem de erro observando que o instantâneo está cheio. O usuário precisa definir políticas de snapshot para excluir os snapshots mais antigos, caso contrário, os snapshots não serão tirados. No ONTAP 9.3 e versões anteriores, um volume pode conter até 255 cópias Snapshot. No ONTAP 9.4 e posterior, um volume pode conter até 1023 cópias snapshot. Consulte a documentação do ONTAP para obter informações "Definição da política de eliminação de instantâneos" sobre .
A segurança do workload não consegue tirar snapshots.	Certifique-se de que a função que está sendo usada para criar snapshots tenha o xref.:/ https://docs.NetApp.com/US-en/cloudinsights/task_add_Collector_svm.html . Certifique-se de que <i>csrole</i> é criado com direitos de acesso adequados para tirar snapshots: Função de login de segurança criar -vserver <vservername> -role csrole -cmddirname "volume snapshot" -acessar tudo
Os snapshots estão falhando em alertas mais antigos em SVMs que foram removidos do Workload Security e posteriormente adicionados novamente. Para novos alertas que ocorrem após a adição da SVM novamente, snapshots são feitos.	Este é um cenário raro. Caso isso ocorra, faça login no ONTAP e tire os snapshots manualmente para os alertas mais antigos.
Na página <i>Detalhes do alerta</i> , a mensagem erro "Falha na última tentativa" é vista abaixo do botão <i>tirar instantâneo</i> . Passar o Mouse sobre o erro exibe "Invoke API comando excedeu o tempo limite para o coletor de dados com id".	Isso pode acontecer quando um coletor de dados é adicionado à segurança de carga de trabalho por meio do IP de gerenciamento de SVM, se o LIF da SVM estiver no estado <i>disabled</i> no ONTAP. Ative o LIF em particular no ONTAP e acione <i>tirar instantâneo manualmente</i> da Segurança da carga de trabalho. A ação Snapshot será então bem-sucedida.

Forense

Forensics - todas as atividades

A página All Activity ajuda você a entender as ações executadas em entidades no

ambiente Workload Security.

Examinando todos os dados de atividade

Clique em **Forensics > Activity Forensics** e clique na guia **All Activity** para acessar a página All Activity. Esta página fornece uma visão geral das atividades do seu inquilino, destacando as seguintes informações:

- Um gráfico mostrando *Histórico de atividades* (com base no intervalo de tempo global selecionado)

Você pode ampliar o gráfico arrastando um retângulo no gráfico. A página inteira será carregada para exibir o intervalo de tempo ampliado. Quando ampliada, é apresentado um botão que permite ao utilizador reduzir o zoom.

- Uma lista dos dados *All Activity*.
- Um grupo por lista suspensa fornecerá a opção de agrupar a atividade por usuários, caminho, tipo de entidade etc.
- Um botão de caminho comum estará disponível acima da tabela em clique da qual podemos obter slide out painel com detalhes de caminho de entidade.

A tabela **All Activity** mostra as seguintes informações. Observe que nem todas essas colunas são exibidas por padrão. Você pode selecionar colunas a serem exibidas clicando no ícone "engrenagem".

- A **hora** que uma entidade foi acessada incluindo o ano, mês, dia e hora do último acesso.
- O **usuário** que acessou a entidade com um link para o "[Informações do utilizador](#)" como um painel deslizante.
- A **atividade** realizada pelo usuário. Os tipos suportados são:
 - **Alterar propriedade do grupo** - a propriedade do grupo é de arquivo ou pasta é alterada. Para obter mais detalhes sobre a propriedade do grupo, consulte "[este link](#)."
 - **Alterar proprietário** - a propriedade do arquivo ou pasta é alterada para outro usuário.
 - **Alterar permissão** - a permissão de arquivo ou pasta é alterada.
 - * Criar* - criar arquivo ou pasta.
 - **Excluir** - Excluir arquivo ou pasta. Se uma pasta for excluída, os eventos *delete* serão obtidos para todos os arquivos dessa pasta e subpastas.
 - **Leia** - o ficheiro é lido.
 - **Leia metadados** - somente na opção de monitoramento de pastas ativada. Será gerado ao abrir uma pasta no Windows ou executando "ls" dentro de uma pasta no Linux.
 - **Renomear** - Renomear arquivo ou pasta.
 - **Write** - os dados são gravados em um arquivo.
 - **Write Metadata** - os metadados do arquivo são escritos, por exemplo, permissão alterada.
 - **Outra alteração** - qualquer outro evento que não esteja descrito acima. Todos os eventos não mapeados são mapeados para o tipo de atividade "outra mudança". Aplicável a ficheiros e pastas.
- O **Path** é *entity path*.
- A pasta de nível **1st (raiz)** é o diretório raiz do caminho da entidade em letras minúsculas.
- A pasta de nível **2nd** é o diretório de segundo nível do caminho da entidade em letras minúsculas.
- A pasta de nível **3rd** é o diretório de terceiro nível do caminho da entidade em letras minúsculas.

- A pasta **4th Level** é o diretório de quarto nível do caminho da entidade em letras minúsculas.
- A extensão **Entity Type**, incluindo entidade (ou seja, arquivo) (.doc, .docx, .tmp, etc.).
- O **dispositivo** onde as entidades residem.
- O **Protocolo** usado para buscar eventos.
- O **caminho original** usado para renomear eventos quando o arquivo original foi renomeado. Esta coluna não está visível na tabela por padrão. Use o seletor de coluna para adicionar essa coluna à tabela.
- O **volume** onde as entidades residem. Esta coluna não está visível na tabela por padrão. Use o seletor de coluna para adicionar essa coluna à tabela.

A seleção de uma linha de tabela abre um painel deslizante com o perfil de usuário em uma guia e a visão geral da atividade e da entidade em outra guia.

The screenshot displays the NetApp Cloud Insights interface for Forensics. The main view shows a table of activity logs with columns for Time, User, Domain, Source IP, and Activity. A filter is applied for 'Noise Reduction' and 'Temporary'. The activity overview panel on the right provides details for a specific activity, including the user profile, activity details (Time, User, Source IP, Activity, Protocol, Volume), and the entity profile (Entity, Type, Path, Folder structure, Last Accessed, Size, Device, and Location).

Time	User	Domain	Source IP	Activity
6 days ago 3 Dec 2024 16:09	ldap:qa2.contrail.com:s-1-5-21-1192448160-1988033612-275769208-495		10.100.20.134	Write
6 days ago 3 Dec 2024 16:09	ldap:qa2.contrail.com:s-1-5-21-1192448160-1988033612-275769208-495		10.100.20.134	Rename
6 days ago 3 Dec 2024 16:09	ldap:qa2.contrail.com:s-1-5-21-1192448160-1988033612-275769208-495		10.100.20.134	Rename
6 days ago 3 Dec 2024 16:09	ldap:qa2.contrail.com:s-1-5-21-1192448160-1988033612-275769208-495		10.100.20.134	Read
6 days ago 3 Dec 2024 16:09	ldap:qa2.contrail.com:s-1-5-21-1192448160-1988033612-275769208-495		10.100.20.134	Write

O método padrão *Group by* é *Activity Forensics*. Se você selecionar um método *Group by* diferente—por exemplo, tipo de entidade—a tabela entidade *Group by* será exibida. Se nenhuma seleção for feita, *Group by All* será exibido.

- A contagem de atividades é apresentada como uma hiperligação; selecionar esta opção irá adicionar o agrupamento selecionado como um filtro. A tabela de atividade será atualizada com base nesse filtro.
- Observe que se você alterar o filtro, alterar o intervalo de tempo ou atualizar a tela, não será possível retornar aos resultados filtrados sem definir o filtro novamente.

Filtragem de dados do histórico de atividades forenses

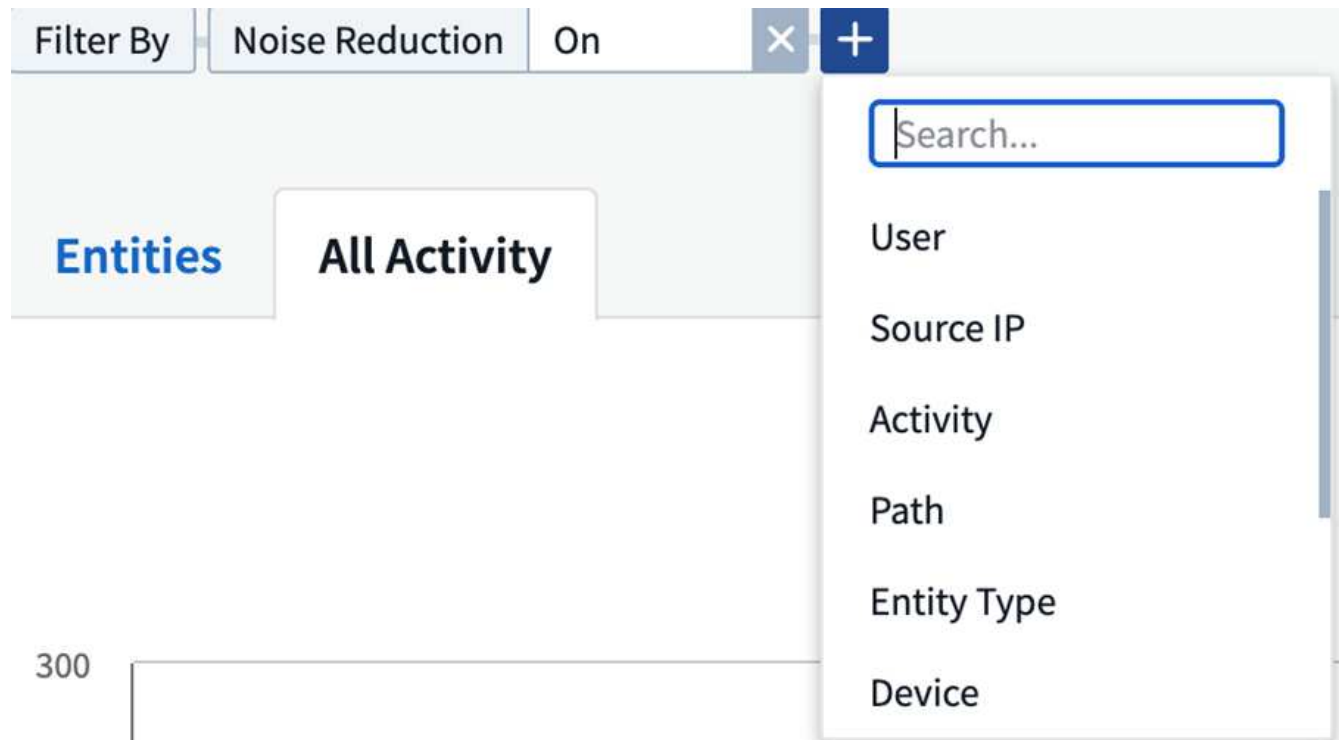
Existem dois métodos que você pode usar para filtrar dados.

- O filtro pode ser adicionado a partir do painel deslizante. O valor é adicionado aos filtros apropriados na

lista acima *Filtrar por*.

- Filtre dados digitando no campo *Filtrar por*.

Selecione o filtro apropriado no topo do widget 'Filtrar por' clicando no botão *[



Introduza o texto de pesquisa

Pressione Enter ou clique fora da caixa de filtro para aplicar o filtro.

Você pode filtrar os dados de atividade Forense pelos seguintes campos:

- O tipo **Activity**.
- **IP de origem** a partir do qual a entidade foi acessada. Você deve fornecer um endereço IP de origem válido em aspas duplas, por exemplo "10,1.1,1". IPs incompletos, como "10,1.1.", "**10,1..***", etc., não funcionarão.
- **Protocolo** para buscar atividades específicas do protocolo.
- **Nome de usuário** do usuário que realiza a atividade. Você precisa fornecer o nome de usuário exato para filtrar. A pesquisa com nome de usuário parcial ou nome de usuário parcial pré-fixado ou sufixo com '*' não funcionará.
- **Redução de ruído** para filtrar arquivos criados nas últimas 2 horas pelo usuário. Ele também é usado para filtrar arquivos temporários (por exemplo, arquivos .tmp) acessados pelo usuário.
- **Domínio** do usuário que realiza a atividade. Você precisa fornecer o **domínio exato** para filtrar. Procurar domínio parcial, ou domínio parcial prefixado ou sufixo com curinga (*), não funcionará. *None* pode ser especificado para procurar domínio ausente.

Os seguintes campos estão sujeitos a regras especiais de filtragem:

- **Entity Type**, usando a extensão entity (file) - é preferível especificar o tipo exato de entidade dentro de aspas. Por exemplo "txt".

- **Path** da entidade - filtros de caminho de diretório (string de caminho que termina com /) até 4 diretórios profundos são recomendados para resultados mais rápidos. Por exemplo, *"/home/userX/nested1/nested2/"*. Consulte a tabela abaixo para obter mais detalhes.
- 1st Level Folder (root) - diretório raiz do Entity Path como filtros. Por exemplo, se o caminho da entidade for */home/userX/nested1/nested2/*, então Home OU "Home" pode ser usado.
- Pasta de nível 2nd - diretório de nível 2nd dos filtros Entity Path. Por exemplo, se o caminho da entidade é */home/userX/nested1/nested2/*, então userX OU "userX" pode ser usado.
- Pasta de nível 3rd – diretório de nível 3rd dos filtros Entity Path.
- Por exemplo, se o caminho da entidade é */home/userX/nested1/nested2/*, então nested1 OU "nested1" pode ser usado.
- Pasta de nível 4th - diretório de nível 4th dos filtros Entity Path. Por exemplo, se o caminho da entidade é */home/userX/nested1/nested2/*, então nested2 OU "nested2" pode ser usado.
- **Usuário** realizando a atividade - é preferível especificar o usuário exato dentro de aspas. Por exemplo, *"Administrador"*.
- **Dispositivo** (SVM) onde as entidades residem
- **Volume** onde as entidades residem
- O **caminho original** usado para renomear eventos quando o arquivo original foi renomeado.

Os campos anteriores estão sujeitos ao seguinte ao filtrar:

- O valor exato deve estar entre aspas: Exemplo: "Searchtext"
- Strings curinga não devem conter aspas: Exemplo: Searchtext, * searchtext*, irá filtrar para quaisquer strings contendo 'searchtext'.
- String com um prefixo, exemplo: Searchtext* , pesquisará quaisquer strings que começam com 'searchtext'.

Exemplos de filtro de atividade Forensics:

Expressão de filtro aplicada pelo usuário	Resultado esperado	Avaliação de desempenho	Comentário
Caminho: "/home/userX/nested1/nested2/"	Pesquisa recursiva de todos os arquivos e pastas sob determinado diretório	Rápido	Pesquisas de diretório até 4 diretórios serão rápidas.
Caminho: "/home/userX/nested1/"	Pesquisa recursiva de todos os arquivos e pastas sob determinado diretório	Rápido	Pesquisas de diretório até 4 diretórios serão rápidas.
Caminho: "/home/userX/nested1/test"	Pesquisa recursiva de todos os arquivos e pastas sob determinado caminho regex(test* pode significar ARQUIVO OU diretório OU ambos)	Mais lento	A pesquisa de regex será mais lenta em comparação com as pesquisas de diretório.

Expressão de filtro aplicada pelo usuário	Resultado esperado	Avaliação de desempenho	Comentário
Caminho: "/home/userX/nested1/nested2/nested3/"	Pesquisa recursiva de todos os arquivos e pastas sob determinado diretório	Mais lento	Mais de 4 buscas de diretórios são mais lentas para pesquisar.
Quaisquer outros filtros não baseados em caminho. Filtros de tipo de usuário e entidade recomendados para estar entre aspas, por exemplo,		Rápido	

NOTA:

1. A contagem de atividades exibida ao lado do ícone todas as atividades é arredondada para 30 minutos quando o intervalo de tempo selecionado se estende por mais de 3 dias. Por exemplo, um intervalo de tempo de *Set 1st 10:15 am a Set 7th 10:15 am* mostrará contagens de atividades de *Set 1st 10:00 am a Sept 7th 10:30 am*.
2. Da mesma forma, as métricas de contagem mostradas no gráfico Histórico de atividades são arredondadas para 30 minutos quando o intervalo de tempo selecionado se estende por mais de 3 dias.

Ordenar dados do histórico de atividades forenses

Você pode classificar os dados do histórico de atividades por *hora*, *Usuário*, *IP de origem*, *atividade*, *tipo de entidade*, pasta de nível 1st (raiz), pasta de nível 2nd, pasta de nível 3rd e pasta de nível 4th. Por padrão, a tabela é ordenada por ordem decrescente *time*, o que significa que os dados mais recentes serão exibidos primeiro. A ordenação está desativada para os campos *Device* e *Protocol*.

Guia do usuário para exportações assíncronas

Visão geral

O recurso de exportações assíncronas no Storage Workload Security foi projetado para lidar com grandes exportações de dados.

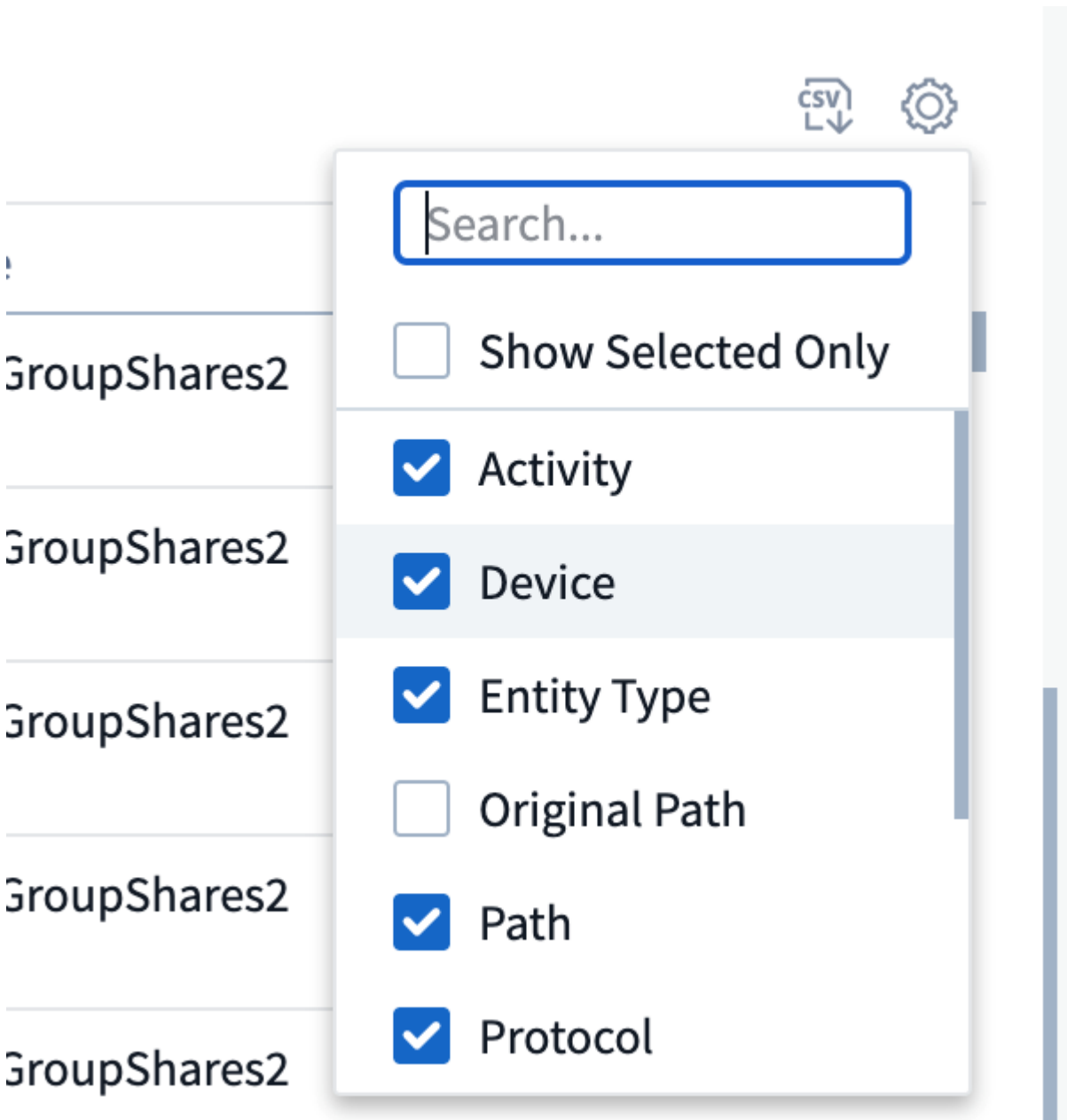
Guia passo a passo: Exportando dados com exportações assíncronas

1. **Iniciar exportação:** Selecione a duração e os filtros desejados para a exportação e clique no botão Exportar.
2. **Aguarde a conclusão da exportação:** O tempo de processamento pode variar de alguns minutos a algumas horas. Talvez seja necessário atualizar a página forense algumas vezes. Quando o trabalho de exportação estiver concluído, o botão "Transferir último ficheiro CSV de exportação" será ativado.
3. *** Download*:** Clique no botão "Download último arquivo de exportação criado" para obter os dados exportados em um formato .zip. Esses dados estarão disponíveis para download até que o usuário inicie outra exportação assíncrona ou decorram 3 dias, o que ocorrer primeiro. O botão permanecerá ativado até que outra exportação assíncrona seja iniciada.
4. **Limitações:**
 - O número de downloads assíncronos está atualmente limitado a 1 por usuário e 3 por locatário.
 - Os dados exportados estão limitados a um máximo de 1 milhões de Registros.

Um script de exemplo para extrair dados forenses via API está presente em `/opt/NetApp/cloudsecure/Agent/export-script/` no agente. Consulte o readme neste local para obter mais detalhes sobre o script.

Seleção de coluna para todas as atividades

A tabela *all activity* mostra as colunas selecionadas por padrão. Para adicionar, remover ou alterar as colunas, clique no ícone de engrenagem à direita da tabela e selecione na lista de colunas disponíveis.



The image shows a table with five rows, each containing the text "GroupShares2". To the right of the table is a settings menu. At the top of the menu is a search bar with the text "Search...". Below the search bar is a checkbox labeled "Show Selected Only", which is currently unchecked. Below that are several options, each with a checked checkbox: "Activity", "Device", "Entity Type", "Original Path", "Path", and "Protocol". The "Device" option is highlighted with a light blue background. In the top right corner of the table area, there are two icons: a "CSV" icon with a downward arrow and a gear icon.

Retenção do histórico da atividade

O histórico de atividades é retido por 13 meses para ambientes ativos de segurança de workload.

Aplicabilidade dos filtros na Página Forensics

Filtro	O que faz	Exemplo	Aplicável a estes filtros	Não aplicável a estes filtros	Resultado
* (Asterisco)	permite-lhe procurar tudo	Auto*03172022 se o texto de pesquisa contiver hífen ou sublinhado, dê expressão entre parênteses. Por exemplo, (svm*) para pesquisar svm-123	Usuário, tipo de entidade, dispositivo, volume, caminho original, pasta 1stLevel, pasta 2ndLevel, pasta 3rdLevel, pasta 4thLevel		Retorna todos os recursos que começam com "Auto" e terminam com "03172022"
? (ponto de interrogação)	permite-lhe procurar um número específico de caracteres	AutoSabotageUser1_03172022?	Usuário, tipo de entidade, dispositivo, volume, pasta 1stLevel, pasta 2ndLevel, pasta 3rdLevel, pasta 4thLevel		Retorna AutoSabotageUser1_03172022A, AutoSabotageUser1_03172022B, AutoSabotageUser1_031720225 e assim por diante
OU	permite especificar várias entidades	AutoSabotageUser1_03172022 OR AutoRansomUser4_03162022	Usuário, domínio, tipo de entidade, caminho original		Retorna qualquer um de AutoSabotageUser1_03172022 OU AutoRansomUser4_03162022
NÃO	permite excluir texto dos resultados da pesquisa	NOT AutoRansomUser4_03162022	Usuário, domínio, tipo de entidade, caminho original, pasta 1stLevel, pasta 2ndLevel, pasta 3rdLevel, pasta 4thLevel	Dispositivo	Retorna tudo o que não começa com "AutoRansomUser4_03162022"
Nenhum	Procura valores NULL em todos os campos	Nenhum	Domínio		retorna resultados onde o campo de destino está vazio

Pesquisa de caminho / caminho original

Os resultados da pesquisa com e sem / serão diferentes

"/AutoDir1/AutoFile03242022"	Somente a busca exata funciona; retorna todas as atividades com o caminho exato como /AutoDir1/AutoFile03242022 (caso insensível)
------------------------------	---

"/AutoDir1/ "	Trabalha; retorna todas as atividades com diretório de 1st níveis correspondente a AutoDir1 (caso insensível)
"/AutoDir1/AutoFile03242022/"	Funciona; retorna todas as atividades com diretório de 1st níveis que correspondem com diretório de AutoDir1 e 2nd níveis que correspondem com AutoFile03242022 (caso insensível)
/AutoDir1/AutoFile03242022 OU /AutoDir1/AutoFile03242022	Não funciona
NÃO /AutoDir1/AutoFile03242022	Não funciona
NÃO /AutoDir1	Não funciona
NÃO /AutoFile03242022	Não funciona
*	Não funciona

Alterações na atividade do usuário do SVM raiz local

Se um usuário local root SVM estiver executando qualquer atividade, o IP do cliente no qual o compartilhamento NFS é montado agora é considerado no nome de usuário, que será mostrado como root at <ip-address-of-the-client> em ambas as páginas de atividade forense e atividade do usuário.

Por exemplo:

- Se o SVM-1 for monitorado pelo Workload Security e o usuário raiz desse SVM montar o compartilhamento em um cliente com endereço IP 10.197.12.40, o nome de usuário exibido na página de atividade forense será *root@10.197.12.40*.
- Se o mesmo SVM-1 estiver montado em outro cliente com endereço IP 10.197.12.41, o nome de usuário mostrado na página de atividade forense será *root@10.197.12.41*.

*• isso é feito para segregar a atividade do usuário raiz NFS pelo endereço IP. Anteriormente, toda a atividade foi considerada feita apenas pelo usuário *root*, sem distinção de IP.

Solução de problemas

Problema	Tente isto
----------	------------

<p>Na tabela "todas as atividades", sob a coluna "Usuário", o nome de usuário é mostrado como: "ldap:HQ.COMPANYNAME.COM:S-1-5-21-3577637-1906459482-1437260136-1831817" ou "LDAP:default:80038003"</p>	<p>Possíveis razões podem ser: 1. Ainda não foram configurados coletores de diretório de utilizadores. Para adicionar um, vá para Workload Security > Collectors > User Directory Collectors e clique em * User Directory Collector*. Escolha <i>ative Directory</i> ou <i>LDAP Directory Server</i>. 2. Um Coletor de diretório de usuários foi configurado, no entanto ele parou ou está em estado de erro. Aceda a Collectors > User Directory Collectors e verifique o estado. Consulte "Solução de problemas do User Directory Collector"a seção da documentação para obter dicas de solução de problemas. Depois de configurar corretamente, o nome será resolvido automaticamente dentro de 24 horas. Se ele ainda não for resolvido, verifique se você adicionou o coletor de dados de usuário correto. Certifique-se de que o usuário faz parte do ative Directory/LDAP Directory Server adicionado.</p>
<p>Alguns eventos NFS não são vistos na IU.</p>	<p>Verifique o seguinte: 1. Um coletor de diretório de usuário para servidor AD com conjunto de atributos POSIX deve ser executado com o atributo unixid habilitado a partir da UI. 2. Qualquer usuário que fizer acesso NFS deve ser visto quando pesquisado na página de usuário da IU 3. Eventos brutos (Eventos para os quais o usuário ainda não foi descoberto) não são compatíveis com NFS 4. O acesso anônimo à exportação NFS não será monitorado. 5. Certifique-se de que a versão NFS usada em menos de NFS4,1.</p>
<p>Depois de digitar algumas letras contendo um caractere curinga como asterisco (*) nos filtros nas páginas Forensics <i>All Activity</i> ou <i>entities</i>, as páginas são carregadas muito lentamente.</p>	<p>Um asterisco () na cadeia de pesquisa procura tudo. No entanto, as cadeias de caracteres curinga principais como <searchTerm> ou *<searchTerm>* resultarão em uma consulta lenta. Para obter um melhor desempenho, use strings de prefixo no formato <searchTerm>* (em outras palavras, anexe o asterisco (*) <i>after</i> um termo de pesquisa). Exemplo: Use a string <i>testvolume*</i>, em vez de <i>*testvolume</i> ou <i>*test*volume</i>. Use uma pesquisa de diretório para ver todas as atividades abaixo de uma determinada pasta recursivamente (pesquisa hierárquica). Por exemplo, <i>/path1/path2/path3/</i> listará todas as atividades recursivamente em <i>/path1/path2/path3</i>. Alternativamente, use a opção "Adicionar ao filtro" na guia todas as atividades."</p>
<p>Estou encontrando um erro "solicitação falhou com o código de status 500/503" ao usar um filtro Path.</p>	<p>Tente usar um intervalo de datas menor para filtrar Registros.</p>
<p>A IU forense está carregando dados lentamente ao usar o filtro <i>path</i>.</p>	<p>Filtros de caminho de diretório (string de caminho terminando com /) até 4 diretórios profundos são recomendados para resultados mais rápidos. Por exemplo, se o caminho de diretório for <i>/AAA/BBB/CCC/DDD</i>, tente pesquisar <i>/AAA/BBB/CCC/DDD/</i> para carregar dados mais rapidamente.</p>

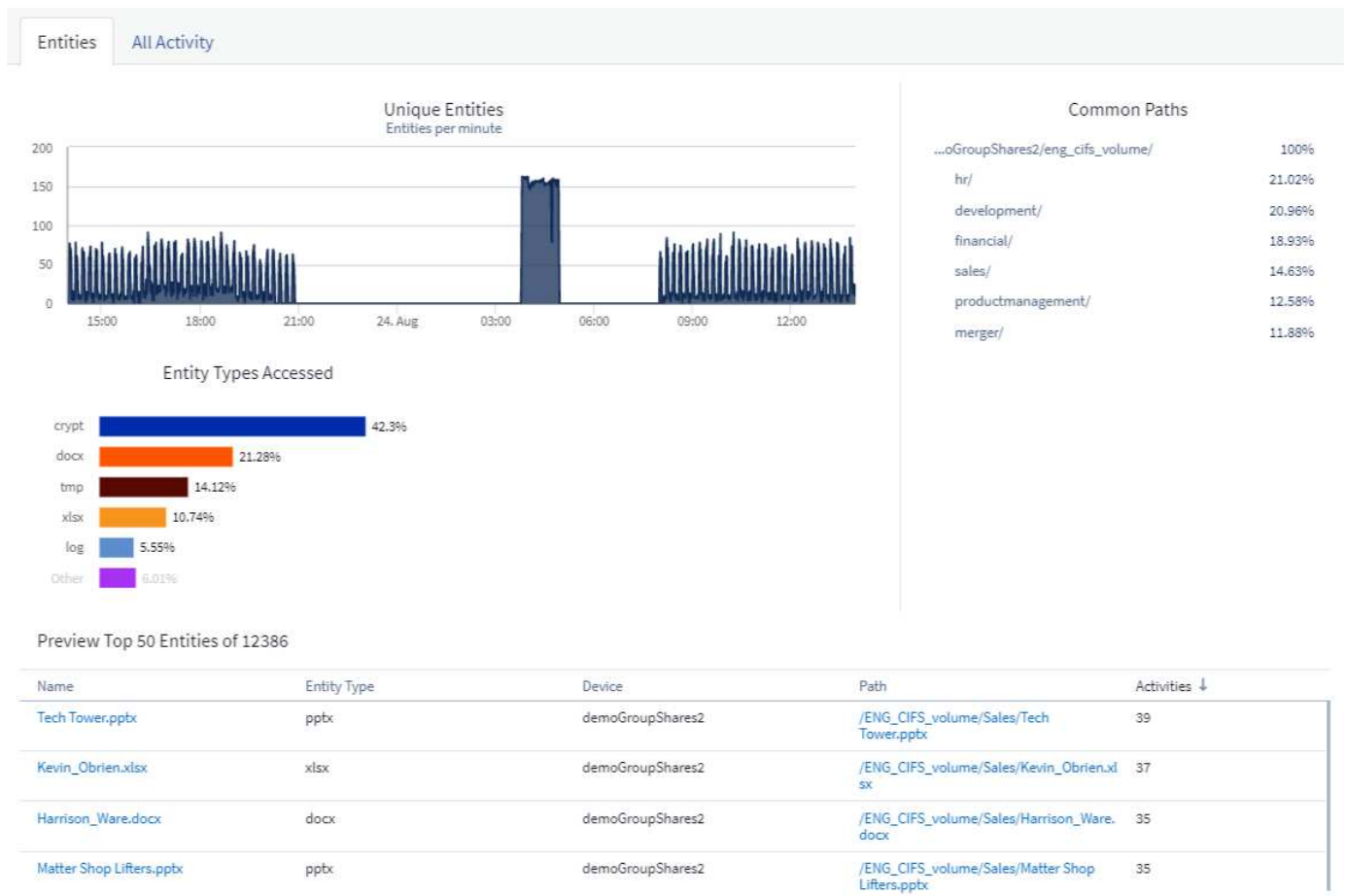
Página de entidades forenses

A página entidades Forensics fornece informações detalhadas sobre a atividade da entidade no seu inquilino.

Examinando informações da entidade

Clique em **Forensics > Activity Forensics** e clique na guia *entities* para acessar a página entidades.

Esta página fornece uma visão geral da atividade da entidade no seu inquilino, destacando as seguintes informações: * Um gráfico mostrando *entidades únicas* acessadas por minuto * Um gráfico de *tipos de entidade acessados* * um detalhamento dos *caminhos comuns* * Uma lista das *principais 50 entidades* do número total de entidades



Clicar em uma entidade na lista abre uma página de visão geral para a entidade, mostrando um perfil da entidade com detalhes como nome, tipo, nome do dispositivo, IP de localização mais acessada e caminho, bem como o comportamento da entidade, como o usuário, IP e hora em que a entidade foi acessada pela última vez.

Entity Overview

Entity Profile

Name Kevin_Obrien.xlsx	Most Accessed Location 10.197.144.115	Size 91 KB
Type xlsx	Device Name demoGroupShares2	Path /ENG_CIFS_volume/Sales/Kevin_Obrien.xlsx

Entity Behaviour

Recent Activity	Operations (last 7 days)
Last accessed : 12 minutes ago <i>Aug 24, 2020 2:02 PM</i>	Read :89
Last accessed by: Tyrique Ray	Read Metadata :22
Last accessed from : 10.197.144.115	Other Activities :43

Visão geral do utilizador forense

As informações para cada usuário são fornecidas na Visão geral do usuário. Use essas visualizações para entender as características do usuário, entidades associadas e atividades recentes.

Perfil de utilizador

As informações do perfil de usuário incluem informações de Contato e localização do usuário. O perfil fornece as seguintes informações:

- Nome do utilizador
- Endereço de e-mail do usuário
- Gestor do utilizador
- Contacto telefónico para o utilizador
- Localização do utilizador

Comportamento do usuário

As informações de comportamento do usuário identificam atividades e operações recentes realizadas pelo usuário. Esta informação inclui:

- Atividade recente
 - Localização do último acesso
 - Gráfico de atividade
 - Alertas
- Operações nos últimos sete dias
 - Número de operações

Intervalo de atualização

A lista de utilizadores é atualizada a cada 12 horas.

Política de retenção

Se não for atualizada novamente, a lista de utilizadores é mantida durante 13 meses. Após 13 meses, os dados serão apagados. Se o ambiente do Workload Security for excluído, todos os dados associados ao ambiente serão excluídos.

Políticas de resposta automatizadas

As políticas de resposta acionam ações como tirar um instantâneo ou restringir o acesso do usuário em caso de ataque ou comportamento anormal do usuário.

Pode definir políticas em dispositivos específicos ou em todos os dispositivos. Para definir uma política de resposta, selecione **Admin > Automated Response Policies** e clique no botão apropriado. Você pode criar políticas para ataques ou avisos.

Add Attack Policy ✕

Policy Name*

For Attack Type(s) *

Ransomware Attack

Data Destruction - File Deletion

On Device

All Devices ▾

+ Another Device

Actions

Take Snapshot ?

Block User File Access ?

Time Period

12 hours ▾

Cancel Save

Você deve salvar a política com um nome exclusivo.

Para desativar uma ação de resposta automatizada (por exemplo, tirar Snapshot), basta desmarcar a ação e salvar a política.

Quando um alerta é acionado contra os dispositivos especificados (ou todos os dispositivos, se selecionados), a política de resposta automática tira um instantâneo dos seus dados. Pode ver o estado do instantâneo no ["Página de detalhes do alerta"](#).

Consulte a ["Restringir o acesso do usuário"](#) página para obter mais detalhes sobre como restringir o acesso do usuário por IP.

Você pode modificar ou pausar uma Política de resposta automatizada escolhendo a opção no menu

suspensão da política.

O Workload Security excluirá automaticamente os instantâneos uma vez por dia com base nas configurações de eliminação de instantâneos.

Snapshot Purge Settings ✕

Define purge periods to automatically delete snapshots taken by Cloud Secure.

Attack Automated Response

Delete Snapshot after

Warning Automated Response

Delete Snapshot after

User Created


Delete Snapshot after

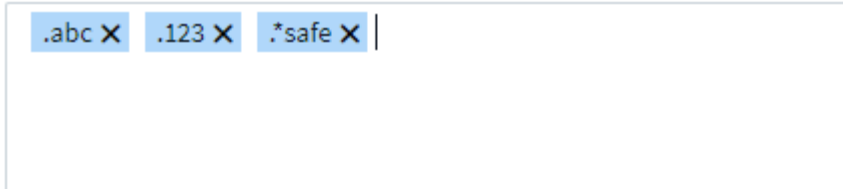
Políticas de tipos de ficheiros permitidos

Se um ataque de ransomware for detetado para uma extensão de arquivo conhecida e alertas estiverem sendo gerados na tela *Alertas*, essa extensão de arquivo pode ser adicionada a uma lista *allowed file types* para evitar alertas desnecessários.

Navegue até **Workload Security > Políticas** e vá para a guia *allowed File Type Policies*.

Allowed File Types Policies

Ransomware alerts will not be triggered for the following file types: 



Uma vez adicionado à lista *allowed file types*, nenhum alerta de ataque de ransomware será gerado para esse tipo de arquivo permitido. Observe que a política *allowed File Types* só é aplicável para detecção de ransomware.

Por exemplo, se um arquivo chamado *test.txt* for renomeado para *test.txt.abc* e o Workload Security estiver detetando um ataque de ransomware por causa da extensão *.abc*, a extensão *.abc* pode ser adicionada à lista *allowed file types*. Depois de serem adicionados à lista, os ataques de ransomware não serão mais gerados contra arquivos com a extensão *.abc*.

Os tipos de ficheiro permitidos podem ser correspondências exatas (por exemplo, ".abc") ou expressões (por exemplo, ".type", ".type" ou "type"). Expressões dos tipos ".a*c", ".p*f" não são suportadas.

Integração com a proteção autônoma contra ransomware do ONTAP

O recurso ONTAP Autonomous ransomware Protection (ARP) usa análise de workload em ambientes nas (NFS e SMB) para detectar e avisar proativamente sobre atividades anormais no arquivo que podem indicar um ataque de ransomware.

Detalhes adicionais e requisitos de licença sobre o ARP podem ser ["aqui"](#) encontrados .

A segurança do workload se integra ao ONTAP para receber eventos ARP e fornece uma camada adicional de análise e respostas automáticas.

A Segurança da carga de trabalho recebe os eventos ARP do ONTAP e realiza as seguintes ações:

1. Correlaciona os eventos de criptografia de volume com a atividade do usuário para identificar quem está causando o dano.
2. Implementa políticas de resposta automática (se definidas)
3. Fornece recursos forenses:
 - Permitir que os clientes realizem investigações de violação de dados.
 - Identificar quais arquivos foram afetados, ajudando a recuperar mais rapidamente e conduzir investigações de violação de dados.

Pré-requisitos

1. Versão mínima do ONTAP: 9.11.1
2. Volumes ativados por ARP. Detalhes sobre como ativar ARP podem ser ["aqui"](#) encontrados . O ARP deve ser ativado via OnCommand System Manager. A Segurança da carga de trabalho não pode ativar o ARP.
3. O coletor de segurança de carga de trabalho deve ser adicionado via IP de cluster.
4. Credenciais de nível de cluster são necessárias para que esse recurso funcione. Em outras palavras, as credenciais no nível do cluster devem ser usadas ao adicionar o SVM.

Permissões de usuário necessárias

Se você estiver usando credenciais de administração de cluster, não serão necessárias novas permissões.

Se você estiver usando um usuário personalizado (por exemplo, *csuser*) com permissões dadas ao usuário, siga as etapas abaixo para conceder permissões à Segurança de carga de trabalho para coletar informações relacionadas ao ARP do ONTAP.

Para *csuser* com credenciais de cluster, faça o seguinte na linha de comando ONTAP:

```
security login rest-role create -role arwrole -api /api/storage/volumes
-access readonly -vserver <cluster_name>
security login rest-role create -api /api/security/anti-ransomware -access
readonly -role arwrole -vserver <cluster_name>
security login create -user-or-group-name csuser -application http
-authmethod password -role arwrole
```

Leia mais sobre como configurar outro ["Permissões da ONTAP"](#).

Alerta de amostra

Um alerta de exemplo gerado devido a evento ARP é mostrado abaixo:



POTENTIAL ATTACK: AL_1315
Ransomware Attack

Detected
5 months ago
Oct 20, 2022 3:06 AM

Action Taken
⚠ Access Blocked on 5 SVMs
Snapshots Taken

Status
New

Blocked permanently by
auto response policy

Last snapshots taken by
auto response policy
Oct 20, 2022 3:09 AM

How To:
Restore Entities

Change Block Period

Re-Take Snapshots

Unblock User

Total Attack Results

1 Affected Volumes | 83 Deleted Files | 81 Encrypted Files

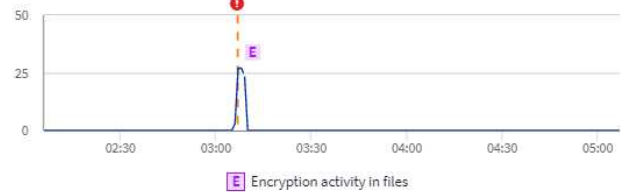
81 Files have been copied, deleted, and potentially encrypted by 1 user account.

The extension "osiris" was added to each file.

High Confidence Detection
Ransomware behavior and in-file encryption activities were detected.

Encrypted Files

Activity per minute



Related Users



Jamelia Graham
Business Partner
HR

User/IP Access

Blocked

81 Encrypted Files
Detected 5 months ago
Oct 20, 2022 3:06 AM

Username
us024
Domain
cslab.netapp.com
Email
Graham@netapp.com
Phone
9251140014

Department
HR
Manager
Iwan Holt
Location
WA

Top Activity Types

Activity per minute
Last accessed from: 10.193.113.247

View Activity Detail



Access Limitation History for This User (3)

Time	Action	Duration	Action Taken by	Response	Blocked IPs on NFS
Oct 20, 2022 3:09 AM	⚠ Block more detail	Never Expires		Automatic	none
Mar 10, 2022 4:59 AM	Unblock		system	Blocking Expired	10.197.144.115
Mar 10, 2022 3:57 AM	⚠ Block more detail	1h		Automatic	10.197.144.115

Affected Devices/Volumes

Device ↑	Volume	Encrypted Files	Associated Snapshot Taken
subprod_rtp	stargazer	81	Oct 20, 2022 3:09 AM cloudsecure_attack_auto _1666249787062 Automatic Take Snapshot

Um banner de alta confiança indica que o ataque mostrou comportamento de ransomware, juntamente com atividades de criptografia de arquivos. O gráfico de arquivos criptografados indica o carimbo de data/hora no qual a atividade de criptografia de volume foi detetada pela solução ARP.

Limitações

No caso de um SVM não ser monitorado pela Segurança de carga de trabalho, mas houver eventos ARP gerados pelo ONTAP, os eventos ainda serão recebidos e exibidos pela Segurança de carga de trabalho. No entanto, as informações forenses relacionadas ao alerta, bem como o mapeamento do usuário, não serão capturadas ou mostradas.

Solução de problemas

Problemas conhecidos e suas resoluções são descritos na tabela a seguir.

Problema:	Resolução:
Os alertas por e-mail são recebidos 24 horas após um ataque ser detetado. Na IU, os alertas são exibidos 24 horas antes quando os e-mails são recebidos pelo Data Infrastructure Insights Workload Security.	Quando o ONTAP envia o evento <i>ransomware Detected</i> para a Segurança de carga de trabalho do Insights da infraestrutura de dados (ou seja, Segurança de carga de trabalho), o e-mail é enviado. O evento contém uma lista de ataques e seus carimbos de data/hora. A IU de Segurança do workload exibe o carimbo de data/hora do alerta do primeiro arquivo atacado. O ONTAP envia o evento <i>ransomware Detected</i> para informações de infraestrutura de dados quando um certo número de arquivos é codificado. Portanto, pode haver uma diferença entre a hora em que o alerta é exibido na IU e a hora em que o e-mail é enviado.

Integração com o ONTAP Access negada

O recurso Acesso negado do ONTAP usa análise de workload em ambientes nas (NFS e SMB) para detectar e avisar proativamente sobre operações de arquivos com falha (ou seja, um usuário tentando executar uma operação para a qual não tenha permissão). Essas notificações falhadas de operação de arquivos - especialmente em casos de falhas relacionadas à segurança - ajudarão a bloquear ataques internos nos estágios iniciais.

A segurança de workload se integra ao ONTAP para receber eventos de acesso negado e fornecer uma camada de resposta automática e analítica adicional.

Pré-requisitos

- Versão mínima do ONTAP: 9.13.0.
- Um administrador de Segurança de carga de trabalho deve habilitar o recurso Acesso negado ao adicionar um novo coletor ou editar um coletor existente, selecionando a caixa de seleção *Monitor Access Neged Events* em Configuração Avançada.

NetApp Cloud Insights Tutorial 0% Complete Getting Started

CI dev 1 / Workload Security / Collectors / Add Data Collector

Enter complete Share Names to be excluded, separated by a comma.
Share Names

Volume Names
Enter complete Volume Names to be excluded, separated by a comma.
Volume names

Advanced Configuration

Monitor Directory Read & Open Activity (SMB only)
Note: Generates many directory access events (noise)

Monitor Access Denied Events
Note: This feature will be available from ONTAP 9.13 and above

Fpolicy Server Send Buffer Size
1MB

Cancel Save

Permissões de usuário necessárias

Se o Data Collector for adicionado usando credenciais de administração de cluster, nenhuma nova permissão será necessária.

Se o Coletor for adicionado usando um usuário personalizado (por exemplo, *csuser*) com permissões dadas ao usuário, siga as etapas abaixo para dar à Segurança da carga de trabalho a permissão necessária para se Registrar para eventos de acesso negado com o ONTAP.

Para *csuser* com credenciais *cluster*, execute os seguintes comandos a partir da linha de comando ONTAP. Observe que *csrestrole* é função personalizada e *csuser* é usuário personalizado do ONTAP.

```
security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <cluster_name>
security login create -user-or-group-name csuser -application http
-authmethod password -role csrestrole
```

Para *csuser* com credenciais *SVM*, execute os seguintes comandos da linha de comando ONTAP:

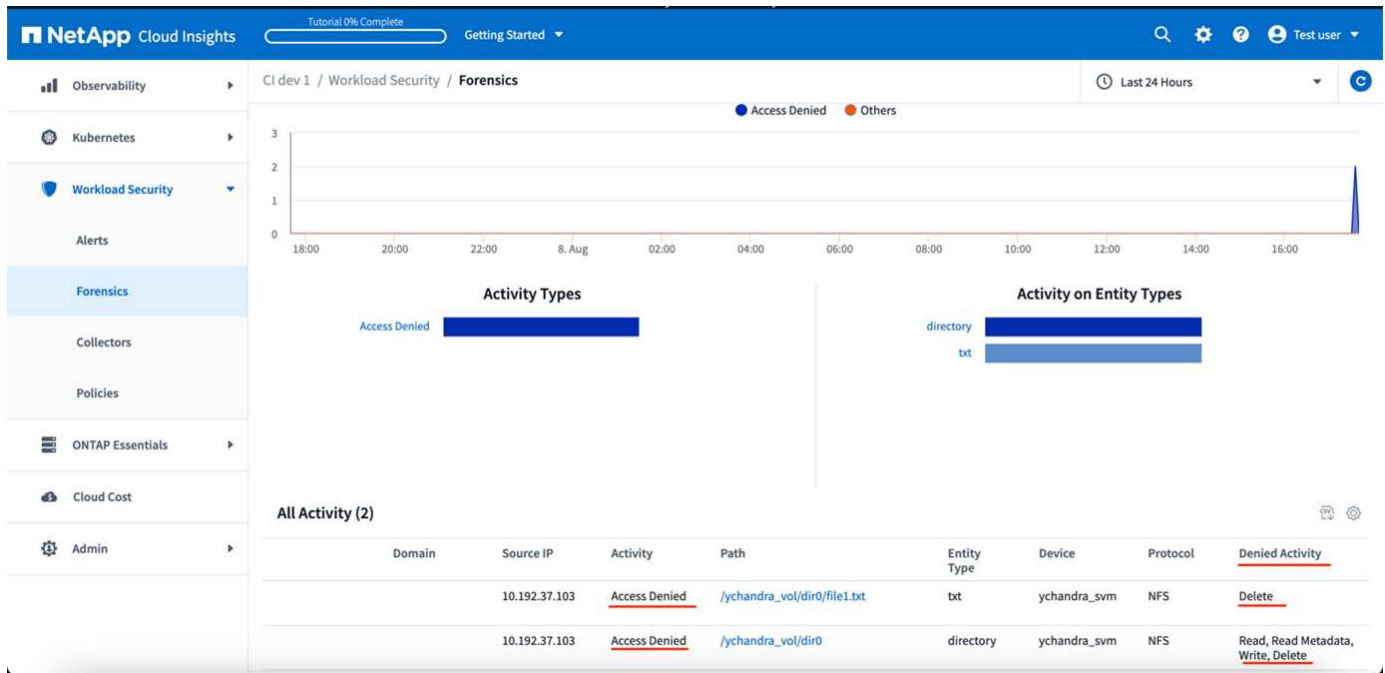
```
security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <svm_name>
security login create -user-or-group-name csuser -application http
-authmethod password -role csrestrole -vserver <svm_name>
```

Leia mais sobre como configurar outro ["Permissões da ONTAP"](#).

Acesso negado eventos

Uma vez que os eventos tenham sido adquiridos do sistema ONTAP, a página Forensics de Segurança de

carga de trabalho mostrará eventos de Acesso negado. Além das informações exibidas, você pode visualizar as permissões de usuário ausentes para uma determinada operação adicionando a coluna *atividade desejada* à tabela a partir do ícone de engrenagem.



Bloquear o acesso do utilizador

Uma vez que um ataque é detetado, o Workload Security pode parar o ataque bloqueando o acesso do usuário ao sistema de arquivos. O acesso pode ser bloqueado automaticamente, usando políticas de resposta automatizadas ou manualmente a partir das páginas de alerta ou detalhes do usuário.

Ao bloquear o acesso do usuário, você deve definir um período de tempo de bloqueio. Após o término do período de tempo selecionado, o acesso do usuário é restaurado automaticamente. O bloqueio de acesso é compatível com protocolos SMB e NFS.

O usuário é bloqueado diretamente para SMB e o endereço IP das máquinas host, fazendo com que o ataque seja bloqueado para NFS. Esses endereços IP da máquina serão bloqueados para acessar qualquer uma das máquinas virtuais de armazenamento (SVMs) monitoradas pelo Workload Security.

Por exemplo, digamos que o Workload Security gerencia 10 SVMs e a Política de resposta automática está configurada para quatro desses SVMs. Se o ataque tiver origem em um dos quatro SVMs, o acesso do usuário será bloqueado em todos os 10 SVMs. O Snapshot ainda é usado na SVM de origem.

Se houver quatro SVMs com um SVM configurado para SMB, um configurado para NFS e os dois restantes configurados para NFS e SMB, todas as SVMs serão bloqueadas se o ataque tiver origem em qualquer uma das quatro SVMs.

Pré-requisitos para bloqueio de acesso do usuário

Credenciais de nível de cluster são necessárias para que esse recurso funcione.

Se você estiver usando credenciais de administração de cluster, não serão necessárias novas permissões.

Se você estiver usando um usuário personalizado (por exemplo, *csuser*) com permissões dadas ao usuário, siga as etapas abaixo para conceder permissões ao Workload Security para bloquear o usuário.

Para *csuser* com credenciais de cluster, faça o seguinte na linha de comando ONTAP:

```
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
```

Certifique-se de rever a seção permissões da ["Configurando o coletor de dados SVM do ONTAP"](#) página também.

Como ativar a funcionalidade?

- Em Workload Security, navegue até **Workload Security > Políticas > Automated Response Policies**. Escolha * Política de ataque *.
- Selecione (marque) *Bloquear Acesso ao Arquivo de Usuário*.

Como configurar o bloqueio de acesso automático do usuário?

- Crie uma nova Política de ataque ou edite uma política de ataque existente.
- Selecione as SVMs nas quais a política de ataque deve ser monitorada.
- Clique na caixa de verificação "Bloquear acesso ao ficheiro do utilizador". A funcionalidade será ativada quando esta for selecionada.
- Em "período de tempo", selecione o tempo até o qual o bloqueio deve ser aplicado.
- Para testar o bloqueio automático do usuário, você pode simular um ataque por meio de um ["script simulado"](#).

Como saber se existem utilizadores bloqueados no sistema?

- Na página listas de alertas, um banner na parte superior da tela será exibido no caso de qualquer usuário ser bloqueado.
- Clicar no banner irá levá-lo para a página "usuários", onde a lista de usuários bloqueados pode ser vista.
- Na página "usuários", há uma coluna chamada "Usuário/Acesso IP". Nessa coluna, o estado atual de bloqueio do usuário será exibido.

Restringir e gerenciar o acesso do usuário manualmente

- Pode aceder ao ecrã de detalhes de alerta ou de detalhes do utilizador e, em seguida, bloquear ou restaurar manualmente um utilizador a partir desses ecrãs.

Histórico de limitação de acesso do utilizador

Na página de detalhes do alerta e detalhes do usuário, no painel do usuário, você pode visualizar uma auditoria do histórico de limitação de acesso do usuário: Tempo, Ação (Bloquear, desbloquear), duração, ação realizada por, manual/automática e IPs afetados para NFS.

Como desativar a funcionalidade?

A qualquer momento, você pode desativar o recurso. Se houver usuários restritos no sistema, você deve restaurar o acesso deles primeiro.

- Em Workload Security, navegue até **Workload Security > Políticas > Automated Response Policies**. Escolha * Política de ataque *.
- Desmarque (desmarque) *Bloquear acesso ao ficheiro do utilizador*.

O recurso ficará oculto de todas as páginas.

Restaure manualmente IPs para NFS

Siga as etapas a seguir para restaurar manualmente qualquer IPs do ONTAP se a avaliação de Segurança de carga de trabalho expirar ou se o agente/coletor estiver inativo.

1. Listar todas as políticas de exportação em um SVM.

```
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
          cifs              10.11.12.13
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. Exclua as regras de todas as políticas no SVM que têm "cloudsecure_rule" como correspondência do cliente especificando seu respectivo RuleIndex. Regra de Segurança da carga de trabalho geralmente será em 1.

```

contrail-qa-fas8020::*> export-policy rule delete -vserver <svm name>
-policyname * -ruleindex 1
. Certifique-se de que a regra de segurança de carga de trabalho seja
excluída (etapa opcional para confirmar).

```

```

contrail-qa-fas8020::*> export-policy rule show -vserver <svm name>

```

Vserver	Policy Name	Rule Index	Access Protocol	Client Match	RO Rule
svm0	default	4	cifs, nfs	0.0.0.0/0	any
svm2	test	3	cifs, nfs, flexcache	0.0.0.0/0	any

2 entries were displayed.

Restaurar manualmente os usuários para SMB

Siga as etapas a seguir para restaurar manualmente qualquer usuário do ONTAP se a avaliação de Segurança de carga de trabalho expirar ou se o agente/coletor estiver inativo.

Você pode obter a lista de usuários bloqueados no Workload Security na página de lista de usuários.

1. Faça login no cluster do ONTAP (onde você deseja desbloquear usuários) com credenciais *admin* do cluster. (Para o Amazon FSX, faça login com credenciais FSX).
2. Execute o seguinte comando para listar todos os usuários bloqueados pelo Workload Security para SMB em todos os SVMs:

```

vserver name-mapping show -direction win-unix -replacement " "

```

```

Vserver: <vservename>
Direction: win-unix
Position Hostname IP Address/Mask
-----
1 - - Pattern: CSLAB\\US040
Replacement:
2 - - Pattern: CSLAB\\US030
Replacement:
2 entries were displayed.

```

Na saída acima, 2 usuários foram bloqueados (US030, US040) com domínio CSLAB.

1. Uma vez que identificamos a posição da saída acima, execute o seguinte comando para desbloquear o usuário:

```
vserver name-mapping delete -direction win-unix -position <position>
. Confirme se os usuários estão desbloqueados executando o comando:
```

```
vserver name-mapping show -direction win-unix -replacement " "
```

Nenhuma entrada deve ser exibida para os usuários bloqueados anteriormente.

Solução de problemas

Problema	Tente isto
Alguns dos usuários não estão ficando restritos, embora haja um ataque.	1. Certifique-se de que o coletor de dados e o agente das SVMs estejam no estado <i>Running</i> . A Segurança da carga de trabalho não poderá enviar comandos se o Coletor de dados e o Agente estiverem parados. 2. Isso ocorre porque o usuário pode ter acessado o armazenamento de uma máquina com um novo IP que não foi usado antes. A restrição acontece através do endereço IP do host através do qual o usuário está acessando o armazenamento. Verifique na IU (Detalhes de alerta > Histórico de limitação de acesso para este utilizador > IPs afetados) a lista de endereços IP restritos. Se o usuário estiver acessando o armazenamento de um host que tenha um IP diferente dos IPs restritos, o usuário ainda poderá acessar o armazenamento por meio do IP não restrito. Se o usuário estiver tentando acessar a partir dos hosts cujos IPs são restritos, o armazenamento não estará acessível.
Clicar manualmente em restringir acesso dá "endereço IP deste usuário já foram restritos".	O IP a ser restrito já está sendo restringido de outro usuário.
Não foi possível modificar a política. Motivo: Não autorizado para esse comando.	Verifique se usando <i>csuser</i> , as permissões são dadas ao usuário como mencionado acima.
O bloqueio de usuário (endereço IP) para NFS funciona, mas para SMB / CIFS, vejo uma mensagem de erro: "SID para transformação DomainName falhou. Tempo limite da razão: O soquete não está estabelecido"	Isso pode acontecer é <i>csuser</i> não tem permissão para executar <i>ssh</i> . (Assegure a conexão no nível do cluster e, em seguida, certifique-se de que o usuário pode executar <i>ssh</i>). <i>csuser</i> função requer essas permissões. https://docs.netapp.com/us-en/cloudinsights/cs_restrict_user_access.html#prerequisites-for-user-access-blocking Para <i>csuser</i> com credenciais de cluster, faça o seguinte a partir da linha de comando ONTAP: Security login role create -role csrole -cmddirname "vserver export-policy rule" -access all security login role ONTAP

Problema	Tente isto
Estou recebendo a mensagem de erro <i>SID translate failed. reason:255:Error: Command failed: Not Authorized for that commandError: "Access-check" não é um comando reconhecido</i> , quando um usuário deve ter sido bloqueado.	Isso pode acontecer quando <i>csuser</i> não tem permissões corretas. Consulte " Pré-requisitos para bloqueio de acesso do usuário " para obter mais informações. Depois de aplicar as permissões, é recomendável reiniciar o coletor de dados do ONTAP e o coletor de dados do diretório do usuário. Os comandos de permissão necessários estão listados abaixo. ---- função de login de segurança criar -role csrole -cmddirname "vserver export-policy rule" -access all security login role create -role csrole -cmddirname set -access all security login role create -rule csrole -csrole -csname -csname -csname-

Segurança da carga de trabalho: Simulando um ataque

Você pode usar as instruções nesta página para simular um ataque para testar ou demonstrar o Workload Security usando o script de simulação de ransomware incluído.

Coisas a observar antes de começar

- O script de simulação de ransomware funciona apenas no Linux.
- O script é fornecido com os arquivos de instalação do agente Workload Security. Ele está disponível em qualquer máquina que tenha um agente Workload Security instalado.
- Você pode executar o script na própria máquina do agente Workload Security; não há necessidade de preparar outra máquina Linux. No entanto, se você preferir executar o script em outro sistema, basta copiar o script e executá-lo lá.

Tenha pelo menos 1.000 arquivos de amostra

Esse script deve ser executado em uma SVM com uma pasta que tenha arquivos para criptografar. Recomendamos ter pelo menos 1.000 arquivos dentro dessa pasta e quaisquer subpastas. Os ficheiros não podem estar vazios. Não crie os arquivos e criptografe-os usando o mesmo usuário. O Workload Security considera esta uma atividade de baixo risco e, portanto, não gera um alerta (ou seja, o mesmo usuário modifica os arquivos que ele/ela/eles acabaram de criar).

Veja abaixo as instruções para "[crie arquivos não vazios programaticamente](#)".

Diretrizes antes de executar o simulador:

1. Certifique-se de que os ficheiros encriptados não estão vazios.
2. Certifique-se de encriptar > 50 ficheiros. Um pequeno número de arquivos será ignorado.
3. Não execute um ataque com o mesmo usuário várias vezes. Depois de algumas vezes, o Workload Security vai aprender esse comportamento do usuário e assumir que é o comportamento normal do usuário.
4. Não criptografe arquivos que o mesmo usuário acabou de criar. Alterar um arquivo que acabou de ser criado por um usuário não é considerado uma atividade arriscada. Em vez disso, use arquivos criados por outro usuário OU aguarde algumas horas entre a criação dos arquivos e a criptografia.

Prepare o sistema

Primeiro, monte o volume alvo na máquina. Você pode montar uma montagem NFS ou exportação CIFS.

Para montar a exportação NFS no Linux:

```
mount -t nfs -o vers=4.0 10.193.177.158:/svmvoll /mntpt
mount -t nfs -o vers=4.0 Vserver data IP>:/nfsvol /destinationlinuxfolder
```

Não monte o NFS versão 4,1; ele não é suportado pelo Fpolicy.

Para montar CIFS no Linux:

```
mount -t cifs //10.193.77.91/sharedfolderincluster
/root/destinationfolder/ -o username=raisa
Em seguida, configure um Data Collector:
```

1. Configure o agente Workload Security se ainda não tiver sido feito.
2. Configurar o coletor de dados SVM, se ainda não tiver feito.

Execute o script ransomware Simulator

1. Faça login (ssh) na máquina do agente Workload Security.
2. Navegue para: `/opt/NetApp/cloudsecure/Agent/install`
3. Chame o script do simulador sem parâmetros para ver o uso:

```
# pwd
/opt/netapp/cloudsecure/agent/install
# ./ransomware_simulator.sh
Error: Invalid directory provided.
Usage: ./ransomware_simulator.sh [-e] [-d] [-i <input_directory>]
    -e to encrypt files (default)
    -d to restore files
    -i <input_directory> - Files under the directory to be encrypted
```

```
Encrypt command example: ./ransomware_simulator.sh -e -i
/mnt/audit/reports/
Decrypt command example: ./ransomware_simulator.sh -d -i
/mnt/audit/reports/
```

Criptografe seus arquivos de teste

Para criptografar os arquivos, execute o seguinte comando:

```
# ./ransomware_simulator.sh -e -i /root/for/  
Encryption key is saved in /opt/netapp/cloudsecure/cloudsecure-agent-  
1.251.0/install/encryption-key,  
which can be used for restoring the files.  
Encrypted /root/for/File000.txt  
Encrypted /root/for/File001.txt  
Encrypted /root/for/File002.txt  
...
```

Restaurar ficheiros

Para descriptografar, execute o seguinte comando:

```
[root@scspa2527575001 install]# ./ransomware_simulator.sh -d -i /root/for/  
File /root/for/File000.txt is restored.  
File /root/for/File001.txt is restored.  
File /root/for/File002.txt is restored.  
...
```

Execute o script várias vezes

Depois de gerar um ataque de ransomware para um usuário, mude para outro usuário para gerar um ataque adicional. O Workload Security aprende o comportamento do usuário e não alerta sobre ataques repetidos de ransomware em um curto período para o mesmo usuário.

Crie arquivos programaticamente

Antes de criar os arquivos, você deve primeiro parar ou pausar o processamento do coletor de dados. Execute as etapas abaixo antes de adicionar o coletor de dados ao Agente. Se você já adicionou o coletor de dados, basta editar o coletor de dados, inserir uma senha inválida e salvá-la. Isso colocará temporariamente o coletor de dados no estado de erro. Nota: Certifique-se de anotar a palavra-passe original!



A opção recomendada é "[pausar o coletor](#)" antes de criar seus arquivos.]

Antes de executar a simulação, você deve primeiro adicionar arquivos para serem criptografados. Você pode copiar manualmente os arquivos a serem criptografados na pasta de destino ou usar um script (veja o exemplo abaixo) para criar programaticamente os arquivos. Qualquer que seja o método utilizado, copie pelo menos 1.000 ficheiros.

Se você optar por criar programaticamente os arquivos, faça o seguinte:

1. Faça login na caixa Agente.
2. Montar uma exportação NFS do SVM do arquivador para a máquina Agent. CD para essa pasta.

3. Nessa pasta, crie um arquivo chamado createfiles.sh
4. Copie as linhas a seguir para esse arquivo.

```
for i in {000..1000}
do
    echo hello > "File${i}.txt"
done
echo 3 > /proc/sys/vm/drop_caches ; sync
```

5. Salve o arquivo.
6. Certifique-se de executar permissão no arquivo:

```
chmod 777 ./createfiles.sh
. Execute o script:
```

```
./createfiles.sh
```

os ficheiros 1000 serão criados na pasta atual.

7. Reative o coletor de dados

Se você desativou o coletor de dados na etapa 1, edite o coletor de dados, insira a senha correta e salve. Certifique-se de que o coletor de dados está de volta no estado em execução.

8. Se você fez uma pausa no coletor antes de seguir estas etapas, certifique-se "[retomar o coletor](#)" de .

Configurar notificações de e-mail para alertas, avisos e integridade do coletor de agente/fonte de dados

Para configurar os destinatários do alerta de segurança do Workload, clique em **Admin > notificações** e insira um endereço de e-mail na(s) seção(s) apropriada(s) para cada destinatário.

Alertas e avisos de ataque potenciais

Para enviar notificações de alerta *potencial ataque*, insira os endereços de e-mail dos destinatários na seção *Enviar alertas de ataque potencial*. As notificações por e-mail são enviadas para a lista de destinatários de alerta para cada ação no alerta.

Para enviar notificações *Aviso*, insira os endereços de e-mail dos destinatários na seção *Enviar alertas de aviso*.

Monitoramento de integridade do agente e coletor de dados

Você pode monitorar a integridade de agentes e fontes de dados por meio de notificações.

Para receber notificações no caso de um agente ou coletor de fonte de dados não funcionar, insira os endereços de e-mail dos destinatários na seção *Alertas de integridade da coleta de dados*.

Tenha em mente o seguinte:

- Os alertas de integridade serão enviados somente depois que o agente/coletor parar de informar por pelo menos uma hora.
- Somente uma notificação por e-mail é enviada aos destinatários pretendidos em um determinado período de 24 horas, mesmo que o Agente ou coletor de dados esteja desconetado por uma duração maior.
- Em caso de falha do Agente, um alerta será enviado (não um por coletor). O e-mail incluirá uma lista de todos os SVMs impactados.
- A falha de coleta de diretório ativo é relatada como um aviso; ela não afeta a detecção de ransomware.
- A lista de configuração Introdução agora inclui uma nova fase *Configurar notificações por e-mail*.

Recebendo notificações de atualização de Agente e Coletor de dados

- Insira o(s) ID(s) de e-mail nos "Alertas de integridade da coleta de dados".
- A caixa de verificação "Ativar notificações de atualização" torna-se ativada.
- As notificações de e-mail de atualização do agente e do coletor de dados são enviadas para os IDs de e-mail um dia antes da atualização planejada.

Solução de problemas

Problema:	Tente isto:
Os IDs de e-mail estão presentes nos "Alertas de integridade do coletor de dados", no entanto, não estou recebendo notificações.	Os e-mails de notificação são enviados a partir do domínio de informações de infraestrutura de dados da NetApp, ou seja, a partir de <code>[[cloudinsights.NetApp.com_]]</code> . Algumas empresas bloqueiam e-mails recebidos se forem de um domínio externo. Certifique-se de que as notificações externas dos domínios do Insights da infraestrutura de dados do NetApp estejam na lista branca.

API de segurança de carga de trabalho

A API de segurança de carga de trabalho permite que clientes da NetApp e fornecedores de software independentes (ISVs) integrem a segurança de carga de trabalho com outros aplicativos, como CMDB ou outros sistemas de emissão de tíquetes.

Requisitos para acesso à API:

- Um modelo de token de acesso à API é usado para conceder acesso.
- O gerenciamento de token de API é realizado por usuários do Workload Security com a função Administrador.

Documentação da API (Swagger)

As informações mais recentes da API são encontradas efetuando login no Workload Security e navegando até

Admin > API Access. Clique no link **Documentação da API**. A Documentação da API é baseada no Swagger, que fornece uma breve descrição e informações de uso para a API e permite que você experimente no seu locatário.



Ao chamar a API de atividade Forensics, use a API `cloudsecure_forensics.Activities.v2` API. Se você estiver fazendo várias chamadas para essa API, verifique se as chamadas ocorrem sequencialmente, não em paralelo. Várias chamadas paralelas podem fazer com que a API termine o tempo limite.

Tokens de acesso à API

Antes de usar a API Workload Security, você deve criar um ou mais **tokens de acesso à API**. Os tokens de acesso concedem permissões de leitura. Você também pode definir a expiração para cada token de acesso.

Para criar um token de acesso:

- Clique em **Admin > API Access**
- Clique em * API Access Token*
- Digite **Nome do Token**
- Especifique **validade do token**



Seu token só estará disponível para copiar para a área de transferência e salvar durante o processo de criação. Os tokens não podem ser recuperados depois que são criados, por isso é altamente recomendável copiar o token e salvá-lo em um local seguro. Você será solicitado a clicar no botão Copiar token de acesso à API antes de fechar a tela de criação de token.

Você pode desativar, ativar e revogar tokens. Os tokens que estão desativados podem ser ativados.

Os tokens concedem acesso de propósito geral às APIs da perspectiva do cliente, gerenciando o acesso às APIs no escopo de seu próprio locatário.

O aplicativo recebe um token de acesso depois que um usuário autentica e autoriza o acesso com êxito e passa o token de acesso como uma credencial quando chama a API de destino. O token passado informa à API que o portador do token foi autorizado a acessar a API e executar ações específicas com base no escopo que foi concedido durante a autorização.

O cabeçalho HTTP onde o token de acesso é passado é **X-CloudInsights-ApiKey**:

Por exemplo, use o seguinte para recuperar ativos de armazenamento:

```
curl https://<tenant_host_name>/rest/v1/cloudsecure/activities -H 'X-CloudInsights-ApiKey: <API_Access-Token>'
```

Onde `<API_Access-Token>` é o token que você salvou durante a criação da chave de acesso à API.

Informações detalhadas podem ser encontradas no link *API Documentation* em **Admin > API Access**.

Script para extrair dados através da API

Os agentes de segurança de carga de trabalho incluem um script de exportação para facilitar chamadas paralelas para a API v2 dividindo o intervalo de tempo solicitado em lotes menores.

O script está localizado em `/opt/NetApp/cloudsecure/Agent/export-script`. Um arquivo README no mesmo diretório fornece instruções de uso.

Aqui está um comando de exemplo para invocar o script:

```
python3 data-export.py --tenant_url <tenant
id>.cs01.cloudinsights.netapp.com --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
```

Parâmetros-chave: - `--iteration_interval 12`: Divide o intervalo de tempo solicitado em intervalos de 12 horas. - `--num_workers 3`: Fetches esses intervalos em paralelo usando 3 threads.

Solução de problemas

Solução de problemas gerais do Data Infrastructure Insights

Aqui você encontrará sugestões para solução de problemas do Data Infrastructure Insights.

Consulte também "[Solução de problemas da Unidade de aquisição do Linux](#)" e "[Solução de problemas da Unidade de aquisição do Windows](#)".

Problemas de login

Problema:	Tente isto:
O Data Infrastructure Insights faz logout automaticamente a cada 6 horas	Isso se deve a cookies de terceiros desativados no navegador. Os usuários podem configurar seu navegador para habilitar todos os cookies de 3rd partes, ou usar uma lista de exceções mais restrita para apenas habilitar aqueles para o Data Infrastructure Insights. Exemplo: Abra as configurações do seu navegador. Selecione a opção "permitir todos os cookies". OR Selecione "Bloquear cookies de terceiros" e adicione exceções para <i>[.]auth0.com</i> e <i>[.]NetApp.com</i> . O Microsoft Edge segue o mesmo formato para exceções que o Chrome. No Firefox, as exceções de cookies são designadas simplesmente como <i>auth0.com</i> e <i>NetApp.com</i> .
Tenho uma conta BlueXP , mas não consigo iniciar sessão no BlueXP .	Abra um ticket do https://mysupport.netapp.com/site/help . Selecione a categoria BlueXP .NetApp.com > problemas de conta/login ou BlueXP .NetApp.com > problemas de Federação . Estes são especificamente para problemas ou perguntas do BlueXP . Para todos os outros problemas de suporte técnico do Data Infrastructure Insights, entre em Contato " Suporte à NetApp " com .
Fui convidado para o Data Infrastructure Insights, mas recebo uma mensagem "não autorizada".	Verifique se você se inscreveu em uma conta do BlueXP ou se sua organização usa login SSO com o BlueXP . Verifique se o endereço de e-mail do seu perfil do BlueXP corresponde ao endereço de e-mail exibido no e-mail de boas-vindas do Insights de infraestrutura de dados. Se o e-mail não corresponder, solicite um novo convite com o endereço de e-mail correto.

Problema:	Tente isto:
Eu fiz logout do BlueXP e fui desconetado automaticamente do Insights de infraestrutura de dados.	O logon único (SSO) em todos os serviços de nuvem da NetApp faz logout de todas as sessões do Insights de infraestrutura de dados. Se você tiver acesso a várias contas do Data Infrastructure Insights, fazer logout de qualquer uma das sessões ativas. Inicie sessão novamente para aceder à sua conta.
Eu fui desconetado automaticamente após vários dias.	As contas de nuvem do NetApp exigem nova autenticação a cada poucos dias (a configuração atual do BlueXP é de 7 dias). Inicie sessão novamente para aceder à sua conta.
Recebo uma mensagem de erro "já não está autorizado a iniciar sessão".	Entre em Contato com o administrador da conta para verificar o acesso ao Data Infrastructure Insights. Verifique se o endereço de e-mail do seu perfil do BlueXP corresponde ao endereço de e-mail exibido no e-mail de boas-vindas do Insights de infraestrutura de dados
Outros erros de login	Experimente o modo de navegação anônima no Chrome ou limpe o histórico do navegador, os cookies e o cache. Tente com um perfil de navegador diferente (ou seja, Chrome - adicionar pessoa).

Outras questões

Pergunta:	Resposta:
Minhas cotas duras do Qtree estão sendo exibidas corretamente em consultas, mas minhas cotas suaves estão sendo exibidas como a capacidade total do volume. Está correto?	Somente cotas rígidas — definidas manualmente ou definidas através do Trident—serão exibidas como as cotas definidas; se nenhuma cota rígida for especificada, a capacidade do Qtree será a capacidade de volume interno.
Eu tenho uma cota suave e uma cota rígida manualmente definida no mesmo Qtree, mas a capacidade total exibida é a cota rígida; isso está correto?	Sim, se for especificada uma cota rígida, essa será mostrada como a capacidade total.
Ao inserir um horário de programação de relatórios do Cognos, às vezes eu acabo com um "m" extra no horário de programação. Por exemplo, se eu inserir a hora como "02:15 PM", ele pode adicionar um caractere extra: "02:15 PMM" (ou PMM). Quando eu clico fora, ele muda para "2:15 AM". Posso salvar o relatório, mas quando reabro o relatório salvo, a hora do horário aparece como AM (ou seja, manhã), independentemente de eu ter inserido AM ou PM na hora do horário.	Volte a introduzir a hora da programação, tendo o cuidado de não introduzir os caracteres "AM" ou "PM" completos; basta introduzir "A" para "AM" ou "P" para "PM". Se não for apresentado o caráter extra, a hora de programação será definida corretamente.

Recursos

Dicas adicionais de solução de problemas podem ser encontradas no ["Base de conhecimento da NetApp"](#) (login de suporte necessário).

Informações adicionais de suporte podem ser encontradas na página Insights de infraestrutura de dados "[Suporte](#)".

Se você tiver uma assinatura ativa do Data Infrastructure Insights, poderá usar estas opções de suporte:

"[Telefone](#)" "[Ticket de suporte](#)"

Para obter mais informações, consulte "[Documentação de suporte do Data Infrastructure Insights](#)".

Solução de problemas da Unidade de aquisição no Linux

Aqui você encontrará sugestões para solucionar problemas com unidades de aquisição em um servidor Linux.

Problema:	Tente isto:
O status da AU na página observabilidade > coletores na guia unidades de aquisição exibe "certificado expirado" ou "certificado revogado".	Clique no menu à direita da AU e selecione Restaurar conexão . Siga as instruções para restaurar a sua Unidade de aquisição: 1. Pare o serviço da unidade de aquisição (AU). Você pode clicar no botão <i>Copy Stop Command</i> para copiar rapidamente o comando para a área de transferência e, em seguida, colar esse comando em um prompt de comando na máquina da unidade de aquisição. 2. Crie um arquivo chamado "token" na pasta <i>/var/lib/NetApp/cloudinsights/acq/conf</i> na AU. 3. Clique no botão <i>Copy Token</i> e cole esse token no arquivo que você criou. 4. Reinicie o serviço AU. Clique no botão <i>Copy Restart Command</i> e cole o comando em um prompt de comando na AU.
Permissão negada ao iniciar o Serviço de servidor da Unidade de aquisição	Quando a AU é instalada no SELINUX, se deve ser definido para o modo <i>permissivo</i> . O modo <i>imforing</i> não é suportado. Depois de definir O SELINUX para o modo permissivo, reinicie o serviço AU. " Saiba mais ".
Requisitos de servidor não atendidos	Certifique-se de que o servidor da Unidade de aquisição ou VM atende " requisitos "
Requisitos de rede não atendidos	Verifique se o servidor/VM da Unidade de aquisição pode acessar seu ambiente de Insights de infraestrutura de dados (<environment-name>.C01.cloudinsights.NetApp.com) por meio de conexão SSL pela porta 443. Tente os seguintes comandos: <i>Ping <environment-name>.C01.cloudinsights.NetApp.com</i> <i>traceroute <environment-name>.C01.cloudinsights.NetApp.com</i> <i>curl://<environment-name>.C01.cloudinsights.NetApp.com</i> <i>wget://<environment-name>.C01.cloudinsights.NetApp.com</i> Note que a porta 443 precisa ser aberta para "a infra-estrutura de saída".

Servidor proxy não configurado corretamente	Verifique suas configurações de proxy e desinstale/reinstale o software da Unidade de aquisição, se necessário, para inserir as configurações de proxy corretas. 1. Tente "curl". Consulte a informação/documentação "man curl" sobre proxies: --preproxy, --proxy-* (isso é um curinga "*" porque o curl suporta muitas configurações de proxy). 2. Tente "wget". Verifique a documentação para opções de proxy.
A instalação da unidade de aquisição falhou no Data Infrastructure Insights com erros de credenciais ao iniciar o serviço de aquisição (e visível no acq.log).	Isso pode ser causado pela inclusão de caracteres especiais nas credenciais do proxy. Desinstale o AU (<i>sudo cloudinsights-uninstall.sh</i>) e reinstale sem usar caracteres especiais.
Linux: Biblioteca / arquivo ausente não encontrado	Certifique-se de que o servidor/VM da Unidade de aquisição do Linux tenha todas as bibliotecas necessárias. Por exemplo, você deve ter a biblioteca <i>unzip</i> instalada no servidor. Para instalar a biblioteca <i>unzip</i> , execute o comando <i>*sudo yum install unzip*</i> antes de executar o script de instalação da Unidade de aquisição
Problemas de permissão	Certifique-se de que você está conectado como um usuário com permissões <i>sudo</i>
Aquisição não em execução:	Reunir o acq.log de /opt/NetApp/cloudsights/acq/logs (Linux) reinicie o Serviço de aquisição: Sudo <i>cloudinsights-service.sh restart acquisition</i>
Problemas de coleta de dados:	Envie um relatório de erro da página inicial do Data Collector clicando no botão "Enviar relatório de erro"
Status: Heartbeat falhou	A unidade de aquisição (AU) envia um batimento cardíaco ao Data Infrastructure Insights a cada 60 segundos para renovar sua concessão. Se a chamada de heartbeat falhar devido a problemas de rede ou Insights de infraestrutura de dados não responsivos, o tempo de concessão da AU não será atualizado. Quando o tempo de concessão da UA expira, o Data Infrastructure Insights mostra um status de "Heartbeat Failed". Etapas de solução de problemas: Verifique a conexão de rede entre o servidor de Unidade de aquisição e o CloudInsights. Verifique se o serviço Unidade de aquisição está em execução. Se o serviço não estiver em execução, inicie o serviço. Verifique o registro da unidade de aquisição (/var/log/NetApp/cloudinsights/acq/acq.log) para ver se existem erros.
Estou vendo uma mensagem "Heartbeat Error:"	Esse erro pode ocorrer se houver uma interrupção da rede que faça com que a comunicação entre a Unidade de aquisição e o ambiente Data Infrastructure Insights seja interrompida por mais de um minuto. Verifique se a conexão entre a AU e o Data Infrastructure Insights está estável e ativa.

Ao reinstalar a Unidade de aquisição, estou vendo "ValueError: Contexto de arquivo para /opt/NetApp/cloudinsights(/.*)? Já definido".

Em um sistema com SELinux, essa mensagem de erro pode aparecer depois de `cloudinsights-uninstall.sh -p` ter sido executada e a Unidade de aquisição deve ser reinstalada. Executar o comando `semanage fcontext -d -t usr_t "/opt/netapp/cloudinsights(/.*)?"` deve corrigir o problema e remover a mensagem.

Considerações sobre Proxies e firewalls

Se a sua organização exigir o uso de proxy para acesso à Internet, talvez seja necessário entender o comportamento de proxy da sua organização e buscar certas exceções para que o Data Infrastructure Insights funcione. Tenha em mente o seguinte:

- Primeiro, sua organização bloqueia o acesso por padrão e só permite o acesso a sites/domínios específicos por exceção? Em caso afirmativo, você precisará adicionar o seguinte domínio à lista de exceções:

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

Sua Unidade de aquisição do Data Infrastructure Insights, bem como suas interações em um navegador da Web com o Data Infrastructure Insights, serão todos enviados para hosts com esse nome de domínio.

- Em segundo lugar, alguns proxies tentam executar a inspeção TLS/SSL, personificando sites da Web Insights de infraestrutura de dados com certificados digitais não gerados pelo NetApp. O modelo de segurança da Unidade de aquisição do Data Infrastructure Insights é fundamentalmente incompatível com essas tecnologias. Você também precisaria do nome de domínio acima excetuado dessa funcionalidade para que a Unidade de aquisição do Data Infrastructure Insights faça login com sucesso no Data Infrastructure Insights e facilite a descoberta de dados.

Caso o proxy esteja configurado para inspeção de tráfego, o ambiente Data Infrastructure Insights deve ser adicionado a uma lista de exceções na configuração do proxy. O formato e a configuração dessa lista de exceções variam de acordo com o ambiente proxy e as ferramentas, mas, em geral, você deve adicionar os URLs dos servidores Data Infrastructure Insights a essa lista de exceções para permitir que a AU se comunique adequadamente com esses servidores.

A maneira mais simples de fazer isso é adicionar o próprio domínio Data Infrastructure Insights à lista de exceções:

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

No caso em que o proxy não está configurado para inspeção de tráfego, uma lista de exceções pode ou não ser necessária. Se você não tiver certeza se precisa adicionar o Data Infrastructure Insights a uma lista de exceções, ou se tiver dificuldades em instalar ou executar o Data Infrastructure Insights devido à configuração de proxy e/ou firewall, fale com sua equipe de administração de proxy para configurar o gerenciamento do proxy de intercetação SSL.

Visualização de endpoints Proxy

Você pode visualizar seus endpoints proxy clicando no link **Configurações de proxy** ao escolher um coletor de dados durante a integração ou no link em *Configurações de proxy* na página **Ajuda > suporte**. Uma tabela como a seguinte é exibida. Se você tiver o Workload Security no seu ambiente, os URLs de endpoint configurados também serão exibidos nesta lista.

Proxy Settings ✕

i If your organization requires proxy usage for internet access, you need to understand your organization's proxy behavior and seek certain exceptions for Cloud Insights to work. The simplest way is to add the following domains to the exception list:

Hostname	Port	Protocol	Methods	Endpoint URL Purpose
qtrjkso.proxyserver.cloudinsights-dev.netapp.com	443	https	GET, POST, PATCH, PUT, DELETE	Tenant
00b1100.1234.abcd.12bc.a1b2c3ef56a7.proxyserver.cloudinsights-dev.netapp.com	443	https	GET, POST, PATCH, PUT, DELETE	Acquisition Unit Ingestion
aulogin.proxyserver.cloudinsights-dev.netapp.com	443	https	GET, POST, PATCH, PUT, DELETE	Acquisition Unit Authentication
portal.proxy.cloud.netapp.com	443	https	GET, POST, PATCH, PUT, DELETE	Gateway

Close

Recursos

Dicas adicionais de solução de problemas podem ser encontradas no ["Base de conhecimento da NetApp"](#) (login de suporte necessário).

Informações adicionais de suporte podem ser encontradas na página Insights de infraestrutura de dados ["Suporte"](#).

Solução de problemas da Unidade de aquisição no Windows

Aqui você encontrará sugestões para solucionar problemas com unidades de aquisição em um servidor Windows.

Problema:	Tente isto:
O status da AU na página observabilidade > coletores na guia unidades de aquisição exibe "certificado expirado" ou "certificado revogado".	Clique no menu à direita da AU e selecione Restaurar conexão . Siga as instruções para restaurar a sua Unidade de aquisição: 1. Pare o serviço da unidade de aquisição (AU). Você pode clicar no botão <i>Copy Stop Command</i> para copiar rapidamente o comando para a área de transferência e, em seguida, colar esse comando em um prompt de comando na máquina da unidade de aquisição. 2. Crie um arquivo com o nome "token" na pasta <i>c: Arquivos de programas Cloud Insights na AU</i> . 3. Clique no botão <i>_Copy Token</i> e cole esse token no arquivo que você criou. 4. Reinicie o serviço AU. Clique no botão <i>Copy Restart Command</i> e cole o comando em um prompt de comando na AU.

Requisitos de servidor não atendidos	Certifique-se de que o servidor da Unidade de aquisição ou VM atende " requisitos "
Requisitos de rede não atendidos	Verifique se o servidor/VM da Unidade de aquisição pode acessar seu ambiente de Insights de infraestrutura de dados (<environment-name>.C01.cloudinsights.NetApp.com) por meio de conexão SSL pela porta 443. Tente os seguintes comandos: <i>Ping <environment-name>.C01.cloudinsights.NetApp.com</i> <i>traceroute <environment-name>.C01.cloudinsights.NetApp.com</i> <i>curl://<environment-name>.C01.cloudinsights.NetApp.com</i> <i>wget://<environment-name>.C01.cloudinsights.NetApp.com</i> Note que a porta 443 precisa ser aberta para "a infra-estrutura de saída".
Servidor proxy não configurado corretamente	Verifique suas configurações de proxy e desinstale/reinstale o software da Unidade de aquisição, se necessário, para inserir as configurações de proxy corretas. 1. Tente "curl". Consulte a informação/documentação "man curl" sobre proxies: --preproxy, --proxy-* (isso é um curinga "*" porque o curl suporta muitas configurações de proxy). 2. Tente "wget". Verifique a documentação para opções de proxy.
A instalação da unidade de aquisição falhou no Data Infrastructure Insights com erros de credenciais ao iniciar o serviço de aquisição (e visível no acq.log).	Isso pode ser causado pela inclusão de caracteres especiais nas credenciais do proxy. Desinstale o AU (<i>sudo cloudinsights-uninstall.sh</i>) e reinstale sem usar caracteres especiais.
Problemas de permissão	Certifique-se de que você está conectado como um usuário com permissões de administrador
Aquisição não em execução	Você pode encontrar informações no acq.log na pasta <install directory> Cloud Insights Reinicie a aquisição através dos Serviços do Windows
Problemas de coleta de dados	Envie um relatório de erro da página inicial do Data Collector clicando no botão "Enviar relatório de erro"

Status: Heartbeat falhou	A unidade de aquisição (AU) envia um batimento cardíaco ao Data Infrastructure Insights a cada 60 segundos para renovar sua concessão. Se a chamada de heartbeat falhar devido a problemas de rede ou Insights de infraestrutura de dados não responsivos, o tempo de concessão da AU não será atualizado. Quando o tempo de concessão da UA expira, o Data Infrastructure Insights mostra um status de "Heartbeat Failed". Etapas de solução de problemas: * Verifique a conexão de rede entre o servidor de Unidade de aquisição e o CloudInsights. * Verifique se o serviço Unidade de aquisição está em execução. Se o serviço não estiver em execução, inicie o serviço. * Verifique o log da unidade de aquisição (<Install dir>:/Program Files/Cloud Insights/acq.log) para ver se existem erros.
Estou vendo uma mensagem "Heartbeat Error:	Esse erro pode ocorrer se houver uma interrupção da rede que faça com que a comunicação entre a Unidade de aquisição e o ambiente Data Infrastructure Insights seja interrompida por mais de um minuto. Verifique se a conexão entre a AU e o Data Infrastructure Insights está estável e ativa.

Considerações sobre Proxies e firewalls

Se a sua organização exigir o uso de proxy para acesso à Internet, talvez seja necessário entender o comportamento de proxy da sua organização e buscar certas exceções para que o Data Infrastructure Insights funcione. Tenha em mente o seguinte:

- Primeiro, sua organização bloqueia o acesso por padrão e só permite o acesso a sites/domínios específicos por exceção? Em caso afirmativo, você precisará adicionar o seguinte domínio à sua lista de exceções:

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

Sua Unidade de aquisição do Data Infrastructure Insights, bem como suas interações em um navegador da Web com o Data Infrastructure Insights, serão todos enviados para hosts com esse nome de domínio.

- Em segundo lugar, alguns proxies tentam executar a inspeção TLS/SSL, personificando sites da Web Insights de infraestrutura de dados com certificados digitais não gerados pelo NetApp. O modelo de segurança da Unidade de aquisição do Data Infrastructure Insights é fundamentalmente incompatível com essas tecnologias. Você também precisaria do nome de domínio acima excetuado dessa funcionalidade para que a Unidade de aquisição do Data Infrastructure Insights faça login com sucesso no Data Infrastructure Insights e facilite a descoberta de dados.

Visualização de endpoints Proxy

Você pode visualizar seus endpoints proxy clicando no link **Configurações de proxy** ao escolher um coletor de dados durante a integração ou no link em *Configurações de proxy* na página **Ajuda > suporte**. Uma tabela como a seguinte é exibida. Se você tiver o Workload Security no seu ambiente, os URLs de endpoint configurados também serão exibidos nesta lista.

i If your organization requires proxy usage for internet access, you need to understand your organization's proxy behavior and seek certain exceptions for Cloud Insights to work. The simplest way is to add the following domains to the exception list:

Hostname	Port	Protocol	Methods	Endpoint URL Purpose
qtrjkso.proxyserver.cloudinsights-dev.netapp.com	443	https	GET, POST, PATCH, PUT, DELETE	Tenant
00b1100.1234.abcd.12bc.a1b2c3ef56a7.proxyserver.cloudinsights-dev.netapp.com	443	https	GET, POST, PATCH, PUT, DELETE	Acquisition Unit Ingestion
aulogin.proxyserver.cloudinsights-dev.netapp.com	443	https	GET, POST, PATCH, PUT, DELETE	Acquisition Unit Authentication
portal.proxy.cloud.netapp.com	443	https	GET, POST, PATCH, PUT, DELETE	Gateway

Close

Recursos

Dicas adicionais de solução de problemas podem ser encontradas no ["Base de conhecimento da NetApp"](#) (login de suporte necessário).

Informações adicionais de suporte podem ser encontradas na página Insights de infraestrutura de dados ["Suporte"](#).

Pesquisando um coletor de dados com falha

Se um coletor de dados tiver uma mensagem de falha e um impacto Alto ou Médio, você precisará pesquisar esse problema usando a página de resumo do coletor de dados com suas informações vinculadas.

Siga as etapas a seguir para determinar a causa dos coletores de dados com falha. As mensagens de falha do coletor de dados são exibidas no menu **Admin** e na página **Installed Data Collectors**.

Passos

1. Clique em **Admin > coletores de dados > coletores de dados instalados**.
2. Clique no Nome vinculado do coletor de dados com falha para abrir a página Resumo.
3. Na página Resumo, verifique a área Comentários para ler quaisquer notas que possam ter sido deixadas por outro engenheiro que também possa estar investigando essa falha.
4. Anote todas as mensagens de desempenho.
5. Mova o ponteiro do Mouse sobre os segmentos do gráfico da linha de tempo do evento para exibir informações adicionais.
6. Selecione uma mensagem de erro para um dispositivo e exibida abaixo da linha do tempo do evento e clique no ícone Detalhes do erro que é exibido à direita da mensagem.

Os detalhes do erro incluem o texto da mensagem de erro, causas mais prováveis, informações em uso e sugestões do que pode ser tentado para corrigir o problema.

7. Na área dispositivos reportados por este coletor de dados, você pode filtrar a lista para exibir apenas os dispositivos de interesse, e você pode clicar no **Nome** vinculado de um dispositivo para exibir a página de ativos desse dispositivo.
8. Quando você retornar à página de resumo do coletor de dados, marque a área **Mostrar alterações recentes** na parte inferior da página para ver se as alterações recentes poderiam ter causado o problema.

Matriz de suporte do Data Infrastructure Insights Data Collector

A Matriz de suporte do Data Collector fornece referência para coletores de dados suportados pelo Data Infrastructure Insights, incluindo informações de fornecedor e modelo.

Armazenamento HP Enterprise 3PAR/Alletra 9000/Primera StoreServ

Modelos e versões suportados por este coletor de dados:

Modelos	Versões de firmware
HPE ALLETRA HPE_T800 HPE_3PAR 7440C V400 HPE_3PAR 20850 HPE_3PAR 20850_R2 HPE_9080 HPE_3PAR 20450 HPE_3PAR 7200C HPE_3PAR 7400 HPE_3PAR 7200 HPE_3PAR A670 HPE_3PAR 20800 HPE_3PAR A650 HPE_3PAR 9450 HPE_3PAR A630 HPE_3PAR 8440 HPE_3PAR 8450 HPE_3PAR 8400 HP_3PAR 7450C HP_3PAR 8200 HP_F400 HP_3PAR 7200C HP_3PAR 7400 HP_3PAR 7450C HP_T400 HP_3PAR 8400 HP_3PAR 20800 HP_3PAR 8200 HP_3PAR 7400C	3.1.1 (MU1) 3.1.2 (MU1) 4.4.1 (4.5.11) 3.3.1 (MU5) 3.3.2 3.3.2 (MU1) 3.3.1 (MU2) 3.2.2 (MU6) 3.3.1 (MU2) 3.2.2 (MU4) 3.2.1 (MU5) 3.2.2 3.2.2 (MU3) 3.2.1 (MU3) 3.1.3 (MU2) 3.1.3 (MU3) 3.1.3 tipo de versão: Suporte padrão versão MU1 tipo de versão: Suporte estendido versão 4.5.3 tipo de versão: Suporte estendido 4.5.7 tipo de versão: Suporte estendido versão 9.5.8

Produtos suportados por este coletor de dados:

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
fundação					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/Atributo	Estado	Protocolo	Informações adicionais
			Folga	Utilizado	
		protocolo			
		Porta de armazenamento	Implementado	SSH	
		Iniciador	Implementado	SSH	
		Controlador de protocolo	Implementado	SSH	
		Porta de armazenamento	Implementado	SSH	
		Tipo	Folga	SSH	
	Máscara de volume				
	Ref. Volume	Nome	Implementado	SSH	
		IP de armazenamento	Implementado	SSH	
	WWN Alias	Aliases de host	Implementado	SSH	
		Tipo Objeto	Implementado	SSH	
		Fonte	Implementado	SSH	
		WWN	Implementado	SSH	

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
desempenho					
626					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

					todos os discos) em MB/s.
		Gravação de Característica/Atributo	Implementado	SMI-S	
Produto	Categoria	Gravação de Característica/Atributo	Estado	Protocolo utilizado	Informações adicionais
		Escrever pendente	Implementado	SMI-S	total de escrita pendente

APIs de gerenciamento usadas por este coletor de dados:

API	Protocolo utilizado	Protocolo da camada de transporte utilizado	Portas de entrada usadas	Portas de saída usadas	Suporta autenticação	Requer apenas credenciais "só de leitura"	Suporta criptografia	Firewall amigável (portas estáticas)
3PAR SMI-S	SMI-S	HTTP/HTTPS	5988/5989		verdadeiro	verdadeiro	verdadeiro	verdadeiro
3Par CLI	SSH	SSH	22		verdadeiro	falso	verdadeiro	verdadeiro

Amazon AWS EC2

Modelos e versões suportados por este coletor de dados:

Versões da API:

- 1 de outubro de 2014

Produtos suportados por este coletor de dados:

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
fundação					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

	Disk	OID do VirtualDisk	Implementado	HTTPS	
Produto	Categoria	Característica/Attribute	Estado	Protocolo utilizado	Informações adicionais
	Host	Sistema operacional de host	Implementado	HTTPS	
		IPS	Implementado	HTTPS	
		Fabricante	Implementado	HTTPS	
		Nome	Implementado	HTTPS	
		OID	Implementado	HTTPS	
	Informações	Descrição da API	Implementado	HTTPS	
		Nome da API	Implementado	HTTPS	
		Versão da API	Implementado	HTTPS	
		Nome da fonte de dados	Implementado	HTTPS	Informações
		Data	Implementado	HTTPS	
		ID do originador	Implementado	HTTPS	
		Chave originadora	Implementado	HTTPS	

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
desempenho					
636					

Produto	Categoria	Característica/Atributo	Estado	Protocolo utilizado	Informações adicionais
		Gravação de Característica/Atributo	Implementado	HTTPS	
		Gravação de Característica/Atributo	Implementado	HTTPS	
	vm	Capacidade total	Implementado	HTTPS	
	vm	Capacidade utilizada	Implementado	HTTPS	
	vm	Relação capacidade utilizada	Implementado	HTTPS	
	vm	Utilização total da CPU	Implementado	HTTPS	
	vm	Leitura de IOPS	Implementado	HTTPS	Número de IOPS de leitura no disco
	vm	Disklops.Total	Implementado	HTTPS	
	vm	Gravação de IOPs de disco	Implementado	HTTPS	
	vm	Leitura de latência	Implementado	HTTPS	
	vm	Total de latência	Implementado	HTTPS	
	vm	Gravação de latência	Implementado	HTTPS	
	vm	Taxa de transferência do disco lida	Implementado	HTTPS	
	vm	Taxa de transferência de leitura	Implementado	HTTPS	leitura da taxa de transferência total do disco
	vm	Gravação da taxa de transferência do disco	Implementado	HTTPS	
	vm	Taxa de transferência IP lida	Implementado	HTTPS	
	vm	Taxa de transferência total	Implementado	HTTPS	Taxa de transferência IP total
	vm	IpThroughput.write	Implementado	HTTPS	
	vm	Utilização total da memória	Implementado	HTTPS	

APIs de gerenciamento usadas por este coletor de dados:

API	Protocolo utilizado	Protocolo da camada de transporte utilizado	Portas de entrada usadas	Portas de saída usadas	Suporta autenticação	Requer apenas credenciais "só de leitura"	Suporta criptografia	Firewall amigável (portas estáticas)
EC2 API	HTTPS	HTTPS	443		verdadeiro	verdadeiro	verdadeiro	verdadeiro

Amazon AWS S3

Modelos e versões suportados por este coletor de dados:

Modelos	Versões de firmware
S3	1 de agosto de 2010

Produtos suportados por este coletor de dados:

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
fundação					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/Atributo	Estado	Protocolo utilizado	Informações adicionais
	Pool de storage	Incluir na capacidade DWH	Implementado	HTTPS	Uma maneira de ACQ para cotnrol que piscinas de estroage são interessantes na capacidade DWH
		Nome	Implementado	HTTPS	
		Capacidade do disco físico (MB)	Implementado	HTTPS	usado como capacidade bruta para pool de storage
		Grupo RAID	Implementado	HTTPS	Indica se esse storagePool é um grupo raid
		Relação bruta/utilizável	Implementado	HTTPS	taxa para converter de capacidade utilizável para capacidade bruta
		ID do conjunto de armazenamento	Implementado	HTTPS	
		Thin Provisioning suportado	Implementado	HTTPS	Se esse volume interno é compatível com thin Provisioning para a camada de volume em cima dele
		Capacidade total alocada	Implementado	HTTPS	
		Tipo	Folga	HTTPS	
		Virtual	Implementado	HTTPS	Este é um dispositivo de virtualização de armazenamento ?

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
desempenho	Volume interno	Capacidade total	Implementado	HTTPS	
		Capacidade utilizada	Implementado	HTTPS	
		Relação capacidade utilizada	Implementado	HTTPS	
		Total de objetos	Implementado	HTTPS	

APIs de gerenciamento usadas por este coletor de dados:

API	Protocolo utilizado	Protocolo da camada de transporte utilizado	Portas de entrada usadas	Portas de saída usadas	Suporta autenticação	Requer apenas credenciais "só de leitura"	Suporta criptografia	Firewall amigável (portas estáticas)
S3 API	HTTPS	HTTPS	443		verdadeiro	verdadeiro	verdadeiro	verdadeiro

Microsoft Azure NetApp Files

Modelos e versões suportados por este coletor de dados:

Versões de API	Modelos
1 de junho de 2019	Azure NetApp Files

Produtos suportados por este coletor de dados:

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
fundação					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

		alocada			
Produto	Categoria	Capacidade total utilizada	Implementado	HTTPS	Capacidade total em MB
		Característica/Atributo	Estado Folga	Protocolo utilizado	Informações adicionais
		Virtual	Implementado	HTTPS	Este é um dispositivo de virtualização de armazenamento ?

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
desempenho					
650					

Produto	Categoria	Característica/Atributo	Capacidade de dados utilizados	Implementado	Protocolo utilizado	Informações adicionais
			Estado			
Disco do StoragePool		Leitura de IOPS	Implementado			Número de IOPS de leitura no disco
		Total de IOPS	Implementado			
		Gravação de IOPS	Implementado			
		Taxa de transferência de leitura	Implementado			
		Taxa de transferência total	Implementado			Taxa total média do disco (leitura e gravação em todos os discos) em MB/s.
		Gravação de taxa de transferência	Implementado			

APIs de gerenciamento usadas por este coletor de dados:

API	Protocolo utilizado	Protocolo da camada de transporte utilizado	Portas de entrada usadas	Portas de saída usadas	Suporta autenticação	Requer apenas credenciais "só de leitura"	Suporta criptografia	Firewall amigável (portas estáticas)
API REST do Azure NetApp Files	HTTPS	HTTPS	443		verdadeiro	verdadeiro	verdadeiro	verdadeiro

Switches Fibre Channel Brocade

Modelos e versões suportados por este coletor de dados:

Modelos	Versões de firmware
4 Brocade X6 Brocade incorporado X7 Brocade 5000 Brocade 5100 Brocade 8 Brocade X7 Brocade G620 Brocade X6 Brocade 4 Brocade DCX8510 Brocade G630 Brocade G720 Brocade G610 Brocade DCX Brocade DCX-4S backbone Brocade DCX8510-4 Brocade 6548-8 Brocade 7840 Brocade 6505 Brocade 7800 Brocade 6520 Brocade M5424 Brocade 4024 Brocade 6510-5480 Brocade 5300-8 Brocade 200E-48000 Brocade 3900 Brocade 300E-178,0 183,0	v5,3 1d v8,2 2c v8,2 3 v8,2 3b v8,2 0b v9,0 1c v9,0 v9,1 1.2j v8,1 0b v8,2 2a v8,2 2d v8,2 3a v8,2 3c v8,2 1a v9,0 1d v9,0 0b v9,1 01 v9,1.2k v8,2 1c v8,2 2b v8,2 v8,2 v8,2 v9,0 v9,0 1e v9,0 1 v9,1 1b.2g v8,1.2c v8,0.2d v8,1.2a v8,0.2h v7,4.v8,0.01 v7,4.2g.824494.2g v7,4.2c v7,4.2d v7,4.2a v7,4.1d v7,4.1f v7,4.1d v7,4.0c v7,3_cvr_0c v7,3_1b v7,1.2a v7,0.2j1 0 v7,0.2 v6,4.2 v6,4.1a v6,4.2g v6,3.2c v6,2.1b v6,2.0 v8,2

Produtos suportados por este coletor de dados:

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
fundação					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

	Zona	Nome da zona	Implementado	SSH	
Produto	Membro da zona Categoria	Tipo	Folga	SSH	Informações adicionais
		Característica/A WWN	Estado Implementado	Protocolo SSH	
	Capacidades de zoneamento	Configuração ativa	Implementado	SSH	
		Nome da configuração	Implementado	SSH	
		Comportamento de Zoneamento padrão	Implementado	SSH	
		WWN	Implementado	SSH	

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
desempenho					
658					

Produto	Categoria	Característica/Atributo	Estado	Protocolo utilizado	Informações adicionais
		Taxa de fotogramas de trânsito	Implementado	SNMP	
		Taxa de trânsito total	Implementado	SNMP	
		Taxa de fotogramas de trânsito	Implementado	SNMP	
		Tamanho médio do quadro	Implementado	SNMP	Tamanho médio do quadro de tráfego
		Fotogramas TX	Implementado	SNMP	tamanho médio do quadro de tráfego
		Taxa de trânsito	Implementado	SNMP	
		Taxa de trânsito total	Implementado	SNMP	
		Taxa de trânsito	Implementado	SNMP	
		Utilização do tráfego	Implementado	SNMP	
		Utilização do tráfego	Implementado	SNMP	Utilização total do tráfego
		Utilização do tráfego	Implementado	SNMP	

APIs de gerenciamento usadas por este coletor de dados:

API	Protocolo utilizado	Protocolo da camada de transporte utilizado	Portas de entrada usadas	Portas de saída usadas	Suporta autenticação	Requer apenas credenciais "só de leitura"	Suporta criptografia	Firewall amigável (portas estáticas)
SNMP do Brocade	SNMP	SNMPv1, SNMPv2, SNMPv3	161		verdadeiro	verdadeiro	verdadeiro	verdadeiro
SSH do Brocade	SSH	SSH	22		falso	falso	verdadeiro	verdadeiro
Configuração do assistente de origem de dados	Introdução manual				verdadeiro	verdadeiro	verdadeiro	verdadeiro

Consultor de rede Brocade

Modelos e versões suportados por este coletor de dados:

Versões de API	Modelos	Versões de firmware
14.4.1 14.4.3 14.4.4 14.4.5	Brocade 5300 Brocade 6510 Brocade 6520 Brocade 6548 Brocade DCX 8510-8 Brocade G620 DS-6620B EMC Connectrix ED-DCX8510-8B	v7.2.1a v7.3.1a v7.4.1b v7.4.2d v8.2.3b v8.2.3c v9.0.1a v9.0.1b v9.0.1e1

Produtos suportados por este coletor de dados:

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
fundação					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/Atributo	Estado	Protocolo utilizado	Informações adicionais
		Característica/Atributo	Estado	Protocolo utilizado	
		gigabits			
		Conetividade desconhecida	Implementado	HTTP/S	
		Característica/Atributo	Implementado	HTTP/S	
	Interrutor	ID do domínio	Implementado	HTTP/S	
		Versão do firmware	Implementado	HTTP/S	
		IP	Implementado	HTTP/S	
		Gerenciar URL	Implementado	HTTP/S	
		Fabricante	Implementado	HTTP/S	
		Modelo	Implementado	HTTP/S	
		Nome	Implementado	HTTP/S	
		Número de série	Implementado	HTTP/S	
		Função do interruptor	Implementado	HTTP/S	
		Estado do interruptor	Implementado	HTTP/S	
		Estado do interruptor	Implementado	HTTP/S	
		Tipo	Folga	HTTP/S	
		WWN	Implementado	HTTP/S	
	Desconhecido	Condutor	Implementado	HTTP/S	
		Firmware	Implementado	HTTP/S	
		Fabricante	Implementado	HTTP/S	
		Modelo	Implementado	HTTP/S	
		WWN	Implementado	HTTP/S	
	WWN Alias	Aliases de host	Implementado	HTTP/S	
		Tipo Objeto	Implementado	HTTP/S	
		Fonte	Implementado	HTTP/S	
		WWN	Implementado	HTTP/S	
	Zona	Nome da zona	Implementado	HTTP/S	
	Membro da zona	Tipo	Folga	HTTP/S	
		WWN	Implementado	HTTP/S	
	Capacidades de zoneamento	Configuração ativa	Implementado	HTTP/S	
		Nome da configuração	Implementado	HTTP/S	
		WWN	Implementado	HTTP/S	

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
desempenho	porta	BbCreditZero.Total	Implementado	HTTP/S	
		Crédito BB	Implementado	HTTP/S	
		BbCreditZeroMs	Implementado	HTTP/S	
		portErrors.class3 Discard	Implementado	HTTP/S	
		PortErrors.crc	Implementado	HTTP/S	
		Erro de porta	Implementado	HTTP/S	
		Erro de porta	Implementado	HTTP/S	Erros de porta devido a quadro curto
		PortErrors.linkFailure	Implementado	HTTP/S	Falha no link erros de porta
		Erro de porta	Implementado	HTTP/S	Perda de sinal de erros de porta
		Erro de porta	Implementado	HTTP/S	Perda de sincronização de erro de porta
		Erro de porta	Implementado	HTTP/S	eliminação do tempo limite dos erros da porta
		Erro de porta	Implementado	HTTP/S	Total de erros de porta
		Taxa de trânsito	Implementado	HTTP/S	
		Taxa de trânsito total	Implementado	HTTP/S	
		Taxa de trânsito	Implementado	HTTP/S	
		Utilização do tráfego	Implementado	HTTP/S	
		Utilização do tráfego	Implementado	HTTP/S	Utilização total do tráfego
Utilização do tráfego	Implementado	HTTP/S			

APIs de gerenciamento usadas por este coletor de dados:

API	Protocolo utilizado	Protocolo da camada de transporte utilizado	Portas de entrada usadas	Portas de saída usadas	Suporta autenticação	Requer apenas credenciais "só de leitura"	Suporta criptografia	Firewall amigável (portas estáticas)
API REST do consultor de rede Brocade	HTTP/HTTPS	HTTP/HTTPS	80/443		verdadeiro	verdadeiro	verdadeiro	verdadeiro

Brocade FOS REST

Modelos e versões suportados por este coletor de dados:

Modelos	Versões de firmware
Brocade 6505 Brocade G720 Brocade X6-8	v8.2.3c v8.2.3c1 v9.0.1e1 v9.1.1b

Produtos suportados por este coletor de dados:

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
fundação					
666					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

	Zona	Nome da zona	Implementado	HTTPS	
Produto	Membro da zona Categoria	Tipo	Folga	HTTPS	Informações adicionais
		Característica/A WWN	Estado Implementado	Protocolo HTTPS	
	Capacidades de zoneamento	Configuração ativa	Implementado	HTTPS	
		Nome da configuração	Implementado	HTTPS	
		Comportamento de Zoneamento padrão	Implementado	HTTPS	
		WWN	Implementado	HTTPS	

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
desempenho					
670					

Produto	Categoria	Característica/Atributo	Estado	Protocolo utilizado	Informações adicionais
		Taxa de trânsito total	Implementado	HTTPS	
		Tamanho médio do quadro	Implementado	HTTPS	Tamanho médio do quadro de tráfego
		Fotogramas TX	Implementado	HTTPS	tamanho médio do quadro de tráfego
		Taxa de trânsito	Implementado	HTTPS	
		Taxa de trânsito total	Implementado	HTTPS	
		Taxa de trânsito	Implementado	HTTPS	
		Utilização do tráfego	Implementado	HTTPS	
		Utilização do tráfego	Implementado	HTTPS	Utilização total do tráfego
		Utilização do tráfego	Implementado	HTTPS	

APIs de gerenciamento usadas por este coletor de dados:

API	Protocolo utilizado	Protocolo da camada de transporte utilizado	Portas de entrada usadas	Portas de saída usadas	Suporta autenticação	Requer apenas credenciais "só de leitura"	Suporta criptografia	Firewall amigável (portas estáticas)
API REST do Brocade FOS	HTTPS		443		verdadeiro	verdadeiro	verdadeiro	verdadeiro

Switches de malha Cisco MDS e Nexus

Modelos e versões suportados por este coletor de dados:

Modelos	Versões de firmware
8978 K9 C9396T C9509 C9710 K9 C5596UP N5K 6248UP 6332-C9396S K9 C9513 C9718 K9 N5K C56128P N5K 6296UP 16UP DS-C9250I K9 C9506 C9706 8GFC C5548UP N5K C5696Q 6332 6454-K9- K9 DS-K9-48P DS-C9148T-K9 DS-32P-K9 DS- C9148-16P-K9 DS-C9148-C9134-K9 DS-C9148-K9- K9 DS-C9148S-2 DS-C9132T-C9124 DS-K9-C9124 DS-C9222I-E04 CN1610	3,3 4,21e N2 3 5,0 4,22c 5,2 3 5,2 8 5,2 8d 5,2 8h 6,2 11 6,2 11e 6,2 15 6,2 21 6,2 27 6,2 33 6,2 7 6,2 9c D1 0(3 5,0 4,21j N2 3 5,0 2D N2 6a 5,2 8c 5,2 8g 5,2 1 6,2 11c 6,2 13a 6,2 19 6,2 25 6,2 31 6,2 5a 6,2 9a 7,3 1 1) 4,13i N2 3 5,0 4,21k N2 8 5,2 2,28g 5,2 8b 5,2 8F 5,2 8i 6,2 11b 6,2 13 6,2 17 6,2 23 6,2 29 6,2 5 6,2 9 6,2 0 7,3 7,3(3) N2(5,0) N2(4,13e)3(4,04e) 5,0(N2)5,0(3) 5,0(3)N2(4,01d) N2(3,23o)3(3,11e) 5,0(N2)5,0(3) 1a(3a)5,0(4,1) 5,0(1c 1 1 7,3 1 N1 1 7,3 13 N1 1 7,3 6 N1 1 7,3 8 N1 1 8,1 1 8,1 1a 8,1 1b 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 1 9,2 1a 9,2 2 9,3 2 9,3 2a 9,3 5 l42 2a 9,3 5 l42 2c

Produtos suportados por este coletor de dados:

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
fundação					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	VSAN atiyado	Folga	SNMP	Informações adicionais
		Característica/Atributo	Estado	Protocolo Utilizado	
	Desconhecido	Conductor	Implementado	SNMP	
		Firmware	Implementado	SNMP	
		Gerado	Implementado	SNMP	
		Fabricante	Implementado	SNMP	
		Modelo	Implementado	SNMP	
		Nome	Implementado	SNMP	
		WWN	Implementado	SNMP	
	WWN Alias	Aliases de host	Implementado	SNMP	
		Tipo Objeto	Implementado	SNMP	
		Fonte	Implementado	SNMP	
		WWN	Implementado	SNMP	
	Zona	Nome da zona	Implementado	SNMP	
		Tipo de zona	Implementado	SNMP	
	Membro da zona	Tipo	Folga	SNMP	
		WWN	Implementado	SNMP	
	Capacidades de zoneamento	Configuração ativa	Implementado	SNMP	
		Nome da configuração	Implementado	SNMP	
		Comportamento de Zoneamento padrão	Implementado	SNMP	
		Controlo de mesclagem	Implementado	SNMP	
		WWN	Implementado	SNMP	

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
desempenho					
676					

Produto	Categoria	Característica/Atributo	Estado	Protocolo utilizado	Informações adicionais
		Tamanho médio do quadro	Implementado	SNMP	Tamanho médio do quadro de tráfego
		Fotogramas TX	Implementado	SNMP	tamanho médio do quadro de tráfego
		Taxa de trânsito	Implementado	SNMP	
		Taxa de trânsito total	Implementado	SNMP	
		Taxa de trânsito	Implementado	SNMP	
		Utilização do tráfego	Implementado	SNMP	
		Utilização do tráfego	Implementado	SNMP	Utilização total do tráfego
		Utilização do tráfego	Implementado	SNMP	

APIs de gerenciamento usadas por este coletor de dados:

API	Protocolo utilizado	Protocolo da camada de transporte utilizado	Portas de entrada usadas	Portas de saída usadas	Suporta autenticação	Requer apenas credenciais "só de leitura"	Suporta criptografia	Firewall amigável (portas estáticas)
SNMP do Cisco	SNMP	SNMPv1 (apenas inventário), SNMPv2, SNMPv3	161		verdadeiro	verdadeiro	verdadeiro	verdadeiro

Cohesity

Modelos e versões suportados por este coletor de dados:

Modelos	Versões de firmware
NÓ DE COMPUTAÇÃO C2500 C2505 C4000 C4600 C5036 C5066 C6025 C6035 C6055 PXG1 UCS-C240M5H10	6,5 6,8 20230412 u3 u1.u1 1 6,8 20230509 20230222_release-20210913 20221022 u2 1 7,0_13f6a4bf 1.1f_u1_release-20211027_9e4e40cb 6,6.0d_u6_release-20221204_c03629f0 6,8.6,5_release-20220807_6c9115ef 6,8.1_1f_release

Produtos suportados por este coletor de dados:

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
fundação					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

compatível com thin Provisioning para a camada de armazenamento adicional

Produto	Categoria	Característica/Atributo	Estado	Protocolo utilizado	Informações adicionais
		Capacidade total alocada	Implementado		
		Capacidade total utilizada	Implementado		Capacidade total em MB
		Tipo	Folga		
		Virtual	Implementado		Este é um dispositivo de virtualização de armazenamento ?
		Encriptado	Implementado		

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
desempenho					
686					

Produto	Categoria	Característica/Atributo	Estado	Protocolo utilizado	Informações adicionais	
	Total de IOPS	Implementado			Gravação de latência	
	Implementado			Total de utilização	Implementado	
			Disco do StoragePool	Leitura de IOPS	Implementado	
	Número de IOPS de leitura no disco			Gravação de IOPS	Implementado	
				Taxa de transferência de leitura	Implementado	
				Gravação de taxa de transferência	Implementado	
				Taxa de transferência total	Implementado	
				Total de IOPS	Implementado	
		Taxa total média do disco (leitura e gravação em todos os discos) em MB/s.				

APIs de gerenciamento usadas por este coletor de dados:

API	Protocolo utilizado	Protocolo da camada de transporte utilizado	Portas de entrada usadas	Portas de saída usadas	Suporta autenticação	Requer apenas credenciais "só de leitura"	Suporta criptografia	Firewall amigável (portas estáticas)
API REST Cohesity	HTTPS	HTTPS	443		verdadeiro	verdadeiro	verdadeiro	verdadeiro

EMC Celerra (SSH)

Modelos e versões suportados por este coletor de dados:

Modelos	Versões de firmware
NS-480FC NSX VG8 VNX5200 VNX5300 VNX5400 VNX5600 VNX7600	5,5.38-1 6,0.65-2 7,1.76-4 7,1.79-8 7,1.83-2 8,1.21-266 8,1.21-303 8,1.9-155

Produtos suportados por este coletor de dados:

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
fundação					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

					para a camada de volume em cima dele
Produto	Categoria	Característica/atributo	Estado	Protocolo utilizado	Informações adicionais
		Capacidade total utilizada	Implementado	SSH	Capacidade total em MB
		Tipo	Folga	SSH	
		Virtual	Implementado	SSH	Este é um dispositivo de virtualização de armazenamento ?

APIs de gerenciamento usadas por este coletor de dados:

API	Protocolo utilizado	Protocolo da camada de transporte utilizado	Portas de entrada usadas	Portas de saída usadas	Suporta autenticação	Requer apenas credenciais "só de leitura"	Suporta criptografia	Firewall amigável (portas estáticas)
CLI do Celerra	SSH	SSH			verdadeiro	falso	verdadeiro	verdadeiro

EMC CLARiiON (Navicli)

Modelos e versões suportados por este coletor de dados:

Versões de API	Modelos	Versões de firmware
6,23 6,26 6,28 7,30 7,32 7,33	AX4-5F8 CX3-20F CX3-40F CX4-480 VNX5100 VNX5200 VNX5300 VNX5400 VNX5500 VNX5600 VNX5700 VNX5800 VNX7600 VNX8000	04.28.000.5.710 04.30.000.5.525 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 05.33.009.5.155 05.33.009.5.184 05.33.009.5.186 05.33.009.5.218 05.33.009.5.231 05.33.009.5.236 05.33.009.5.238 05.33.009.6.305 05.33.021.5.256 05.33.021.5.266 2.23.50.5.710 3.26.20.5.011 3.26.40.5.029

Produtos suportados por este coletor de dados:

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
fundação					
698					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Thin Provisioning	Implementado	CLI	
		Característica/Atributo	Folga Estado	CLI Protocolo Utilizado	Informações adicionais
		Capacidade utilizada	Implementado	CLI	
	Mapa de volume	LUN	Implementado	CLI	Nome do lun de back-end
		Controlador de protocolo	Implementado	CLI	
		Porta de armazenamento	Implementado	CLI	
		Tipo	Folga	CLI	
	Máscara de volume	Iniciador	Implementado	CLI	
		Controlador de protocolo	Implementado	CLI	
		Porta de armazenamento	Implementado	CLI	
		Tipo	Folga	CLI	
	Membro do volume	Capacidade	Implementado	CLI	Capacidade de captura instantânea usada em MB
		Nome	Implementado	CLI	
		Classificação	Implementado	CLI	
		Capacidade bruta total	Implementado	CLI	Capacidade bruta total (soma de todos os discos no array)
		Redundância	Implementado	CLI	Nível de redundância
		ID do conjunto de armazenamento	Implementado	CLI	
		Capacidade utilizada	Implementado	CLI	
	WWN Alias	Aliases de host	Implementado	CLI	
		IP	Implementado	CLI	
		Tipo Objeto	Implementado	CLI	
		Fonte	Implementado	CLI	
		WWN	Implementado	CLI	

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
desempenho					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

		Total de utilização	Implementado	CLI	
Produto	Categoria	Característica/Atribuição	Estado	Protocolo utilizado	Informações adicionais
	Volume	Taxa de acerto do cache ler	Implementado	CLI	
		Taxa de acerto do cache total	Implementado	CLI	
		Cache HIT Ratio Write	Implementado	CLI	
		Capacidade bruta	Implementado	CLI	
		Capacidade total	Implementado	CLI	
		Capacidade utilizada	Implementado	CLI	
		Relação capacidade utilizada	Implementado	CLI	
		Leitura de IOPS	Implementado	CLI	Número de IOPS de leitura no disco
		Total de IOPS	Implementado	CLI	
		Gravação de IOPS	Implementado	CLI	
		Leitura de latência	Implementado	CLI	
		Total de latência	Implementado	CLI	
		Gravação de latência	Implementado	CLI	
		Relação bloqueada parcial	Implementado	CLI	
		Taxa de transferência de leitura	Implementado	CLI	
		Taxa de transferência total	Implementado	CLI	Taxa total média do disco (leitura e gravação em todos os discos) em MB/s.
		Gravação de taxa de transferência	Implementado	CLI	

APIs de gerenciamento usadas por este coletor de dados:

API	Protocolo utilizado	Protocolo da camada de transporte utilizado	Portas de entrada usadas	Portas de saída usadas	Suporta autenticação	Requer apenas credenciais "só de leitura"	Suporta criptografia	Firewall amigável (portas estáticas)
CLI NAVI	CLI		6389,2162,2163,443 (HTTPS)/80 (HTTP)		verdadeiro	verdadeiro	verdadeiro	falso

EMC Data Domain (SSH)

Modelos e versões suportados por este coletor de dados:

Modelos	Versões de firmware
DD VE DD2200 DD2500 DD3300 DD4200 DD6300 DD6800 DD6900 DD7200 DD9300 DD9400 DD9500 DD9800 DD990 DD9900	6,1.2.051-633576 6,1.2.20-606786 6,1.2.50-632120 6,2.0.30-629757 6,2.0.0-1008134.0.7-1007134 7,7.1.10-1011247 7,7.2.011-1011427 7,7.0.90-692270 7,6.0.20-689174 7,6.0.30-690691 7,7.0.50-671975 7,2.0.60-682124 7,2.0.70-686759 7,2.0-1017741 7.10.1.0-1042928 7,2.0.30-663847 7,2.1.30-663869 6,2.1.40-671977 6,2.1.60-686365 7.10.0.2.10-1011249 7,7.3.0-1011963 7,7.0.35-635767 6,2.5.1-1040473 7,7.5.11-1046187 7,8.4.0-1017976 7,7

Produtos suportados por este coletor de dados:

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
fundação					
712					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/Atributo	Estado	Protocolo utilizado	Informações adicionais
		Relação bruta/utilizável	Implementado	SSH	taxa para converter de capacidade
		ID do conjunto de armazenamento	Implementado	SSH	
		Thin Provisioning suportado	Implementado	SSH	Se esse volume interno é compatível com thin Provisioning para a camada de volume em cima dele
		Capacidade total alocada	Implementado	SSH	
		Capacidade total utilizada	Implementado	SSH	Capacidade total em MB
		Tipo	Folga	SSH	
		Virtual	Implementado	SSH	Este é um dispositivo de virtualização de armazenamento ?

APIs de gerenciamento usadas por este coletor de dados:

API	Protocolo utilizado	Protocolo da camada de transporte utilizado	Portas de entrada usadas	Portas de saída usadas	Suporta autenticação	Requer apenas credenciais "só de leitura"	Suporta criptografia	Firewall amigável (portas estáticas)
CLI do domínio de dados	SSH	SSH	22		verdadeiro	verdadeiro	verdadeiro	verdadeiro

EMC ECS

Modelos e versões suportados por este coletor de dados:

Modelos	Versões de firmware
ECS	3.6.1.1 3.6.1.3 3.6.2.1 3.6.2.4 3.7.0.0 3.7.0.3 3.7.0.4 3.7.0.5 3.8.0.1 3.8.0.2

Produtos suportados por este coletor de dados:

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
fundação					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Utilização da	Implementado	HTTPS	
		Capacidade/Atributo	Estado	Protocolo utilizado	Informações adicionais
	Pool de storage	Incluir na capacidade DWH	Implementado	HTTPS	Uma maneira de ACQ para control que piscinas de storage são interessantes na capacidade DWH
		Nome	Implementado	HTTPS	
		Capacidade do disco físico (MB)	Implementado	HTTPS	usado como capacidade bruta para pool de storage
		Grupo RAID	Implementado	HTTPS	Indica se esse storagePool é um grupo raid
		Relação bruta/utilizável	Implementado	HTTPS	taxa para converter de capacidade utilizável para capacidade bruta
		ID do conjunto de armazenamento	Implementado	HTTPS	
		Thin Provisioning suportado	Implementado	HTTPS	Se esse volume interno é compatível com thin Provisioning para a camada de volume em cima dele
		Capacidade total alocada	Implementado	HTTPS	
		Capacidade total utilizada	Implementado	HTTPS	Capacidade total em MB
		Tipo	Folga	HTTPS	
		Virtual	Implementado	HTTPS	Este é um dispositivo de virtualização de armazenamento ?

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
desempenho					

todos os discos) em MB/s.

Produto	Categoria	Característica/Atributo	Estado	Protocolo utilizado	Informações adicionais
		Gravação de Característica/Atributo	Implementado	HTTPS	
	Disco do StoragePool	Capacidade provisionada	Implementado	HTTPS	
		Capacidade bruta	Implementado	HTTPS	
		Capacidade total	Implementado	HTTPS	
		Capacidade utilizada	Implementado	HTTPS	
		Taxa de capacidade de excesso de compromisso	Implementado	HTTPS	Relatado como uma série temporal
		Relação capacidade utilizada	Implementado	HTTPS	

APIs de gerenciamento usadas por este coletor de dados:

API	Protocolo utilizado	Protocolo da camada de transporte utilizado	Portas de entrada usadas	Portas de saída usadas	Suporta autenticação	Requer apenas credenciais "só de leitura"	Suporta criptografia	Firewall amigável (portas estáticas)
API REST DO EMC ECS	HTTPS	HTTPS	443		verdadeiro	verdadeiro	verdadeiro	verdadeiro

Dell EMC Isilon e PowerScale REST

Modelos e versões suportados por este coletor de dados:

Modelos	Versões de firmware
A200 A2000 A300 A3000 F200 F600 F800 F900 H400 H500 NL410 S210 X210 X400 X410	9.1.0.11 9.1.0.6 9.2.1.10 9.2.1.11 9.2.1.12 9.2.1.16 9.2.1.19 9.2.1.21 9.2.1.6 9.2.1.7 9.2.1.9 9.4.0.11 9.4.0.12 9.4.0.13 9.4.0.14 9.4.0.5 9.4.0.7 9.5.0.3 v8,0,0,4 v8,0,0,6 v8,0,0,7 v8,1,2,0 v8,2,2,0

Produtos suportados por este coletor de dados:

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
fundação					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/Atributo	Estado	Protocolo utilizado	Informações adicionais
		Relação bruta/utilizável	Implementado	HTTPS	taxa para converter de capacidade
		Capacidade alocada do Snapshot	Folga	HTTPS	Capacidade alocada de instantâneos em MB
		Capacidade utilizada do Snapshot	Implementado	HTTPS	
		ID do conjunto de armazenamento	Implementado	HTTPS	
		Thin Provisioning suportado	Implementado	HTTPS	Se esse volume interno é compatível com thin Provisioning para a camada de volume em cima dele
		Capacidade total alocada	Implementado	HTTPS	
		Capacidade total utilizada	Implementado	HTTPS	Capacidade total em MB
		Tipo	Folga	HTTPS	
		Virtual	Implementado	HTTPS	Este é um dispositivo de virtualização de armazenamento ?

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
desempenho					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

		usada do Snapshot			temporal
Produto	Categoria	Característica	Estado	Protocolo utilizado	Informações adicionais
		Taxa de transferência total	Implementado	HTTPS	Taxa total média do disco (leitura e gravação em todos os discos) em MB/s.
		Gravação de taxa de transferência	Implementado	HTTPS	

APIs de gerenciamento usadas por este coletor de dados:

API	Protocolo utilizado	Protocolo da camada de transporte utilizado	Portas de entrada usadas	Portas de saída usadas	Suporta autenticação	Requer apenas credenciais "só de leitura"	Suporta criptografia	Firewall amigável (portas estáticas)
API REST EMC Isilon e PowerScale	HTTPS		443		verdadeiro	verdadeiro	verdadeiro	verdadeiro

Dell EMC Isilon / PowerScale (CLI)

Modelos e versões suportados por este coletor de dados:

Modelos	Versões de firmware
A200 A2000 A300 F200 F800 F900 H400 H500 H600 H700 NL400 NL410 S210 X200 X210 X400 X410	9.1.0.10 9.1.0.12 9.1.0.16 9.1.0.18 9.1.0.19 9.1.0.7 9.2.1.11 9.2.1.13 9.2.1.15 9.2.1.22 9.2.1.7 9.2.1.9 9.3.0.3 9.4.0.0 9.4.0.10 9.4.0.12 9.4.0.13 9.4.0.14 9.4.0.6 9.4.0.7 v7,1.1,8 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 v8,2.2,0

Produtos suportados por este coletor de dados:

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
fundação					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

para a camada de volume em cima dele

Produto	Categoria	Característica/atributo	Estado	Protocolo utilizado	Informações adicionais
		Capacidade total utilizada	Implementado	SSH	Capacidade total em MB
		Tipo	Folga	SSH	
		Virtual	Implementado	SSH	Este é um dispositivo de virtualização de armazenamento ?

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
desempenho					
756					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/Atribuição	Estado	Protocolo utilizado	Informações adicionais
		Cravação de taxa de transferência	Implementado	SSH	
	Disco do StoragePool	Capacidade provisionada	Implementado	SSH	
		Capacidade bruta	Implementado	SSH	
		Capacidade total	Implementado	SSH	
		Capacidade utilizada	Implementado	SSH	
		Taxa de capacidade de excesso de compromisso	Implementado	SSH	Relatado como uma série temporal
		Relação capacidade utilizada	Implementado	SSH	
		Capacidade total de dados	Implementado	SSH	
		Capacidade de dados utilizados	Implementado	SSH	
		Capacidade reservada do Snapshot	Implementado	SSH	
		Capacidade utilizada do Snapshot	Implementado	SSH	
		Taxa de capacidade usada do Snapshot	Implementado	SSH	Relatado como uma série temporal

APIs de gerenciamento usadas por este coletor de dados:

API	Protocolo utilizado	Protocolo da camada de transporte utilizado	Portas de entrada usadas	Portas de saída usadas	Suporta autenticação	Requer apenas credenciais "só de leitura"	Suporta criptografia	Firewall amigável (portas estáticas)
Isilon SSH	SSH	SSH	22		verdadeiro	falso	verdadeiro	verdadeiro

EMC PowerStore REST

Modelos e versões suportados por este coletor de dados:

Modelos	Versões de firmware
PowerStore 1000T PowerStore 1200T PowerStore 3000T PowerStore 3200T PowerStore 5000T PowerStore 5000X PowerStore 9000T PowerStore 9200T	2.0.1.3 2.1.1.0 2.1.1.1 3.0.0.1 3.2.0.0 3.2.0.1 3.2.1.0

Produtos suportados por este coletor de dados:

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
fundação					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/Atributo	Estado	Protocolo utilizado	Informações adicionais
Volume		Capacidade	Implementado		Capacidade de captura instantânea usada em MB
		Caminho de junção	Implementado		
		Nome	Implementado		
		Capacidade bruta total	Implementado		Capacidade bruta total (soma de todos os discos no array)
		ID do conjunto de armazenamento	Implementado		
		Thin Provisioning	Implementado		
		Tipo	Folga		
		UUID	Implementado		
		Capacidade utilizada	Implementado		
		QoS - Política	Implementado		
		Mapa de volume		LUN	Implementado
Máscara necessária	Implementado				
Controlador de protocolo	Implementado				
Porta de armazenamento	Implementado				
Tipo	Folga				
Máscara de volume		Iniciador	Implementado		
		Controlador de protocolo	Implementado		
		Tipo	Folga		
WWN Alias		Aliases de host	Implementado		
		Tipo Objeto	Implementado		
		Fonte	Implementado		
		WWN	Implementado		

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
desempenho					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/Atributo	Estado	Protocolo utilizado	Informações adicionais
	Implementado			Volume	Gravação de taxa de transferência
	Implementado				Capacidade bruta
	Implementado				Capacidade total
	Implementado				Capacidade utilizada
	Implementado				Relação capacidade utilizada
	Implementado				Leitura de IOPS
	Implementado		Número de IOPS de leitura no disco		Total de IOPS
	Implementado				Gravação de IOPS
	Implementado				Leitura de latência
	Implementado				Total de latência
	Implementado				Gravação de latência
	Implementado				Taxa de transferência de leitura
	Implementado				Taxa de transferência total
	Implementado		Taxa total média do disco (leitura e gravação em todos os discos) em MB/s.		Gravação de taxa de transferência

APIs de gerenciamento usadas por este coletor de dados:

API	Protocolo utilizado	Protocolo da camada de transporte utilizado	Portas de entrada usadas	Portas de saída usadas	Suporta autenticação	Requer apenas credenciais "só de leitura"	Suporta criptografia	Firewall amigável (portas estáticas)
API REST DO EMC POWERSHORE	HTTPS	HTTPS	443		verdadeiro	verdadeiro	verdadeiro	verdadeiro

EMC RecoverPoint (HTTP)

Modelos e versões suportados por este coletor de dados:

Modelos	Versões de firmware
RecoverPoint	5,1.(c.175) 5,1.SP4.P1(h.89) 5,1.SP4.P1(h.101) 5,1.SP4.P3(h.P2) 5,1.SP4.P4(h.97)

Produtos suportados por este coletor de dados:

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
fundação					
774					

Produto	Categoria	Característica/Atributo	Estado	Protocolo utilizado	Informações adicionais
		Virtual	Implementado	HTTPS	Este é um dispositivo de virtualização de informações
	Nó de storage	Tamanho da memória	Folga	HTTPS	Memória do dispositivo em MB
		Modelo	Implementado	HTTPS	
		Nome	Implementado	HTTPS	
		Contagem de processadores	Implementado	HTTPS	CPU do dispositivo
		Número de série	Implementado	HTTPS	
		Estado	Implementado	HTTPS	texto livre que descreve o estado do dispositivo
		UUID	Implementado	HTTPS	
		Versão	Implementado	HTTPS	versão do software
	Sincronização de armazenamento	Modo	Implementado	HTTPS	
		Modo Enum	Implementado	HTTPS	
		Armazenamento de origem	Implementado	HTTPS	
		Volume de origem	Implementado	HTTPS	
		Estado	Implementado	HTTPS	texto livre que descreve o estado do dispositivo
		Estado Enum	Implementado	HTTPS	
		Storage de destino	Implementado	HTTPS	
		Volume alvo	Implementado	HTTPS	
		Tecnologia	Implementado	HTTPS	tecnologia que faz com que a eficiência de storage seja alterada

APIs de gerenciamento usadas por este coletor de dados:

API	Protocolo utilizado	Protocolo da camada de transporte utilizado	Portas de entrada usadas	Portas de saída usadas	Suporta autenticação	Requer apenas credenciais "só de leitura"	Suporta criptografia	Firewall amigável (portas estáticas)
API REST do RecoverPoint	HTTPS	HTTPS	443		verdadeiro	verdadeiro	verdadeiro	verdadeiro

EMC ScaleIO e PowerFlex REST

Modelos e versões suportados por este coletor de dados:

Modelos	Versões de firmware
ScaleIO	R2_6.11000.113 R2_6.11000.115 R3_0.1400.101 R3_5.1200.104 R3_6.500.113 R3_6.700.103

Produtos suportados por este coletor de dados:

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
fundação					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/Atributo	Estado	Protocolo utilizado	Informações adicionais
		Virtual	Implementado	HTTPS	Este é um dispositivo de virtualização de armazenamento
	Volume	Capacidade	Implementado	HTTPS	Capacidade de captura instantânea usada em MB
		Caminho de junção	Implementado	HTTPS	
		Nome	Implementado	HTTPS	
		Capacidade bruta total	Implementado	HTTPS	Capacidade bruta total (soma de todos os discos no array)
		ID do conjunto de armazenamento	Implementado	HTTPS	
		Thin Provisioning	Implementado	HTTPS	
		UUID	Implementado	HTTPS	
		IPs de host	Implementado	HTTPS	

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
desempenho					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/Atributo	Estado	Protocolo utilizado	Informações adicionais
		transferência total			do disco (leitura e gravação em todos os discos) em MB/s.
		Taxa de IOPS	Implementado		
	Volume	Capacidade bruta	Implementado		
		Capacidade total	Implementado		
		Leitura de IOPS	Implementado		Número de IOPS de leitura no disco
		Total de IOPS	Implementado		
		Gravação de IOPS	Implementado		
		Taxa de transferência de leitura	Implementado		
		Taxa de transferência total	Implementado		Taxa total média do disco (leitura e gravação em todos os discos) em MB/s.
		Gravação de taxa de transferência	Implementado		

APIs de gerenciamento usadas por este coletor de dados:

API	Protocolo utilizado	Protocolo da camada de transporte utilizado	Portas de entrada usadas	Portas de saída usadas	Suporta autenticação	Requer apenas credenciais "só de leitura"	Suporta criptografia	Firewall amigável (portas estáticas)
API REST EMC ScaleIO e PowerFlex	HTTPS	HTTPS	443		verdadeiro	verdadeiro	verdadeiro	verdadeiro

CLI do EMC Symmetrix

Modelos e versões suportados por este coletor de dados:

Versões de API	Modelos	Versões de firmware
V10,0.0,0 V10,0.1,0 V7,6.2,67 V8,3.0,22 V8,3.0,6 V8,4.2,0 V9,2.3,0 V9,2.1,2 V9,2.1,0 V9,2.1,1 V9,2.0,0 V9,2.0,5 V9,1.0,6 V9,2.0,18 V9,1.0,7 V8,4.0,9 V9,1.3,1 V9,2.3,4 V9,2.3,5 V9,2.3,6 V9,2.4,1 V9,2.4,2	DMX3-24 DMX4-24 PMAX2000 POWERMAX_2000 POWERMAX_8000 VMAX-1 VMAX100K VMAX10K VMAX200K VMAX250F VMAX400K VMAX40K VMAX450F VMAX850F VMAX950F	Compilação 60 5977.1151.1151 195 5978.711.711 149 5978.711.711 220 5978.711.711 267 5978.711.711 335 5978.711.711 388 5978.711.711 438 5978.711.711 480 5978.711.711(168D0000) compilação 5 5876.272.177 113 5978.711.711 194 5978.711.711 239 5978.711.711 278 5978.711.711 365 5978.711.711 416 5978.711.711 448 5978.711.711 484 5978.711.711(16F40000) compilação 17590000 9 5978.479.479 139 5978.711.711 196 5978.711.711 252 5978.711.711 287 5978.711.711 366 5978.711.711 436 5978.711.711 461 5978.711.711 502 5978.711.711(16F40000) compilação 115 5876.309.196(16F40000) compilação 59 5977.1151.1151(17590000) compilação 551 5977.1151.1151(17590000) compilação 45 5977.1151.1151(17590000) compilação 162 5977.1131.1131(39 5876.286.194) compilação 5773.198.142(17590000) compilação 529 5978.711.711 8

Produtos suportados por este coletor de dados:

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
fundação					
786					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Porta de armazenamento	Implementado		
		Característica/Atributo	Estado	Protocolo utilizado	Informações adicionais
Membro do volume	Disposição automática em categorias	Implementado		indica se esse storagepool está participando da categorização automática com outros pools	
	Capacidade	Implementado		Capacidade de captura instantânea usada em MB	
	Cilindros	Implementado			
	Nome	Implementado			
	Classificação	Implementado			
	Capacidade bruta total	Implementado		Capacidade bruta total (soma de todos os discos no array)	
	Redundância	Implementado		Nível de redundância	
	ID do conjunto de armazenamento	Implementado			
	UUID	Implementado			
	Capacidade utilizada	Implementado			
Ref. Volume	Nome	Implementado			
	IP de armazenamento	Implementado			
WWN Alias	Aliases de host	Implementado			
	Tipo Objeto	Implementado			
	Fonte	Implementado			
	WWN	Implementado			

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
desempenho					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

todos os discos) em MB/s.

		Gravação de Característica/Atribuição	Implementado		
Produto	Categoria	Característica/Atribuição	Estado	Protocolo utilizado	Informações adicionais
		Escrever pendente	Implementado		total de escrita pendente

APIs de gerenciamento usadas por este coletor de dados:

API	Protocolo utilizado	Protocolo da camada de transporte utilizado	Portas de entrada usadas	Portas de saída usadas	Suporta autenticação	Requer apenas credenciais "só de leitura"	Suporta criptografia	Firewall amigável (portas estáticas)
symcli	CLI		2707		verdadeiro	verdadeiro	verdadeiro	verdadeiro
Symmetrix SMI-S	SMI-S	HTTP/HTTPS	5988/5989		verdadeiro	falso	falso	verdadeiro

Dell Unisphere REST

Modelos e versões suportados por este coletor de dados:

Versões de API	Modelos	Versões de firmware
V10,0.0,5 V10,0.1,3 V9,2.1,6 V9,2.3,20 V9,2.3,22 V9,2.3,4 V9,2.4,1	Powermax_2000 Powermax_2500 Powermax_8000 VMAX250F VMAX950F	build build build build build build 329 build 329 5978.711.711 build 365 5978.711.711 build 278 build 278 5978.711.711 build 287 5978.711.711 build 484 5978.711.711 build 484 build 481 5978.711.711 build 461 5978.711.711 build 481 build 461 build 435 5978.711.711 build 448 5978.711.711 build 416 5978.711.711 build 388 build 388 5978.711.711 build 376 5978.711.711 build 365 build 365 5978.711.711 build 53 6079.175.0 build 0 build 0 build 484 5978.711.711 build 502 6079.125.0 build 53 build 252 5978.711.711 build 5978.479.479 build 350 5978.711.711

Produtos suportados por este coletor de dados:

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
fundação					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/Atributo	Estado	Protocolo utilizado	Informações adicionais
		protocolo			
		Porta de armazenamento	Implementado	HTTPS	
		Tipo	Folga	HTTPS	
	Máscara de volume	Iniciador	Implementado	HTTPS	
		Controlador de protocolo	Implementado	HTTPS	
		Porta de armazenamento	Implementado	HTTPS	
		Tipo	Folga	HTTPS	
	WWN Alias	Aliases de host	Implementado	HTTPS	
		Tipo Objeto	Implementado	HTTPS	
		Fonte	Implementado	HTTPS	
		WWN	Implementado	HTTPS	

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
desempenho					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

					todos os discos) em MB/s.
Produto	Gravação de Categoria	Implementado Característica/A tributo	HTTPS Estado	Protocolo utilizado	Total de Informações adicionais
	Implementado	HTTPS		Volume	Capacidade bruta
	Implementado	HTTPS			Capacidade total
	Implementado	HTTPS			Capacidade utilizada
	Implementado	HTTPS			Relação capacidade utilizada
	Implementado	HTTPS			Capacidade escrita
	Implementado	HTTPS			Leitura de IOPS
	Implementado	HTTPS	Número de IOPS de leitura no disco		Total de IOPS
	Implementado	HTTPS			Gravação de IOPS
	Implementado	HTTPS			Leitura de latência
	Implementado	HTTPS			Total de latência
	Implementado	HTTPS			Gravação de latência
	Implementado	HTTPS			Taxa de transferência de leitura
	Implementado	HTTPS			Taxa de transferência total
	Implementado	HTTPS	Taxa total média do disco (leitura e gravação em todos os discos) em MB/s.		Gravação de taxa de transferência

APIs de gerenciamento usadas por este coletor de dados:

API	Protocolo utilizado	Protocolo da camada de transporte utilizado	Portas de entrada usadas	Portas de saída usadas	Suporta autenticação	Requer apenas credenciais "só de leitura"	Suporta criptografia	Firewall amigável (portas estáticas)
API Dell Unisphere	HTTPS	HTTPS	443		verdadeiro	verdadeiro	verdadeiro	verdadeiro

EMC VNX (SSH)

Modelos e versões suportados por este coletor de dados:

Modelos	Versões de firmware
VNX5300 VNX5400 VNX5700 VNX5800	05.33.009.5.231 7,1.76-4 7,1.80-3 8,1.9-232

Produtos suportados por este coletor de dados:

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
fundação					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	armazenamento	Implementado	SSH	
		Controlador de protocolo	Implementado	SSH	
		Característica/Atributo	Estado	Protocolo Utilizado	Informações adicionais
	Máscara de volume	Porta de armazenamento	Implementado	SSH	
		Iniciador	Implementado	SSH	
		Controlador de protocolo	Implementado	SSH	
		Tipo	Folga	SSH	
	WWN Alias	Fonte	Implementado	SSH	
		Aliases de host	Implementado	SSH	
		WWN	Implementado	SSH	
		Tipo Objeto	Implementado	SSH	
		IP	Implementado	SSH	

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
desempenho					
826					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/Atribuição	Estado	Protocolo utilizado	Informações adicionais
		Gravação de Característica/Atribuição	Implementado	SSH	
	Nó de storage	Leitura de IOPS	Implementado	SSH	Número de IOPS de leitura no disco
		Total de IOPS	Implementado	SSH	
		Gravação de IOPS	Implementado	SSH	
		Total de utilização	Implementado	SSH	

APIs de gerenciamento usadas por este coletor de dados:

API	Protocolo utilizado	Protocolo da camada de transporte utilizado	Portas de entrada usadas	Portas de saída usadas	Suporta autenticação	Requer apenas credenciais "só de leitura"	Suporta criptografia	Firewall amigável (portas estáticas)
VNX SSH E CLI	SSH	SSH	22		verdadeiro	falso	verdadeiro	verdadeiro

EMC VNXe e Unity Unisphere (CLI)

Modelos e versões suportados por este coletor de dados:

Modelos	Versões de firmware
Unidade 380F Unidade 400F Unidade 350F Unidade 480F Unidade 880 Unidade 600F	3.1.17.10223906 3.1.17.10229825 4.1.2.9257522 4.2.1.9535982 4.2.3.9670635 4.5.1.0.5.001 5.0.2.0.5.009 5.0.6.0.5.008 5.0.8.0.5.007 5.1.2.0.5.007 5.1.3.0.5.003 5.2.1.0.5.013 5.2.2.0.5.004 5.2.2.0.6.201 5.3.0.0.5.120
Unidade 300F Unidade 450F Unidade 500F Unidade 300F Unidade 600F Unidade 650F Unidade 680F	

Produtos suportados por este coletor de dados:

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
fundação					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/Atributo	Estado	Protocolo utilizado	Informações adicionais
		Tecnologia	Implementado	HTTPS	tecnologia que faz com que a eficiência de
	Volume	Capacidade	Implementado	HTTPS	Capacidade de captura instantânea usada em MB
		Caminho de junção	Implementado	HTTPS	
		Nome	Implementado	HTTPS	
		Capacidade bruta total	Implementado	HTTPS	Capacidade bruta total (soma de todos os discos no array)
		ID do conjunto de armazenamento	Implementado	HTTPS	
		Thin Provisioning	Implementado	HTTPS	
		UUID	Implementado	HTTPS	
		Capacidade utilizada	Implementado	HTTPS	
	Mapa de volume	LUN	Implementado	HTTPS	Nome do lun de back-end
		Controlador de protocolo	Implementado	HTTPS	
		Porta de armazenamento	Implementado	HTTPS	
		Tipo	Folga	HTTPS	
	Máscara de volume	Iniciador	Implementado	HTTPS	
		Controlador de protocolo	Implementado	HTTPS	
		Porta de armazenamento	Implementado	HTTPS	
		Tipo	Folga	HTTPS	

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
desempenho					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/Atributo	Estado	Protocolo utilizado	Informações adicionais
	Implementado	HTTPS	Taxa total média do disco (leitura e gravação em todos os discos) em MB/s.		Gravação de taxa de transferência
	Implementado	HTTPS		Volume	Capacidade bruta
	Implementado	HTTPS			Capacidade total
	Implementado	HTTPS			Capacidade utilizada
	Implementado	HTTPS			Relação capacidade utilizada
	Implementado	HTTPS			Leitura de IOPS
	Implementado	HTTPS	Número de IOPS de leitura no disco		Total de IOPS
	Implementado	HTTPS			Gravação de IOPS
	Implementado	HTTPS			Total de latência
	Implementado	HTTPS			Taxa de transferência de leitura
	Implementado	HTTPS			Taxa de transferência total
	Implementado	HTTPS	Taxa total média do disco (leitura e gravação em todos os discos) em MB/s.		Gravação de taxa de transferência

APIs de gerenciamento usadas por este coletor de dados:

API	Protocolo utilizado	Protocolo da camada de transporte utilizado	Portas de entrada usadas	Portas de saída usadas	Suporta autenticação	Requer apenas credenciais "só de leitura"	Suporta criptografia	Firewall amigável (portas estáticas)
CLI VNxe Unisphere	HTTPS	HTTPS	443		verdadeiro	verdadeiro	verdadeiro	verdadeiro

EMC VPLEX

Modelos e versões suportados por este coletor de dados:

Modelos	Versões de firmware
VPLEX	5.4.1.00.00.07 5.4.1.01.00.05 6.2.0.03.00.02 6.2.0.04.00.07 6.2.0.05.00.11 6.2.0.07.00.02

Produtos suportados por este coletor de dados:

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
fundação					
844					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/Atributo	Estado	Protocolo utilizado	Informações adicionais
	Volume	Capacidade	Implementado	HTTP/S	tecnologia que faz com que a eficiência de armazenamento seja maior
		Nome	Implementado	HTTP/S	
		Capacidade bruta total	Implementado	HTTP/S	Capacidade bruta total (soma de todos os discos no array)
		Redundância	Implementado	HTTP/S	Nível de redundância
		ID do conjunto de armazenamento	Implementado	HTTP/S	
		Thin Provisioning	Implementado	HTTP/S	
		UUID	Implementado	HTTP/S	
		Virtual	Implementado	HTTP/S	Este é um dispositivo de virtualização de armazenamento ?
	Mapa de volume	LUN	Implementado	HTTP/S	Nome do lun de back-end
		Controlador de protocolo	Implementado	HTTP/S	
		Porta de armazenamento	Implementado	HTTP/S	
		Tipo	Folga	HTTP/S	
	Máscara de volume	Iniciador	Implementado	HTTP/S	
		Controlador de protocolo	Implementado	HTTP/S	
		Porta de armazenamento	Implementado	HTTP/S	
		Tipo	Folga	HTTP/S	

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
desempenho					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/Atribuição	Estado	Protocolo utilizado	Informações adicionais
		Gravação de taxa de transferência	Implementado	SSH	
	Disco do StoragePool	Capacidade provisionada	Implementado	SSH	
		Capacidade total	Implementado	SSH	
		Capacidade utilizada	Implementado	SSH	
		Taxa de capacidade de excesso de compromisso	Implementado	SSH	Relatado como uma série temporal
		Relação capacidade utilizada	Implementado	SSH	
		Outra capacidade total	Implementado	SSH	
		Outra capacidade utilizada	Implementado	SSH	
	Volume	Capacidade bruta	Implementado	SSH	
		Capacidade total	Implementado	SSH	
		Total de IOPS	Implementado	SSH	
		Leitura de latência	Implementado	SSH	
		Total de latência	Implementado	SSH	
		Gravação de latência	Implementado	SSH	
		Taxa de transferência de leitura	Implementado	SSH	
		Taxa de transferência total	Implementado	SSH	Taxa total média do disco (leitura e gravação em todos os discos) em MB/s.
		Gravação de taxa de transferência	Implementado	SSH	

APIs de gerenciamento usadas por este coletor de dados:

API	Protocolo utilizado	Protocolo da camada de transporte utilizado	Portas de entrada usadas	Portas de saída usadas	Suporta autenticação	Requer apenas credenciais "só de leitura"	Suporta criptografia	Firewall amigável (portas estáticas)
CLI DO EMC VPLEX	SSH	SSH	22		verdadeiro	verdadeiro	verdadeiro	verdadeiro
EMC VPLEX API	HTTP/HTTPS	HTTP/HTTPS	80/443		verdadeiro	verdadeiro	verdadeiro	verdadeiro

EMC XtremIO (HTTP)

Modelos e versões suportados por este coletor de dados:

Versões de API	Modelos	Versões de firmware
6.2.1 6.2.2 6.3.1 6.3.2 6.3.3 6.4.0	1 tijolos & 125TB 1 tijolos & 24TB 1 tijolos & 125TB 4 tijolos & 251TB 3 tijolos & 62TB 1 tijolos & 8TB 1X10TB 1X20TB 1X40TB 2 tijolos & 83TB tijolos & 62TB 2 tijolos & 76TB 2 tijolos & 52TB 2 2X10TB 2X20TB 2X40TB 3 tijolos & 31TB 1 tijolos & 283TB 4 tijolos e 26TB 1 tijolos & 503TB 4 tijolos & 628TB 4 tijolos & 754TB 4X20TB 4X40TB	4,0.27-1 4,0.31-11 6,1.0-99_X2 6,3.3-8_X2 6,4.0-22_X2 6,4.0-36_HOTFIX_2_X2

Produtos suportados por este coletor de dados:

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
fundação					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/Atributo	Estado	Protocolo utilizado	Informações adicionais
		Controlador de protocolo	Implementado	HTTPS	back-end
		Iniciador	Implementado	HTTPS	
	Máscara de volume	Controlador de protocolo	Implementado	HTTPS	
		Tipo	Folga	HTTPS	

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
desempenho					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/Atributo	Estado	Protocolo utilizado	Informações adicionais
		Capacidade total de dados	Implementado	HTTPS	
	Volume	Capacidade bruta	Implementado	HTTPS	
		Capacidade total	Implementado	HTTPS	
		Capacidade utilizada	Implementado	HTTPS	
		Relação capacidade utilizada	Implementado	HTTPS	
		Leitura de IOPS	Implementado	HTTPS	Número de IOPS de leitura no disco
		Total de IOPS	Implementado	HTTPS	
		Gravação de IOPS	Implementado	HTTPS	
		Leitura de latência	Implementado	HTTPS	
		Total de latência	Implementado	HTTPS	
		Gravação de latência	Implementado	HTTPS	
		Relação bloqueada parcial	Implementado	HTTPS	
		Taxa de transferência de leitura	Implementado	HTTPS	
		Taxa de transferência total	Implementado	HTTPS	Taxa total média do disco (leitura e gravação em todos os discos) em MB/s.
		Gravação de taxa de transferência	Implementado	HTTPS	

APIs de gerenciamento usadas por este coletor de dados:

API	Protocolo utilizado	Protocolo da camada de transporte utilizado	Portas de entrada usadas	Portas de saída usadas	Suporta autenticação	Requer apenas credenciais "só de leitura"	Suporta criptografia	Firewall amigável (portas estáticas)
API REST DO EMC XTREMIO	HTTPS	HTTPS	443		verdadeiro	verdadeiro	verdadeiro	verdadeiro

NetApp e-Series

Modelos e versões suportados por este coletor de dados:

Modelos	Versões de firmware
2600 2660 2680 2702 2704 2800B 2804 2806 3000 5480 5486 5488 5504 5564 5600 5700 5700B 6000	08.40.60.01 8.10.14.0 8.20.11.0 8.20.27.0 8.20.30.0 8.20.5.0 8.20.8.0 8.25.14.0 8.25.6.0 8.30.1.0 8.40.0.1 8.40.0.3 8.40.20.0 8.40.30.3 8.40.40.0 8.40.50.0 8.40.60.1 8.40.60.2 8.40.60.3 8.42.20.0 8.50.0.3 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 8.70.0.3 8.71.2.0 8.71.3.0 8.72.0.0 8.72.1.0 8.72.2.0 8.73.0.0 8.74.0.0 8.74.1.0 8.74.2.0 8.74.3.0 8.75.0.0

Produtos suportados por este coletor de dados:

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
fundação					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/Atributo	Estado	Protocolo utilizado	Informações adicionais
	Volume	Capacidade	Implementado	RMI	Capacidade de captura instantânea usada em MB
		Tipo de disco	Não disponível	RMI	
		Nome	Implementado	RMI	
		Capacidade bruta total	Implementado	RMI	Capacidade bruta total (soma de todos os discos no array)
		Redundância	Implementado	RMI	Nível de redundância
		ID do conjunto de armazenamento	Implementado	RMI	
		Thin Provisioning	Implementado	RMI	
		Tipo	Folga	RMI	
		UUID	Implementado	RMI	
		Capacidade utilizada	Implementado	RMI	
		Virtual	Implementado	RMI	Este é um dispositivo de virtualização de armazenamento ?
		Capacidade escrita	Implementado	RMI	Capacidade total escrita para este volume por um anfitrião em MB
		Mapa de volume	LUN	Implementado	RMI
	Porta de armazenamento		Implementado	RMI	
	Tipo		Folga	RMI	
	Máscara de volume	Iniciador	Implementado	RMI	
		Porta de armazenamento	Implementado	RMI	
		Tipo	Folga	RMI	

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
desempenho					
872					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

		Total de utilização	Implementado	RMI	
Produto	Categoria	Característica/Atribuição	Estado	Protocolo utilizado	Informações adicionais
	Volume	Taxa de acerto do cache ler	Implementado	RMI	
		Taxa de acerto do cache total	Implementado	RMI	
		Cache HIT Ratio Write	Implementado	RMI	
		Capacidade bruta	Implementado	RMI	
		Capacidade total	Implementado	RMI	
		Capacidade utilizada	Implementado	RMI	
		Capacidade escrita	Implementado	RMI	
		Relação capacidade utilizada	Implementado	RMI	
		Capacidade escrita	Implementado	RMI	
		Leitura de IOPS	Implementado	RMI	Número de IOPS de leitura no disco
		Total de IOPS	Implementado	RMI	
		Gravação de IOPS	Implementado	RMI	
		Leitura de latência	Implementado	RMI	
		Total de latência	Implementado	RMI	
		Gravação de latência	Implementado	RMI	
		Taxa de transferência de leitura	Implementado	RMI	
		Taxa de transferência total	Implementado	RMI	Taxa total média do disco (leitura e gravação em todos os discos) em MB/s.
		Gravação de taxa de transferência	Implementado	RMI	

APIs de gerenciamento usadas por este coletor de dados:

API	Protocolo utilizado	Protocolo da camada de transporte utilizado	Portas de entrada usadas	Portas de saída usadas	Suporta autenticação	Requer apenas credenciais "só de leitura"	Suporta criptografia	Firewall amigável (portas estáticas)
API SANtricity	RMI	TCP			verdadeiro	verdadeiro	falso	falso

Google Cloud Compute

Modelos e versões suportados por este coletor de dados:

Versões da API:

- v1

Produtos suportados por este coletor de dados:

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
fundação					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Fabricante	Implementado	HTTPS	
		Nome Característica/Atributo	Estado	Protocolo Utilizado	Informações adicionais
Informações		Descrição da API	Implementado	HTTPS	
		Nome da API	Implementado	HTTPS	
		Versão da API	Implementado	HTTPS	
		Nome da fonte de dados	Implementado	HTTPS	Informações
		Data	Implementado	HTTPS	
		ID do originador	Implementado	HTTPS	
		Chave originadora	Implementado	HTTPS	

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
desempenho					
882					

Produto	Categoria	Característica/Atributo	Estado	Protocolo utilizado	Informações adicionais
		Gravação de Característica/Atributo	Implementado	HTTPS	todos os discos) em MB/s.
	vm	Capacidade total	Implementado	HTTPS	
	vm	Utilização total da CPU	Implementado	HTTPS	
	vm	Leitura de IOPS	Implementado	HTTPS	Número de IOPS de leitura no disco
	vm	Disklops.Total	Implementado	HTTPS	
	vm	Gravação de IOPs de disco	Implementado	HTTPS	
	vm	Total de latência	Implementado	HTTPS	
	vm	Taxa de transferência do disco lida	Implementado	HTTPS	
	vm	Taxa de transferência de leitura	Implementado	HTTPS	leitura da taxa de transferência total do disco
	vm	Gravação da taxa de transferência do disco	Implementado	HTTPS	
	vm	Taxa de transferência IP lida	Implementado	HTTPS	
	vm	Taxa de transferência total	Implementado	HTTPS	Taxa de transferência IP total
	vm	IpThroughput.write	Implementado	HTTPS	
	vm	Utilização total da memória	Implementado	HTTPS	
	vm	swapRate.inRate	Implementado	HTTPS	
	vm	Taxa de swap	Implementado	HTTPS	
	vm	Taxa de troca total	Implementado	HTTPS	
	vm	Programar tempo de espera	Implementado	HTTPS	A aguardar o horário programado em porcentagem

APIs de gerenciamento usadas por este coletor de dados:

API	Protocolo utilizado	Protocolo da camada de transporte utilizado	Portas de entrada usadas	Portas de saída usadas	Suporta autenticação	Requer apenas credenciais "só de leitura"	Suporta criptografia	Firewall amigável (portas estáticas)
API REST do Google Compute Platform	HTTPS		443		verdadeiro	verdadeiro	verdadeiro	verdadeiro

HDS HCP (HTTPS)

Modelos e versões suportados por este coletor de dados:

Modelos	Versões de firmware
Plataforma de conteúdo Hitachi	9.3.7.2 9.5.0.121

Produtos suportados por este coletor de dados:

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
fundação					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

		alocada			
Produto	Categoria	Capacidade total utilizada	Implementado	HTTPS	Capacidade total em MB
		Característica/Atributo	Estado Folga	Protocolo utilizado	Informações adicionais
		Virtual	Implementado	HTTPS	Este é um dispositivo de virtualização de armazenamento ?

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
desempenho					

Produto	Categoria	Característica/Atribuição	Estado	Protocolo utilizado	Informações adicionais
		Gravação de taxa de transferência	Implementado		
	Disco do StoragePool	Capacidade total	Implementado		
		Relação capacidade utilizada	Implementado		
		Capacidade provisionada	Implementado		
		Capacidade utilizada	Implementado		
		Capacidade bruta	Implementado		
		Limite flexível de capacidade	Implementado		
		Taxa de capacidade de excesso de compromisso	Implementado		Relatado como uma série temporal

APIs de gerenciamento usadas por este coletor de dados:

API	Protocolo utilizado	Protocolo da camada de transporte utilizado	Portas de entrada usadas	Portas de saída usadas	Suporta autenticação	Requer apenas credenciais "só de leitura"	Suporta criptografia	Firewall amigável (portas estáticas)
API REST DO HDS HCP	HTTPS	HTTPS	9090		verdadeiro	verdadeiro	verdadeiro	verdadeiro

Gerenciador de dispositivos HiCommand

Modelos e versões suportados por este coletor de dados:

Versões de API	Modelos	Versões de firmware
7.6.1 8.7.7 8.8.1 8.8.3 8.8.5	DF850MH DF850S HM800 HM850 P9500 RAID700 RAID800 VSP5000 XP24000 XP7	0983 80 00/00 80 00/00 80 00/00 93 05 83 60/00 46 05 83 40/00 48 08 88 60/00 81 08 60 60 70 70 80 80 80/A-H 0988 06 80 06 80 06 80 00/00 45 05 83 60/00 47 05 83 60/00 08 08 90 00/00 83 08 08 06 06 06 06 06/H-S DKC:00/00 86 06- 87 88 06-91 91 06 83 40/00 45 05 83 60/00 48 05 88 60/00 09 08 90 00/01 21/00 54/00 32/00 51/00 76/02 78/00-80 DKC:06-80-80 DKC:06-67 DKC:70-70-06-46-00/00 DKC:08-22-60 DKC:08-65-06-82- 60 DKC 81/00 80 06 82/00 80 06 83/00 80 06 86/00 80 06 88/00 83 05 49 40/00 83 05 49 60/00 83 05 50 60/00 83 05 51 60/00 83 05 52 40/00 83 05 52 60/00 88 08 10 60/00 88 08 11 60/00 90 08 81/00 90 08 83/00

Produtos suportados por este coletor de dados:

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
fundação					
892					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/Atributo	Estado	Potencializado	Informações adicionais
	WWN Alias	Aliases de host	Implementado	API XML DO HDS	
		Tipo Objeto	Implementado	API XML DO HDS	
		Fonte	Implementado	API XML DO HDS	
		WWN	Implementado	API XML DO HDS	

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
desempenho					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/Atributo	Estado	Protocolo utilizado	Relatado como uma série de informações adicionais
		Taxa de capacidade de	Implementado	Exportar/CLI	Relatado como uma série
		Característica/Atributo			de informações
	Volume	Total de latência	Implementado	Exportar/CLI	
		Leitura de IOPS	Implementado	Exportar/CLI	Número de IOPS de leitura no disco
		Leitura de latência	Implementado	Exportar/CLI	
		Taxa de acerto do cache ler	Implementado	Exportar/CLI	
		Gravação de IOPS	Implementado	Exportar/CLI	
		Taxa de acerto do cache total	Implementado	Exportar/CLI	
		Cache HIT Ratio Write	Implementado	Exportar/CLI	
		Taxa de transferência de leitura	Implementado	Exportar/CLI	
		Gravação de taxa de transferência	Implementado	Exportar/CLI	
		Taxa de transferência total	Implementado	Exportar/CLI	Taxa total média do disco (leitura e gravação em todos os discos) em MB/s.
		Total de IOPS	Implementado	Exportar/CLI	
		Gravação de latência	Implementado	Exportar/CLI	

APIs de gerenciamento usadas por este coletor de dados:

API	Protocolo utilizado	Protocolo da camada de transporte utilizado	Portas de entrada usadas	Portas de saída usadas	Suporta autenticação	Requer apenas credenciais "só de leitura"	Suporta criptografia	Firewall amigável (portas estáticas)
Utilitário de exportação (USPV) / SNM CLI (AMS)	Exportar/CLI				falso	falso	falso	falso

API	Protocolo utilizado	Protocolo da camada de transporte utilizado	Portas de entrada usadas	Portas de saída usadas	Suporta autenticação	Requer apenas credenciais "só de leitura"	Suporta criptografia	Firewall amigável (portas estáticas)
API XML do Gerenciador de dispositivos HiCommand	API XML DO HDS	HTTP/HTTPS	2001		verdadeiro	verdadeiro	verdadeiro	verdadeiro

Hitachi Ops Center

Modelos e versões suportados por este coletor de dados:

Modelos	Versões de firmware
VSP 5100 VSP 5500 VSP F1500 VSP F600 VSP G800	80 03/05-01-65-08/00:00-01-65-03/05 90-81-00/00:65-03/05 90-08-40-00-01/03/05 83:05-48-00-01-65-05/47:40-01-65-03/05 83-46-60/00:65-03/05 83-05-00-82-01/00:06-92

Produtos suportados por este coletor de dados:

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
fundação					
908					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/Atributo	Estado	Protocolo utilizado	Informações adicionais
	Volume	Capacidade	Implementado		Capacidade de captura instantânea usada em MB
		Caminho de junção	Implementado		
		Nome	Implementado		
		Tipo de proteção	Implementado		
		Capacidade bruta total	Implementado		Capacidade bruta total (soma de todos os discos no array)
		ID do conjunto de armazenamento	Implementado		
		Thin Provisioning	Implementado		
		Tipo	Folga		
		Capacidade utilizada	Implementado		
		Compressão ativada	Implementado		
	Mapa de volume	LUN	Implementado		Nome do lun de back-end
		Máscara necessária	Implementado		
		Controlador de protocolo	Implementado		
		Porta de armazenamento	Implementado		
		Tipo	Folga		
	Máscara de volume	Iniciador	Implementado		
		Controlador de protocolo	Implementado		
		Porta de armazenamento	Implementado		
		Tipo	Folga		

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
desempenho					
916					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/Atributo	Estado	Protocolo utilizado	Informações adicionais
		transparência total			do disco (leitura e gravação em todos os discos) em MB/s.
		Limite de IOPS	Implementado		
	Disco do StoragePool	Capacidade total	Implementado		
		Relação capacidade utilizada	Implementado		
		Capacidade provisionada	Implementado		
		Capacidade utilizada	Implementado		
		Capacidade bruta	Implementado		
		Limite flexível de capacidade	Implementado		
		Taxa de capacidade de excesso de compromisso	Implementado		Relatado como uma série temporal

APIs de gerenciamento usadas por este coletor de dados:

API	Protocolo utilizado	Protocolo da camada de transporte utilizado	Portas de entrada usadas	Portas de saída usadas	Suporta autenticação	Requer apenas credenciais "só de leitura"	Suporta criptografia	Firewall amigável (portas estáticas)
API REST do Hitachi Ops Center	HTTPS	HTTPS	443		verdadeiro	verdadeiro	verdadeiro	verdadeiro

HDS HNAS (CLI)

Modelos e versões suportados por este coletor de dados:

Modelos	Versões de firmware
G600 G800 HNAS 4080 HNAS 4100 N800	13.9.6918.05 14.5.7413.01 14.6.7520.04

Produtos suportados por este coletor de dados:

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
fundação					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

		Capacidade total utilizada	Implementado	SSH	Capacidade total em MB
Produto	Categoria	Capacidade total utilizada	Implementado	Protocolo utilizado	Informações adicionais
		Relação bruta/utilizável	Implementado	SSH	taxa para converter de capacidade utilizável para capacidade bruta

APIs de gerenciamento usadas por este coletor de dados:

API	Protocolo utilizado	Protocolo da camada de transporte utilizado	Portas de entrada usadas	Portas de saída usadas	Suporta autenticação	Requer apenas credenciais "só de leitura"	Suporta criptografia	Firewall amigável (portas estáticas)
CLI DO HDS HNAS	SSH	SSH	22		verdadeiro	verdadeiro	verdadeiro	verdadeiro

Armazenamento HPE Nimble / Alletra 6000

Modelos e versões suportados por este coletor de dados:

Versões de API	Modelos	Versões de firmware
v1	6030 AF1000 AF20Q AF3000 AF40 AF5000 CS1000 CS300 CS3000 CS500 CS5000 HF20 HF20H HF40 HF60	5,0 6,1.10,0 1,300-1020304 1028597-opt 6,0.0,400-991061-opt 6,0.0,300-677726-opt 5,2.1,900-1003439-opt 5,2.1,800-930936-opt 5,2.1,700-882343-opt 5,2.1,600-841103-opt 5,2.1,400-796142-opt 5,2.1,1000-1017822-opt 5,0.8,0-956221-opt 5,0.7,0-604814-opt 6,1.1,200-742719

Produtos suportados por este coletor de dados:

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
fundação					
928					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/Atributo	Estado	Protocolo	Informações adicionais
			Folga	Utilizado	
		protocolo	Implementado	HTTPS	
		Porta de armazenamento	Implementado	HTTPS	
		Iniciador	Implementado	HTTPS	
		Controlador de protocolo	Implementado	HTTPS	
		Porta de armazenamento	Implementado	HTTPS	
		Tipo	Folga	HTTPS	
	Máscara de volume	Aliases de host	Implementado	HTTPS	
		Tipo Objeto	Implementado	HTTPS	
		Fonte	Implementado	HTTPS	
		WWN	Implementado	HTTPS	

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
desempenho					
936					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/Atributo	Estado	Protocolo utilizado	Informações adicionais
		Gravação de transferência	Implementado	HTTPS	
	Volume	Capacidade bruta	Implementado	HTTPS	
		Capacidade total	Implementado	HTTPS	
		Capacidade utilizada	Implementado	HTTPS	
		Relação capacidade utilizada	Implementado	HTTPS	
		Economia de compressão total	Implementado	HTTPS	
		Espaço de economia de compressão	Implementado	HTTPS	
		Leitura de IOPS	Implementado	HTTPS	Número de IOPS de leitura no disco
		Total de IOPS	Implementado	HTTPS	
		Gravação de IOPS	Implementado	HTTPS	
		Leitura de latência	Implementado	HTTPS	
		Total de latência	Implementado	HTTPS	
		Gravação de latência	Implementado	HTTPS	
		Taxa de transferência de leitura	Implementado	HTTPS	
		Taxa de transferência total	Implementado	HTTPS	Taxa total média do disco (leitura e gravação em todos os discos) em MB/s.
		Gravação de taxa de transferência	Implementado	HTTPS	

APIs de gerenciamento usadas por este coletor de dados:

API	Protocolo utilizado	Protocolo da camada de transporte utilizado	Portas de entrada usadas	Portas de saída usadas	Suporta autenticação	Requer apenas credenciais "só de leitura"	Suporta criptografia	Firewall amigável (portas estáticas)
API REST DO HP NIMBLE	HTTPS	HTTPS	5392		verdadeiro	falso	verdadeiro	verdadeiro

Huawei OceanStor (REST/HTTPS)

Modelos e versões suportados por este coletor de dados:

Modelos	Versões de firmware
5300 V5 5500 V3 5500 V5 5800 V3 Dorado 5000 V6 SAS Dorado 6000 V3 Dorado 6000 V6 NVMe	V300R001C01 V300R002C10 V300R006C20 V300R006C50 V500R007C10 V500R007C30 V600R003C00 FA-X90R3 V600R005C03

Produtos suportados por este coletor de dados:

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
fundação					
940					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/Atributo	Estado	Protocolo utilizado	Informações adicionais
		Virtual	Implementado	HTTPS	Este é um dispositivo de virtualização de armazenamento
	Volume	Capacidade	Implementado	HTTPS	Capacidade de captura instantânea usada em MB
		Caminho de junção	Implementado	HTTPS	
		Nome	Implementado	HTTPS	
		Capacidade bruta total	Implementado	HTTPS	Capacidade bruta total (soma de todos os discos no array)
		Redundância	Implementado	HTTPS	Nível de redundância
		ID do conjunto de armazenamento	Implementado	HTTPS	
		Thin Provisioning	Implementado	HTTPS	
		UUID	Implementado	HTTPS	
		Capacidade utilizada	Implementado	HTTPS	
		Virtual	Implementado	HTTPS	Este é um dispositivo de virtualização de armazenamento ?
	Mapa de volume	LUN	Implementado	HTTPS	Nome do lun de back-end
		Controlador de protocolo	Implementado	HTTPS	
		Porta de armazenamento	Implementado	HTTPS	
		Tipo	Folga	HTTPS	
	Máscara de volume	Iniciador	Implementado	HTTPS	
		Controlador de protocolo	Implementado	HTTPS	
		Porta de armazenamento	Implementado	HTTPS	
		Tipo	Folga	HTTPS	

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
desempenho					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/Atribuição	Estado	Protocolo utilizado	Informações adicionais
		Gravação de latência	Implementado	HTTPS	
	Volume	Taxa de acerto do cache ler	Implementado	HTTPS	
		Taxa de acerto do cache total	Implementado	HTTPS	
		Cache HIT Ratio Write	Implementado	HTTPS	
		Capacidade bruta	Implementado	HTTPS	
		Capacidade total	Implementado	HTTPS	
		Capacidade utilizada	Implementado	HTTPS	
		Relação capacidade utilizada	Implementado	HTTPS	
		Leitura de IOPS	Implementado	HTTPS	Número de IOPS de leitura no disco
		Total de IOPS	Implementado	HTTPS	
		Gravação de IOPS	Implementado	HTTPS	
		Leitura de latência	Implementado	HTTPS	
		Total de latência	Implementado	HTTPS	
		Gravação de latência	Implementado	HTTPS	
		Taxa de transferência de leitura	Implementado	HTTPS	
		Taxa de transferência total	Implementado	HTTPS	Taxa total média do disco (leitura e gravação em todos os discos) em MB/s.
		Gravação de taxa de transferência	Implementado	HTTPS	

APIs de gerenciamento usadas por este coletor de dados:

API	Protocolo utilizado	Protocolo da camada de transporte utilizado	Portas de entrada usadas	Portas de saída usadas	Suporta autenticação	Requer apenas credenciais "só de leitura"	Suporta criptografia	Firewall amigável (portas estáticas)
API REST do OceanStor da Huawei	HTTPS	HTTPS	8088		verdadeiro	verdadeiro	verdadeiro	verdadeiro
API REST do Huawei OceanStor Performance	HTTPS	HTTPS	8088		verdadeiro	falso	verdadeiro	verdadeiro

IBM Cleversafe

Produtos suportados por este coletor de dados:

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
fundação					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

		Versão	Implementado	HTTPS	versão do software
Produto	Categoria	Característica/Atributo	Estado	Protocolo utilizado	Informações adicionais
	Pool de storage	Incluir na capacidade DWH	Implementado	HTTPS	Uma maneira de ACQ para control que piscinas de estorage são interessantes na capacidade DWH
		Nome	Implementado	HTTPS	
		Capacidade do disco físico (MB)	Implementado	HTTPS	usado como capacidade bruta para pool de storage
		Grupo RAID	Implementado	HTTPS	Indica se esse storagePool é um grupo raid
		Relação bruta/utilizável	Implementado	HTTPS	taxa para converter de capacidade utilizável para capacidade bruta
		ID do conjunto de armazenamento	Implementado	HTTPS	
		Thin Provisioning suportado	Implementado	HTTPS	Se esse volume interno é compatível com thin Provisioning para a camada de volume em cima dele
		Capacidade total alocada	Implementado	HTTPS	
		Capacidade total utilizada	Implementado	HTTPS	Capacidade total em MB
		Tipo	Folga	HTTPS	
		Virtual	Implementado	HTTPS	Este é um dispositivo de virtualização de armazenamento ?

APIs de gerenciamento usadas por este coletor de dados:

API	Protocolo utilizado	Protocolo da camada de transporte utilizado	Portas de entrada usadas	Portas de saída usadas	Suporta autenticação	Requer apenas credenciais "só de leitura"	Suporta criptografia	Firewall amigável (portas estáticas)
API REST DO IBM CLEVERSAFE	HTTPS	HTTPS	443		verdadeiro	verdadeiro	verdadeiro	verdadeiro

IBM DS 8K (DSCLI)

Modelos e versões suportados por este coletor de dados:

Modelos	Versões de firmware
2107-951 2107-961 2107-985 2107-996	7.6.31.4250 7.7.51.1400 7.8.57.18 7.9.21.91 7.9.32.126

Produtos suportados por este coletor de dados:

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
fundação					
960					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

	volume	Controlador de protocolo	Implementado	DSNI	
Produto	Categoria	Característica/atributo	Estado	Protocolo utilizado	Informações adicionais
	WWN Alias	Aliases de host	Implementado	DSNI	
		Sistema operacional de host	Implementado	DSNI	
		Tipo Objeto	Implementado	DSNI	
		Fonte	Implementado	DSNI	
		WWN	Implementado	DSNI	

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
desempenho					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

		Total de utilização	Implementado	DSNI	
Produto	Categoria	Característica/Atribuição	Estado	DSNI utilizado	Informações adicionais
	Volume	Taxa de acerto do cache ler	Implementado	DSNI	
		Taxa de acerto do cache total	Implementado	DSNI	
		Cache HIT Ratio Write	Implementado	DSNI	
		Capacidade bruta	Implementado	DSNI	
		Capacidade total	Implementado	DSNI	
		Leitura de IOPS	Implementado	DSNI	Número de IOPS de leitura no disco
		Total de IOPS	Implementado	DSNI	
		Gravação de IOPS	Implementado	DSNI	
		Leitura de latência	Implementado	DSNI	
		Total de latência	Implementado	DSNI	
		Gravação de latência	Implementado	DSNI	
		Taxa de transferência de leitura	Implementado	DSNI	
		Taxa de transferência total	Implementado	DSNI	Taxa total média do disco (leitura e gravação em todos os discos) em MB/s.
		Gravação de taxa de transferência	Implementado	DSNI	

APIs de gerenciamento usadas por este coletor de dados:

API	Protocolo utilizado	Protocolo da camada de transporte utilizado	Portas de entrada usadas	Portas de saída usadas	Suporta autenticação	Requer apenas credenciais "só de leitura"	Suporta criptografia	Firewall amigável (portas estáticas)
Configuração do assistente de origem de dados	Introdução manual				verdadeiro	verdadeiro	verdadeiro	verdadeiro
IBM DS CLI	DSNI	DSNI			verdadeiro	verdadeiro	verdadeiro	verdadeiro

IBM PowerVM (SSH)

Produtos suportados por este coletor de dados:

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
fundação					
970					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

	Disk	OID do VirtualDisk	Implementado	SSH	
Produto	Categoria	Característica/Atividade	Estado	Protocolo utilizado	Informações adicionais
	Host	Contagem de CPU de host	Implementado	SSH	
		Memória instalada do host	Implementado	SSH	
		Modelo anfitrião	Implementado	SSH	
		Contagem de NIC	Implementado	SSH	
		IPS	Implementado	SSH	
		Fabricante	Implementado	SSH	
		Nome	Implementado	SSH	
		OID	Implementado	SSH	
		Tipo de plataforma	Implementado	SSH	
	Informações	Nome da fonte de dados	Implementado	SSH	Informações
		Data	Implementado	SSH	
		ID do originador	Implementado	SSH	

APIs de gerenciamento usadas por este coletor de dados:

API	Protocolo utilizado	Protocolo da camada de transporte utilizado	Portas de entrada usadas	Portas de saída usadas	Suporta autenticação	Requer apenas credenciais "só de leitura"	Suporta criptografia	Firewall amigável (portas estáticas)
Acesso SSH do Console de Gerenciamento de hardware IBM	SSH	SSH	22		verdadeiro	falso	verdadeiro	verdadeiro

IBM SVC (CLI)

Modelos e versões suportados por este coletor de dados:

Modelos	Versões de firmware
2072-AF7 9848-12G 2072-2N4 2072-324 2072-3H4 2072-3N4 2076-124 2076-AE2 9843-24F 2076-AH8 9843-12G 4662-AFF 92G 2078-AF3 4657-924 4662- 2078-24C 2078-24F 2078-324 2078-424 2078-4H4 12F 2078-224 2078-2077-24F 2077-424 2078-AF6 2076-6H2 4666-24G 2076-624 2076-724 2076-824 2076-12F 2076-224 2076-AE3 9846-AG8 9848-AE2 9848-12F 2072-AF8 9848-AG8 SVC	1.5.2.7 1.6.1.2 1.6.1.4 1.6.1.5 7.5.0.11 7.5.0.12 7.7.1.8 7.8.1.14 7.8.1.6 7.8.1.8 8.2.1.10 8.2.1.11 8.2.1.14 8.2.1.9 8.3.1.1 8.3.1.2 8.3.1.5 8.3.1.6 8.3.1.7 8.3.1.9 8.4.0.10 8.4.0.11 8.4.0.6 8.4.0.7 8.4.0.8 8.4.0.9 8.5.0.5 8.5.0.6 8.5.0.7 8.5.0.8 8.5.0.9 8.5.2.2 8.5.3.1 8.5.4.0

Produtos suportados por este coletor de dados:

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
fundação					
974					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/Atributo	Estado	Protocolo utilizado	Informações adicionais
		Virtual	Implementado	SSH	Este é um dispositivo de virtualização de armazenamento
		Capacidade escrita	Implementado	SSH	Capacidade total escrita para este volume por um anfitrião em MB
		Compressão ativada	Implementado	SSH	
		Encriptado	Implementado	SSH	
	Mapa de volume	LUN	Implementado	SSH	Nome do lun de back-end
		Controlador de protocolo	Implementado	SSH	
		Porta de armazenamento	Implementado	SSH	
	Máscara de volume	Iniciador	Implementado	SSH	
		Controlador de protocolo	Implementado	SSH	
		Porta de armazenamento	Implementado	SSH	
		Tipo	Folga	SSH	
	WWN Alias	Aliases de host	Implementado	SSH	
		Tipo Objeto	Implementado	SSH	
		Fonte	Implementado	SSH	
		WWN	Implementado	SSH	

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
desempenho					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

		Total de utilização	Implementado	SSH	
Produto	Categoria	Característica/Atribuição	Estado	Protocolo utilizado	Informações adicionais
	Volume	Taxa de acerto do cache ler	Implementado	SSH	
		Taxa de acerto do cache total	Implementado	SSH	
		Cache HIT Ratio Write	Implementado	SSH	
		Capacidade bruta	Implementado	SSH	
		Capacidade total	Implementado	SSH	
		Capacidade utilizada	Implementado	SSH	
		Capacidade escrita	Implementado	SSH	
		Relação capacidade utilizada	Implementado	SSH	
		Capacidade escrita	Implementado	SSH	
		Leitura de IOPS	Implementado	SSH	Número de IOPS de leitura no disco
		Total de IOPS	Implementado	SSH	
		Gravação de IOPS	Implementado	SSH	
		Leitura de latência	Implementado	SSH	
		Total de latência	Implementado	SSH	
		Gravação de latência	Implementado	SSH	
		Taxa de transferência de leitura	Implementado	SSH	
		Taxa de transferência total	Implementado	SSH	Taxa total média do disco (leitura e gravação em todos os discos) em MB/s.
		Gravação de taxa de transferência	Implementado	SSH	

APIs de gerenciamento usadas por este coletor de dados:

API	Protocolo utilizado	Protocolo da camada de transporte utilizado	Portas de entrada usadas	Portas de saída usadas	Suporta autenticação	Requer apenas credenciais "só de leitura"	Suporta criptografia	Firewall amigável (portas estáticas)
CLI DO IBM SVC	SSH	SSH	22		verdadeiro	falso	verdadeiro	verdadeiro

IBM XIV E A9000 (XIVCLI)

Modelos e versões suportados por este coletor de dados:

Modelos	Versões de firmware
415 A14	10.2.4.e 12.3.2.c

Produtos suportados por este coletor de dados:

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
fundação					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

		protocolo			
	Máscara de volume	Iniciador	Implementado	XIV CLI	
Produto	Categoria	Característica/Atributo	Estado	Protocolo utilizado	Informações adicionais
	WWN Alias	Aliases de host	Implementado	XIV CLI	
		Sistema operacional de host	Implementado	XIV CLI	
		Tipo Objeto	Implementado	XIV CLI	
		Fonte	Implementado	XIV CLI	
		WWN	Implementado	XIV CLI	

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
desempenho					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/Atributo	Estado	Protocolo utilizado	Informações adicionais
		Taxa de capacidade de leitura bruta	Implementado	DSNI	Relatado como uma série de informações
		Taxa de capacidade de gravação bruta	Implementado	DSNI	
	Volume	Total de latência	Implementado	DSNI	
		Leitura de latência	Implementado	DSNI	
		Gravação de IOPS	Implementado	DSNI	
		Espaço de economia de compressão	Implementado	DSNI	
		Taxa de transferência de leitura	Implementado	DSNI	
		Total de IOPS	Implementado	DSNI	
		Gravação de latência	Implementado	DSNI	
		Leitura de IOPS	Implementado	DSNI	Número de IOPS de leitura no disco
		Taxa de acerto do cache ler	Implementado	DSNI	
		Economia de compressão total	Implementado	DSNI	
		Taxa de acerto do cache total	Implementado	DSNI	
		Cache HIT Ratio Write	Implementado	DSNI	
		Gravação de taxa de transferência	Implementado	DSNI	
		Taxa de transferência total	Implementado	DSNI	Taxa total média do disco (leitura e gravação em todos os discos) em MB/s.

APIs de gerenciamento usadas por este coletor de dados:

API	Protocolo utilizado	Protocolo da camada de transporte utilizado	Portas de entrada usadas	Portas de saída usadas	Suporta autenticação	Requer apenas credenciais "só de leitura"	Suporta criptografia	Firewall amigável (portas estáticas)
IBM DS CLI	DSNI	DSNI			verdadeiro	verdadeiro	verdadeiro	verdadeiro
IBM XIV CLI	XIV CLI	TCP	7778		verdadeiro	falso	verdadeiro	falso

Infinidat Infinibox (HTTP)

Modelos e versões suportados por este coletor de dados:

Modelos	Versões de firmware
F6230 F6240 F6303 F6304	6.0.31.0 7.0.14.20

Produtos suportados por este coletor de dados:

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
fundação					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/atributo	Protocolo		Protocolo utilizado	Informações adicionais
			Estado	Folga		
Máscara de volume	Máscara de volume	Iniciador	Implementado		HTTPS	
		Controlador de protocolo	Implementado		HTTPS	
		Tipo	Folga		HTTPS	
		Porta de armazenamento	Implementado		HTTPS	
	WWN Alias	Fonte	Implementado		HTTPS	
		Aliases de host	Implementado		HTTPS	
		WWN	Implementado		HTTPS	
		Tipo Objeto	Implementado		HTTPS	

APIs de gerenciamento usadas por este coletor de dados:

API	Protocolo utilizado	Protocolo da camada de transporte utilizado	Portas de entrada usadas	Portas de saída usadas	Suporta autenticação	Requer apenas credenciais "só de leitura"	Suporta criptografia	Firewall amigável (portas estáticas)
Infinidat REST API	HTTPS	HTTPS	443		verdadeiro	verdadeiro	verdadeiro	verdadeiro

Computação do Microsoft Azure

Modelos e versões suportados por este coletor de dados:

Versões da API:

- 1 de junho de 2018

Produtos suportados por este coletor de dados:

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
fundação					
1008					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

	Disk	OID do VirtualDisk	Implementado	HTTPS	
Produto	Categoria	Característica/Attribute	Estado	Protocolo utilizado	Informações adicionais
	Host	Sistema operacional de host	Implementado	HTTPS	
		IPS	Implementado	HTTPS	
		Fabricante	Implementado	HTTPS	
		Nome	Implementado	HTTPS	
		OID	Implementado	HTTPS	
	Informações	Descrição da API	Implementado	HTTPS	
		Nome da API	Implementado	HTTPS	
		Versão da API	Implementado	HTTPS	
		Nome da fonte de dados	Implementado	HTTPS	Informações
		Data	Implementado	HTTPS	
		ID do originador	Implementado	HTTPS	
		Chave originadora	Implementado	HTTPS	

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
desempenho					

Produto	Categoria	Característica/Atributo	Estado	Protocolo utilizado	Informações adicionais
		Gravação de Característica/Atributo	Implementado	HTTPS	todos os discos) em MB/s.
	vm	Utilização total da CPU	Implementado	HTTPS	
		Leitura de IOPS	Implementado	HTTPS	Número de IOPS de leitura no disco
		Disklops.Total	Implementado	HTTPS	
		Gravação de IOPs de disco	Implementado	HTTPS	
		Taxa de transferência do disco lida	Implementado	HTTPS	
		Taxa de transferência de leitura	Implementado	HTTPS	leitura da taxa de transferência total do disco
		Gravação da taxa de transferência do disco	Implementado	HTTPS	
		Taxa de transferência IP lida	Implementado	HTTPS	
		Taxa de transferência total	Implementado	HTTPS	Taxa de transferência IP total
		IpThroughput.write	Implementado	HTTPS	

APIs de gerenciamento usadas por este coletor de dados:

API	Protocolo utilizado	Protocolo da camada de transporte utilizado	Portas de entrada usadas	Portas de saída usadas	Suporta autenticação	Requer apenas credenciais "só de leitura"	Suporta criptografia	Firewall amigável (portas estáticas)
API REST do Microsoft Azure Compute	HTTPS	HTTPS	443		verdadeiro	verdadeiro	verdadeiro	verdadeiro

Microsoft Hyper-V

Produtos suportados por este coletor de dados:

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
fundação					
1014					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/Atributo	Estado	Protocolo utilizado	Informações adicionais
		Capacidade provisionada	Implementado	WMI	
	VirtualMachine Disk	OID	Implementado	WMI	
		OID do VirtualDisk	Implementado	WMI	
		OID do VirtualMachine	Implementado	WMI	
	Host	Contagem de CPU de host	Implementado	WMI	
		Velocidade da CPU do host	Implementado	WMI	
		Domínio anfitrião	Implementado	WMI	
		Memória instalada do host	Implementado	WMI	
		Modelo anfitrião	Implementado	WMI	
		Contagem de NIC	Implementado	WMI	
		Velocidade da NIC	Implementado	WMI	
		IPS	Implementado	WMI	
		Fabricante	Implementado	WMI	
		Nome	Implementado	WMI	
		OID	Implementado	WMI	
		Tipo de plataforma	Implementado	WMI	
	Nó iSCSI	Aliases de host	Implementado	WMI	
		Nome do nó	Implementado	WMI	
		OID	Implementado	WMI	
		Tipo	Folga	WMI	
	Informações	Nome da fonte de dados	Implementado	WMI	Informações
		Data	Implementado	WMI	
		ID do originador	Implementado	WMI	

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
desempenho					
1018					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/Atributo	Estado	Protocolo utilizado	Informações adicionais
		Gravação de Característica/Atributo	Implementado	WS-Management	
	vm	Capacidade total	Implementado	WS-Management	
	vm	Capacidade utilizada	Implementado	WS-Management	
	vm	Relação capacidade utilizada	Implementado	WS-Management	
	vm	Utilização total da CPU	Implementado	WS-Management	
	vm	Leitura de IOPS	Implementado	WS-Management	Número de IOPS de leitura no disco
	vm	Disklops.Total	Implementado	WS-Management	
	vm	Gravação de IOPs de disco	Implementado	WS-Management	
	vm	Total de latência	Implementado	WS-Management	
	vm	Taxa de transferência do disco lida	Implementado	WS-Management	
	vm	Taxa de transferência de leitura	Implementado	WS-Management	leitura da taxa de transferência total do disco
	vm	Gravação da taxa de transferência do disco	Implementado	WS-Management	
	vm	Taxa de transferência IP lida	Implementado	WS-Management	
	vm	Taxa de transferência total	Implementado	WS-Management	Taxa de transferência IP total
	vm	IpThroughput.write	Implementado	WS-Management	

APIs de gerenciamento usadas por este coletor de dados:

API	Protocolo utilizado	Protocolo da camada de transporte utilizado	Portas de entrada usadas	Portas de saída usadas	Suporta autenticação	Requer apenas credenciais "só de leitura"	Suporta criptografia	Firewall amigável (portas estáticas)
PowerShell	WS-Management	HTTP	5985		verdadeiro	falso	falso	verdadeiro
WMI	WMI	WMI	135		verdadeiro	falso	verdadeiro	verdadeiro

Modo NetApp 7

Modelos e versões suportados por este coletor de dados:

Versões de API	Modelos	Versões de firmware
1,12 1,14 1,17 1,19 1,20 1,21	FAS2040 FAS2050 FAS2220 FAS2240-2 FAS2240-4 FAS2520 FAS2554 FAS3140 FAS3160 FAS3210 FAS3220 FAS3240 FAS3250 FAS3270 FAS6240 FAS6290 FAS8020 FAS8040 FAS8060 FAS8080 N6070 N6240 V3240	7.3.6 8.1.1 7 7 8,2 7 7 8,2 7 Data ONTAP 7.3.3-Mode 7 8.2.4 7 8,2 7 8.2.5 7 8,2 7 7 Data ONTAP 7.3.4.3P2 8,2 8,2 7 8,2 8,2 7 8,2 7 Data ONTAP 8.2.5 7-Mode 8,2.4P1 7-Mode 8.2.3 7.4P10 8.2.1 7-Mode 8,1.4P9D18 7-Mode 7-Mode 8.2.2 7-Mode 8,1-Mode 8,1.3P2 8,1- Mode 7.3P3 7-Mode

Produtos suportados por este coletor de dados:

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
fundação					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Controlador de protocolo	Implementado		back-end
		Característica/Atributo	Estado	Protocolo utilizado	Informações adicionais
	Máscara de volume	Iniciador	Implementado		
		Controlador de protocolo	Implementado		
		Porta de armazenamento	Implementado		
		Tipo	Folga		

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
desempenho					
1038					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

		Total de utilização	Implementado		
Produto	Categoria	Característica/Atribuição	Estado	Protocolo utilizado	Informações adicionais
	Volume	Capacidade bruta	Implementado		
		Capacidade total	Implementado		
		Capacidade utilizada	Implementado		
		Relação capacidade utilizada	Implementado		
		Densidade de e/S lida	Implementado		
		Densidade total de e/S	Implementado		
		Densidade de e/S de gravação	Implementado		
		Leitura de IOPS	Implementado		Número de IOPS de leitura no disco
		Total de IOPS	Implementado		
		Gravação de IOPS	Implementado		
		Leitura de latência	Implementado		
		Total de latência	Implementado		
		Gravação de latência	Implementado		
		Relação bloqueada parcial	Implementado		
		Taxa de transferência de leitura	Implementado		
		Taxa de transferência total	Implementado		Taxa total média do disco (leitura e gravação em todos os discos) em MB/s.
		Gravação de taxa de transferência	Implementado		
		Escrever pendente	Implementado		total de escrita pendente

APIs de gerenciamento usadas por este coletor de dados:

API	Protocolo utilizado	Protocolo da camada de transporte utilizado	Portas de entrada usadas	Portas de saída usadas	Suporta autenticação	Requer apenas credenciais "só de leitura"	Suporta criptografia	Firewall amigável (portas estáticas)
NetApp 7 modo ZAPI	ZAPI	ZAPI			verdadeiro	verdadeiro	verdadeiro	verdadeiro

NetApp Cloud Volumes Service

Modelos e versões suportados por este coletor de dados:

Modelos	Versões de firmware
AWS Cloud volumes	v1

Produtos suportados por este coletor de dados:

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
fundação					
1046					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

		alocada	Implementado		usado como capacidade bruta
Produto	Categoria	Característica/Atributo	Estado	Protocolo utilizado	Informações adicionais
		Relação bruta/utilizável	Implementado		taxa para converter de capacidade utilizável para capacidade bruta

APIs de gerenciamento usadas por este coletor de dados:

API	Protocolo utilizado	Protocolo da camada de transporte utilizado	Portas de entrada usadas	Portas de saída usadas	Suporta autenticação	Requer apenas credenciais "só de leitura"	Suporta criptografia	Firewall amigável (portas estáticas)
API REST do Cloud Volumes Service	HTTPS	HTTPS	443		verdadeiro	verdadeiro	verdadeiro	verdadeiro

Amazon FSX para NetApp ONTAP

Modelos e versões suportados por este coletor de dados:

Modelos	Versões de firmware
FSX para ONTAP	Data ONTAP

Produtos suportados por este coletor de dados:

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
fundação					
1052					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/Atributo	Estado	Protocolo utilizado	Informações adicionais
	VirtualMachine	Volume	Implementado	HTTPS	Capacidade de captura instantânea usada em MB
		Grupo de discos	Implementado	HTTPS	Tipo de Grupo de discos
		Caminho de junção	Implementado	HTTPS	
		Último tempo de acesso conhecido	Implementado	HTTPS	Último acesso ao volume
		Nome	Implementado	HTTPS	
		ID Qtree	Implementado	HTTPS	id único da qtree
		Capacidade bruta total	Implementado	HTTPS	Capacidade bruta total (soma de todos os discos no array)
		ID do conjunto de armazenamento	Implementado	HTTPS	
		Thin Provisioning	Implementado	HTTPS	
		Tipo	Folga	HTTPS	
		UUID	Implementado	HTTPS	
		Capacidade utilizada	Implementado	HTTPS	
		Encriptado	Implementado	HTTPS	
	Mapa de volume	LUN	Implementado	HTTPS	Nome do lun de back-end
		Controlador de protocolo	Implementado	HTTPS	
		Porta de armazenamento	Implementado	HTTPS	
		Tipo	Folga	HTTPS	
	Máscara de volume	Iniciador	Implementado	HTTPS	
		Controlador de protocolo	Implementado	HTTPS	
		Porta de armazenamento	Implementado	HTTPS	
		Tipo	Folga	HTTPS	

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
Desempenho	Armazenamento	Discos com falha	Implementado	HTTPS	
	Nó de storage	Taxa de acerto do cache total	Implementado	HTTPS	
		Leitura total do disco substituída	Implementado	HTTPS	
		Total de utilização	Implementado	HTTPS	
	QTree		Implementado	HTTPS	

APIs de gerenciamento usadas por este coletor de dados:

API	Protocolo utilizado	Protocolo da camada de transporte utilizado	Portas de entrada usadas	Portas de saída usadas	Suporta autenticação	Requer apenas credenciais "só de leitura"	Suporta criptografia	Firewall amigável (portas estáticas)
API NetApp ONTAP	HTTP/HTTPS	HTTP/HTTPS	80/443		verdadeiro	verdadeiro	verdadeiro	verdadeiro

NetApp Clustered Data ONTAP 8.1,1 mais

Modelos e versões suportados por este coletor de dados:

Modelos	Versões de firmware
AFF-A150 AFF-A200 AFF-A220 AFF-A250 AFF-A300 AFF-A320 AFF-C250 AFF-C400 AFF-C800 AFF8020 AFF8040 AFF8060 AFF8080 CDvM100 CDvM200 DM5000H FAS2240 AFF-A800 AFF-A900 AFF-C190 AFF-A400 AFF-A700 AFF-A700s-2 FAS2240-4 FAS2520 FAS2552 FAS2554 FAS2620 FAS2650 FAS2720 FAS2750 FAS3220 FAS3250 FAS3270 FAS500f FAS6210 FAS6220 FAS8020 FAS8040 FAS8060 FAS8080 FAS8200 FAS8300 FAS8700 FAS9000 FAS9500 FASDvM300 SIMBOX V6240	8,2 9,1 9.11.1 9.13.1.3P5 8.3.0 8.3.1 8,3 9,1 9,1 9.12.1.1P2 8.3.2 8,3 9,1 9.10.0 9.10.1 9.13.0.2P12 8,3.2P2 8,3.2P5 9.0.1 9.1.0 9,1.0P1 9,1.0P10 9,1.0P11 9,1.0P12 9,1.0P14 9,1.0P15 9,1.0P17 9,1.0P19 9,3 9,3 9,3 9,3 9,3 9,3 9,3 9,3 9,3 9,3 9,3 9,3 9,3 9,3 9,3 9.4.0 9,4 9,4 9,4 9,4 9.5.0 9,5 9,5 9,5 9,5 9,5 9,5 9,5 9,5 9,5 9,5 9,5 9,5 9,5 9,5 9,5 9,5 9,5 9.6.0 9,6 9,6 9,6 9,6 9,6 9,6 9,6 9,6 9,6 9.7.0 9,7 9.8.0 9,8 9,8 9,8 9,8 9,8 9,8 9,8 9,8 9,8 9,8 9,8 9,8 9,8 9,8 9,8 9,8 9,8 9,8 9,8 9.9.0 9.9.1 9,9 9,9 9,9 9,9 9,9 9,9 9,9 9,9 9,9 9,9 9,9 9,9 9,9 9,9 9,9 9,9

Produtos suportados por este coletor de dados:

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
fundação					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/Atributo	Estado	Protocolo utilizado	Informações adicionais
		Limite de IOPS de QoS	Implementado	HTTPS	
		Limite de QoS EM MBPS	Implementado	HTTPS	
		Limite de QoS bruto	Implementado	HTTPS	
		QoS - Política	Implementado	HTTPS	
	Mapa de volume	LUN	Implementado	HTTPS	Nome do lun de back-end
		Controlador de protocolo	Implementado	HTTPS	
		Porta de armazenamento	Implementado	HTTPS	
		Tipo	Folga	HTTPS	
	Máscara de volume	Iniciador	Implementado	HTTPS	
		Controlador de protocolo	Implementado	HTTPS	
		Porta de armazenamento	Implementado	HTTPS	
		Tipo	Folga	HTTPS	

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
desempenho					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/Atributo	Estado	Protocolo utilizado	Informações adicionais
		Gravação de transferência	Implementado	HTTPS	
	Volume	Capacidade bruta	Implementado	HTTPS	
		Capacidade total	Implementado	HTTPS	
		Capacidade utilizada	Implementado	HTTPS	
		Relação capacidade utilizada	Implementado	HTTPS	
		Densidade de e/S lida	Implementado	HTTPS	
		Densidade total de e/S	Implementado	HTTPS	
		Densidade de e/S de gravação	Implementado	HTTPS	
		Leitura de IOPS	Implementado	HTTPS	Número de IOPS de leitura no disco
		Total de IOPS	Implementado	HTTPS	
		Gravação de IOPS	Implementado	HTTPS	
		Leitura de latência	Implementado	HTTPS	
		Total de latência	Implementado	HTTPS	
		Gravação de latência	Implementado	HTTPS	
		Relação bloqueada parcial	Implementado	HTTPS	
		Taxa de transferência de leitura	Implementado	HTTPS	
		Taxa de transferência total	Implementado	HTTPS	Taxa total média do disco (leitura e gravação em todos os discos) em MB/s.
		Gravação de taxa de transferência	Implementado	HTTPS	

APIs de gerenciamento usadas por este coletor de dados:

API	Protocolo utilizado	Protocolo da camada de transporte utilizado	Portas de entrada usadas	Portas de saída usadas	Suporta autenticação	Requer apenas credenciais "só de leitura"	Suporta criptografia	Firewall amigável (portas estáticas)
API NetApp ONTAP	HTTP/HTTPS	HTTP/HTTPS	80/443		verdadeiro	verdadeiro	verdadeiro	verdadeiro

NetApp SolidFire 8,1 mais

Modelos e versões suportados por este coletor de dados:

Modelos	Versões de firmware
H410S-2 H610S-2 H610S-4 SF19210 SF2405 SF38410 SF4805 SF9605 SF9608 FCN001 H300S H410S-0 H410S-1 H410S-2 H500S H610S-1 H610S-2 H610S-4 H610S2 SF19210 SF38410 SF4805 SF9605	11.1.0.72 11.5.0.63 11.7.0.76 11.8.0.23 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

Produtos suportados por este coletor de dados:

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
fundação					
1100					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Características/Requisitos	Estado	Protocolo utilizado	Informações adicionais
		IOPS de sequência de QoS	Implementado	HTTPS	
		IOPS mín. Do qos	Implementado	HTTPS	
		QoS - Política	Implementado	HTTPS	
	Mapa de volume	LUN	Implementado	HTTPS	Nome do lun de back-end
		Máscara necessária	Implementado	HTTPS	
		Controlador de protocolo	Implementado	HTTPS	
		Porta de armazenamento	Implementado	HTTPS	
		Tipo	Folga	HTTPS	
	Máscara de volume	Iniciador	Implementado	HTTPS	
		Controlador de protocolo	Implementado	HTTPS	
		Porta de armazenamento	Implementado	HTTPS	
		Tipo	Folga	HTTPS	

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
desempenho					
1108					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Capacidade total	Implementado	HTTPS	Informações adicionais
		Característica/Atributo	Estado	Protocolo utilizado	
Volume	Capacidade bruta	Implementado	HTTPS		
	Capacidade total	Implementado	HTTPS		
	Capacidade utilizada	Implementado	HTTPS		
	Relação capacidade utilizada	Implementado	HTTPS		
	Economia de compressão total	Implementado	HTTPS		
	Leitura de IOPS	Implementado	HTTPS	Número de IOPS de leitura no disco	
	Total de IOPS	Implementado	HTTPS		
	Gravação de IOPS	Implementado	HTTPS		
	Leitura de latência	Implementado	HTTPS		
	Total de latência	Implementado	HTTPS		
	Gravação de latência	Implementado	HTTPS		
	Relação bloqueada parcial	Implementado	HTTPS		
	Taxa de transferência de leitura	Implementado	HTTPS		
	Taxa de transferência total	Implementado	HTTPS	Taxa total média do disco (leitura e gravação em todos os discos) em MB/s.	
	Gravação de taxa de transferência	Implementado	HTTPS		
	Total de utilização	Implementado	HTTPS		

APIs de gerenciamento usadas por este coletor de dados:

API	Protocolo utilizado	Protocolo da camada de transporte utilizado	Portas de entrada usadas	Portas de saída usadas	Suporta autenticação	Requer apenas credenciais "só de leitura"	Suporta criptografia	Firewall amigável (portas estáticas)
API REST do SolidFire	HTTPS	HTTPS	443		verdadeiro	verdadeiro	verdadeiro	verdadeiro

NetApp StorageGRID (HTTPS)

Modelos e versões suportados por este coletor de dados:

Versões de API	Modelos	Versões de firmware
3,0 3,2 3,3 3,4 3,5	Webscale	11.2.0 11.4.0 11.4.0.3 11.4.0.4 11.5.0.1 11.5.0.11 11.5.0.2 11.5.0.3 11.5.0.6 11.5.0.7 11.5.0.8 11.5.0.9 11.6.0 11.6.0.1 11.6.0.10 11.6.0.2 11.6.0.4 11.6.0.5 11.6.0.7 11.6.0.8 11.6.0.9 11.7.0

Produtos suportados por este coletor de dados:

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
fundação					
1114					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/Atributo	Estado	Protocolo utilizado	Informações adicionais
	Pool de storage	Incluir na capacidade DWH	Implementado	HTTPS	Uma maneira de ACQ para control que piscinas de estorage são interessantes na capacidade DWH
		Nome	Implementado	HTTPS	
		Capacidade do disco físico (MB)	Implementado	HTTPS	usado como capacidade bruta para pool de storage
		Grupo RAID	Implementado	HTTPS	Indica se esse storagePool é um grupo raid
		Relação bruta/utilizável	Implementado	HTTPS	taxa para converter de capacidade utilizável para capacidade bruta
		ID do conjunto de armazenamento	Implementado	HTTPS	
		Thin Provisioning suportado	Implementado	HTTPS	Se esse volume interno é compatível com thin Provisioning para a camada de volume em cima dele
		Capacidade total alocada	Implementado	HTTPS	
		Capacidade total utilizada	Implementado	HTTPS	Capacidade total em MB
		Tipo	Folga	HTTPS	
		Virtual	Implementado	HTTPS	Este é um dispositivo de virtualização de armazenamento ?

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
desempenho					
1120					

Produto	Categoria	Característica/Atributo	Estado	Protocolo utilizado	Informações adicionais
	Nó de storage	Capacidade dos StoragePools	Implementado		
		Meta dados permitidos utilização capacidade nó	Implementado		
		Total de utilização da capacidade do nó	Implementado		
		Utilização da capacidade do nó utilizável	Implementado		
		Utilização da capacidade do nó usada	Implementado		
		Utilização da capacidade do nó Meta Data usada	Implementado		
		Taxa de transferência de leitura	Implementado		
		Taxa de transferência total	Implementado		Taxa total média do disco (leitura e gravação em todos os discos) em MB/s.
	Disco do StoragePool	Gravação de taxa de transferência	Implementado		
		Capacidade provisionada	Implementado		
Capacidade bruta		Implementado			Capacidade total
Implementado				Capacidade utilizada	Implementado
			Taxa de capacidade de excesso de compromisso	Implementado	
Relatado como uma série temporal		Relação capacidade utilizada	Implementado		

APIs de gerenciamento usadas por este coletor de dados:

API	Protocolo utilizado	Protocolo da camada de transporte utilizado	Portas de entrada usadas	Portas de saída usadas	Suporta autenticação	Requer apenas credenciais "só de leitura"	Suporta criptografia	Firewall amigável (portas estáticas)
API REST do StorageGRID	HTTPS	HTTPS	443		verdadeiro	falso	verdadeiro	verdadeiro

Armazenamento Nutanix (RESTO)

Modelos e versões suportados por este coletor de dados:

Modelos	Versões de firmware
HPE DL360-8035 G7 NX-G7 8150-8150 NX-G6-G6 NX-G6-G6 NX-G7-5155 HPE DL360-8 G10 HPE DL380-12 G10 NX-3060-G5 NX-3170-8150 NX-G7 NX-8035-3170 NX-8035-G6 NX-8 G10 NX-3060 NX-G8	6.5.1.6 6.5.2 6.5.2.5 6.5.2.6 6.5.2.7 6.5.3 6.5.3.1

Produtos suportados por este coletor de dados:

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
fundação					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/Atributo	Estado	Protocolo utilizado	Informações adicionais
		Tipo	Folga	Utilizado	
		porta de armazenamento	Implementado	HTTPS	
		protocolo			
	Máscara de volume	Iniciador	Implementado	HTTPS	
		Controlador de protocolo	Implementado	HTTPS	
		Porta de armazenamento	Implementado	HTTPS	
		Tipo	Folga	HTTPS	

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
desempenho					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/Atributo	Estado	Protocolo utilizado	Informações adicionais
	Implementado	HTTPS	Taxa total média do disco (leitura e gravação em todos os discos) em MB/s.		Gravação de taxa de transferência
	Implementado	HTTPS		Volume	Leitura de IOPS
	Implementado	HTTPS	Número de IOPS de leitura no disco		Total de IOPS
	Implementado	HTTPS			Gravação de IOPS
	Implementado	HTTPS			Leitura de latência
	Implementado	HTTPS			Total de latência
	Implementado	HTTPS			Gravação de latência
	Implementado	HTTPS			Taxa de transferência de leitura
	Implementado	HTTPS			Taxa de transferência total
	Implementado	HTTPS	Taxa total média do disco (leitura e gravação em todos os discos) em MB/s.		Gravação de taxa de transferência

APIs de gerenciamento usadas por este coletor de dados:

API	Protocolo utilizado	Protocolo da camada de transporte utilizado	Portas de entrada usadas	Portas de saída usadas	Suporta autenticação	Requer apenas credenciais "só de leitura"	Suporta criptografia	Firewall amigável (portas estáticas)
NUTANIX REST API	HTTPS	HTTPS	443		verdadeiro	verdadeiro	verdadeiro	verdadeiro

OPENSTACK (API REST / SSH)

Produtos suportados por este coletor de dados:

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
fundação					
1138					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/Attribute	Estado	Protocolo utilizado	Informações adicionais
	Disk	OID do VirtualDisk	Implementado	HTTPS	
	Host	Contagem de CPU de host	Implementado	HTTPS	
	Host	Domínio anfitrião	Implementado	HTTPS	
	Host	Memória instalada do host	Implementado	HTTPS	
	Host	Sistema operacional de host	Implementado	HTTPS	
	Host	IPS	Implementado	HTTPS	
	Host	Nome	Implementado	HTTPS	
	Host	OID	Implementado	HTTPS	
	Nó iSCSI	Aliases de host	Implementado	HTTPS	
	Nó iSCSI	Nome do nó	Implementado	HTTPS	
	Nó iSCSI	OID	Implementado	HTTPS	
	Nó iSCSI	Tipo	Folga	HTTPS	
	Informações	Nome da fonte de dados	Implementado	HTTPS	Informações
	Informações	Data	Implementado	HTTPS	
	Informações	ID do originador	Implementado	HTTPS	
	Informações	Chave originadora	Implementado	HTTPS	

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
desempenho	Armazenamento de dados	Capacidade total	Implementado		
		Relação capacidade utilizada	Implementado		
		Capacidade provisionada	Implementado		
		Capacidade utilizada	Implementado		
		Taxa de capacidade de excesso de compromisso	Implementado		Relatado como uma série temporal
	Host	Utilização total da CPU	Implementado		
		Utilização total da memória	Implementado		
	Disco virtual	Leitura de latência	Implementado		
		Total de latência	Implementado		
		Gravação de latência	Implementado		

APIs de gerenciamento usadas por este coletor de dados:

API	Protocolo utilizado	Protocolo da camada de transporte utilizado	Portas de entrada usadas	Portas de saída usadas	Suporta autenticação	Requer apenas credenciais "só de leitura"	Suporta criptografia	Firewall amigável (portas estáticas)
API REST do OpenStack	HTTPS	HTTPS	443		verdadeiro	falso	verdadeiro	verdadeiro
SSH OpenStack	SSH	SSH	22		verdadeiro	falso	verdadeiro	verdadeiro

Oracle ZFS (HTTPS)

Modelos e versões suportados por este coletor de dados:

Modelos	Versões de firmware
Armazenamento Sun ZFS 7330 armazenamento Sun ZFS 7335 armazenamento Sun ZFS 7350 armazenamento Sun ZFS 7370 armazenamento Sun ZFS 7420 armazenamento Sun ZFS 7430 armazenamento Sun ZFS 7450	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 2013.06.05.8.0 2013.06.05.8.26 2013.06.05.8.29 2013.06.05.8.35 2013.06.05.8.37 2013.06.05.8.47 2013.06.05.8.50 2013.06.05.8.53 2013.06.05.8.6 2013.06.05.8.7

Produtos suportados por este coletor de dados:

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
fundação					
1144					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

		Capacidade utilizada	Implementado	HTTP/S	
Produto	Categoria	Característica/Atributo	Estado	Protocolo utilizado	Informações adicionais
	Mapa de volume	LUN	Implementado	HTTP/S	Nome do lun de back-end
		Porta de armazenamento	Implementado	HTTP/S	
		Máscara necessária	Implementado	HTTP/S	
		Controlador de protocolo	Implementado	HTTP/S	
		Tipo	Folga	HTTP/S	
	Máscara de volume	Porta de armazenamento	Implementado	HTTP/S	
		Iniciador	Implementado	HTTP/S	
		Controlador de protocolo	Implementado	HTTP/S	
		Tipo	Folga	HTTP/S	

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
desempenho					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/Atribuição	Estado	Protocolo utilizado	Informações adicionais	
		Taxa de acerto do cache total	Implementado			
	Disco do StoragePool	Total de IOPS	Implementado			
		Capacidade total	Implementado			
		Relação capacidade utilizada	Implementado			
		Capacidade total de dados	Implementado			
		Capacidade provisionada	Implementado			
		Capacidade de dados utilizados	Implementado			
		Capacidade utilizada	Implementado			
		Outra capacidade utilizada	Implementado			
		Capacidade bruta	Implementado			
		Taxa de capacidade de excesso de compromisso	Implementado			Relatado como uma série temporal
		Capacidade utilizada do Snapshot	Implementado			
		Taxa de capacidade usada do Snapshot	Implementado			Relatado como uma série temporal

APIs de gerenciamento usadas por este coletor de dados:

API	Protocolo utilizado	Protocolo da camada de transporte utilizado	Portas de entrada usadas	Portas de saída usadas	Suporta autenticação	Requer apenas credenciais "só de leitura"	Suporta criptografia	Firewall amigável (portas estáticas)
API REST DO ORACLE ZFS	HTTP/HTTPS	HTTP/HTTPS	215		verdadeiro	verdadeiro	verdadeiro	verdadeiro

Pure Storage FlashArray (HTTP)

Modelos e versões suportados por este coletor de dados:

Modelos	Versões de firmware
DFSC1 X70 FA-420 FA-FA-X10R3 FA-X10R3 FA-X10R3 FA-X10R3 FA-X20R2 FA-X20R3 FA-X20R3 FA-X50R3 FA-X50R3 FA-X70R3 FA-X70R3 FA-X70R3 FA-M20 FA-M70 FA-M50 XL170 C60 450 FA-XL130	4.8.8 5.3.14 5.3.15 5.3.17 5.3.18 5.3.20 5.3.21 5.3.6 5.3.8 6.1.10 6.1.11 6.1.13 6.1.14 6.1.15 6.1.17 6.1.18 6.1.19 6.1.21 6.1.22 6.1.23 6.1.5 6.2.13 6.2.7 6.2.9 6.3.10 6.3.11 6.3.12 6.3.2 6.3.5 6.3.6 6.3.7 6.3.9 6.4.3 6.4.4 6.4.5

Produtos suportados por este coletor de dados:

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
fundação					
1158					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/Atributo	Estado	Protocolo Utilizado	Informações adicionais
		protocolo			
		Porta de armazenamento	Implementado	HTTP/S	
		Iniciador	Implementado	HTTP/S	
		Controlador de protocolo	Implementado	HTTP/S	
		Porta de armazenamento	Implementado	HTTP/S	
		Tipo	Folga	HTTP/S	
	Máscara de volume				
	WWN Alias	Aliases de host	Implementado	HTTP/S	
		Tipo Objeto	Implementado	HTTP/S	
		Fonte	Implementado	HTTP/S	
		WWN	Implementado	HTTP/S	

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
desempenho					
1166					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/Atributo	Estado	Protocolo utilizado	Informações adicionais
		Capacidade bruta	Implementado		
		Capacidade total	Implementado		
		Capacidade utilizada	Implementado		
		Relação capacidade utilizada	Implementado		
		Leitura de IOPS	Implementado		Número de IOPS de leitura no disco
		Total de IOPS	Implementado		
		Gravação de IOPS	Implementado		
		Leitura de latência	Implementado		
		Total de latência	Implementado		
		Gravação de latência	Implementado		
		Taxa de transferência de leitura	Implementado		
		Taxa de transferência total	Implementado		Taxa total média do disco (leitura e gravação em todos os discos) em MB/s.
		Gravação de taxa de transferência	Implementado		

APIs de gerenciamento usadas por este coletor de dados:

API	Protocolo utilizado	Protocolo da camada de transporte utilizado	Portas de entrada usadas	Portas de saída usadas	Suporta autenticação	Requer apenas credenciais "só de leitura"	Suporta criptografia	Firewall amigável (portas estáticas)
API REST do Pure Storage	HTTP/HTTPS	HTTP/HTTPS	80/443		verdadeiro	verdadeiro	verdadeiro	verdadeiro

Red Hat RHV (RESTO)

Produtos suportados por este coletor de dados:

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
fundação					
1170					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

	Disk	OID do VirtualMachine	Implementado	HTTP/S	
Produto	Categoria	Característica/atributo	Estado	Protocolo utilizado	Informações adicionais
	Host	OID	Implementado	HTTP/S	
		Nome	Implementado	HTTP/S	
		IPS	Implementado	HTTP/S	
		Tipo de plataforma	Implementado	HTTP/S	
		Memória instalada do host	Implementado	HTTP/S	
		Fabricante	Implementado	HTTP/S	
		Modelo anfitrião	Implementado	HTTP/S	
		Contagem de CPU de host	Implementado	HTTP/S	
		Velocidade da CPU do host	Implementado	HTTP/S	
		Contagem de NIC	Implementado	HTTP/S	
		Velocidade da NIC	Implementado	HTTP/S	
	Nó iSCSI	OID	Implementado	HTTP/S	
		Nome do nó	Implementado	HTTP/S	
		Tipo	Folga	HTTP/S	
	Informações	Nome da fonte de dados	Implementado	HTTP/S	Informações
		ID do originador	Implementado	HTTP/S	
		Data	Implementado	HTTP/S	

APIs de gerenciamento usadas por este coletor de dados:

API	Protocolo utilizado	Protocolo da camada de transporte utilizado	Portas de entrada usadas	Portas de saída usadas	Suporta autenticação	Requer apenas credenciais "só de leitura"	Suporta criptografia	Firewall amigável (portas estáticas)
API REST do Red Hat RHEV	HTTPS	HTTPS	443		verdadeiro	verdadeiro	verdadeiro	verdadeiro

Rubrik Storage

Modelos e versões suportados por este coletor de dados:

Versões de API	Versões de firmware
v5.3	5,3.3-p1-15949 8,0.3-p3-13584 7,0.2-p4-15876 7,0.3-p1-19391 6,0.3-p2-22743

Produtos suportados por este coletor de dados:

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
fundação					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/atributo	Estado	Protocolo utilizado	Informações adicionais
		Capacidade total alocada	Implementado	HTTPS	
		Tipo	Folga	HTTPS	
		Virtual	Implementado	HTTPS	Este é um dispositivo de virtualização de armazenamento ?
		Percentagem efetiva da capacidade utilizada	Implementado	HTTPS	

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
desempenho					
1180					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/Atribuição	Estado	Protocolo utilizado	Informações adicionais
		Gravação de taxa de transferência	Implementado	HTTPS	
	Disco do StoragePool	Capacidade bruta	Implementado	HTTPS	
		Capacidade total	Implementado	HTTPS	
		Capacidade utilizada	Implementado	HTTPS	
		Relação capacidade utilizada	Implementado	HTTPS	
		Capacidade de dados utilizados	Implementado	HTTPS	
		Leitura de IOPS	Implementado	HTTPS	Número de IOPS de leitura no disco
		Total de IOPS	Implementado	HTTPS	
		Gravação de IOPS	Implementado	HTTPS	
		Outra capacidade utilizada	Implementado	HTTPS	
		Capacidade utilizada do Snapshot	Implementado	HTTPS	
		Taxa de transferência de leitura	Implementado	HTTPS	
		Taxa de transferência total	Implementado	HTTPS	Taxa total média do disco (leitura e gravação em todos os discos) em MB/s.
		Gravação de taxa de transferência	Implementado	HTTPS	

APIs de gerenciamento usadas por este coletor de dados:

API	Protocolo utilizado	Protocolo da camada de transporte utilizado	Portas de entrada usadas	Portas de saída usadas	Suporta autenticação	Requer apenas credenciais "só de leitura"	Suporta criptografia	Firewall amigável (portas estáticas)
API REST do Rubrik Storage	HTTPS	HTTPS	443		verdadeiro	verdadeiro	verdadeiro	verdadeiro

Centro Virtual da NetApp HCI

Modelos e versões suportados por este coletor de dados:

Versões de API
VMware vCenter Server 6.7.0 build-8.0.1 VMware vCenter Server 21815093 build-14368073 VMware vCenter Server 7.0.3 build-19234570 VMware vCenter Server 20395099 build-20150588 VMware vCenter Server 7.0.3 build-7.0.3 VMware vCenter Server 7.0.3 build-20990077 VMware vCenter Server 7.0.3 build-21477706 VMware vCenter Server 7.0.3 build-21784236 VMware vCenter Server 10244857 build-6.7.0

Produtos suportados por este coletor de dados:

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
fundação					
1184					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Nome do nó	Implementado	Serviços da Web	
		OID Característica/Atributo	Estado	Serviços da Web Protocolo Utilizado	Informações adicionais
		Folga			
	Informações	Descrição da API	Implementado	Serviços da Web	
		Nome da API	Implementado	Serviços da Web	
		Versão da API	Implementado	Serviços da Web	
		Nome da API do cliente	Implementado	Serviços da Web	
		Versão da API do cliente	Implementado	Serviços da Web	
		Nome da fonte de dados	Implementado	Serviços da Web	Informações
		Data	Implementado	Serviços da Web	
		ID do originador	Implementado	Serviços da Web	

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
desempenho					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/Atributo	Estado	Protocolo da Web utilizado	Informações adicionais
		Taxa de transferência total	Implementado	Serviços da Web	Taxa de transferência IP total
		Utilização total da memória	Implementado	Serviços da Web	
		swapRate.inRate	Implementado	Serviços da Web	
		Taxa de swap	Implementado	Serviços da Web	
		Taxa de troca total	Implementado	Serviços da Web	
		Programar tempo de espera	Implementado	Serviços da Web	A aguardar o horário programado em porcentagem

APIs de gerenciamento usadas por este coletor de dados:

API	Protocolo utilizado	Protocolo da camada de transporte utilizado	Portas de entrada usadas	Portas de saída usadas	Suporta autenticação	Requer apenas credenciais "só de leitura"	Suporta criptografia	Firewall amigável (portas estáticas)
API REST do VMware	Serviços da Web	HTTP/HTTPS	80/443		verdadeiro	verdadeiro	verdadeiro	verdadeiro

VMware Cloud na AWS

Modelos e versões suportados por este coletor de dados:

Versões da API:

- VMware vCenter Server 7.0.3 build-20532039
- VMware vCenter Server 7.0.3 build-20870699
- VMware vCenter Server 8.0.0 build-21709157

Produtos suportados por este coletor de dados:

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
fundação					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

	Disk	OID do VirtualMachine	Implementado	Serviços da Web	
Produto	Categoria	Característica/Atividade	Estado	Protocolo da Web utilizado	Informações adicionais
	Host	OID	Implementado	Serviços da Web	
		Nome	Implementado	Serviços da Web	
		IPS	Implementado	Serviços da Web	
		Domínio anfitrião	Implementado	Serviços da Web	
		Tipo de plataforma	Implementado	Serviços da Web	
		Memória instalada do host	Implementado	Serviços da Web	
		Fabricante	Implementado	Serviços da Web	
		Modelo anfitrião	Implementado	Serviços da Web	
		Contagem de CPU de host	Implementado	Serviços da Web	
		Velocidade da CPU do host	Implementado	Serviços da Web	
		Contagem de NIC	Implementado	Serviços da Web	
		Velocidade da NIC	Implementado	Serviços da Web	
	Informações	Nome da fonte de dados	Implementado	Serviços da Web	Informações
		ID do originador	Implementado	Serviços da Web	
		Data	Implementado	Serviços da Web	
		Nome da API	Implementado	Serviços da Web	
		Versão da API	Implementado	Serviços da Web	
		Descrição da API	Implementado	Serviços da Web	
		Nome da API do cliente	Implementado	Serviços da Web	
		Versão da API do cliente	Implementado	Serviços da Web	

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
desempenho					
1196					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/Atributo	Estado	Protocolo utilizado	Informações adicionais
		Gravação da taxa de	Implementado	Serviços da Web	
		Utilização total da CPU	Implementado	Serviços da Web	
		Programar tempo de espera	Implementado	Serviços da Web	A aguardar o horário programado em percentagem
		Disklops.Total	Implementado	Serviços da Web	
		Taxa de troca total	Implementado	Serviços da Web	
		Taxa de transferência de leitura	Implementado	Serviços da Web	leitura da taxa de transferência total do disco

APIs de gerenciamento usadas por este coletor de dados:

API	Protocolo utilizado	Protocolo da camada de transporte utilizado	Portas de entrada usadas	Portas de saída usadas	Suporta autenticação	Requer apenas credenciais "só de leitura"	Suporta criptografia	Firewall amigável (portas estáticas)
API REST do VMware	Serviços da Web	HTTP/HTTPS	80/443		verdadeiro	verdadeiro	verdadeiro	verdadeiro

VMware vSphere (Web Services)

Modelos e versões suportados por este coletor de dados:

Versões da API:

- VMware ESXi 6.0.0 build-10719132
- VMware ESXi 6.0.0 build-2494585
- VMware ESXi 6.0.0 build-5572656
- VMware ESXi 6.0.0 build-9313334
- VMware ESXi 6.5.0 build-14990892
- VMware ESXi 6.5.0 build-5969303
- VMware ESXi 7.0.0 build-15843807
- VMware ESXi 7.0.3 build-20036589
- VMware ESXi 7.0.3 build-20328353
- VMware ESXi 7.0.3 build-20842708
- VMware vCenter Server 5.0.0 build-3073236

- VMware vCenter Server 5.0.0 build-455964
- VMware vCenter Server 5.0.0 build-623373
- VMware vCenter Server 5.1.0 build-3814779
- VMware vCenter Server 5.5.0 build-1750787
- VMware vCenter Server 5.5.0 build-2442329
- VMware vCenter Server 5.5.0 build-3000241
- VMware vCenter Server 5.5.0 build-3252642
- VMware vCenter Server 5.5.0 build-3721164
- VMware vCenter Server 5.5.0 build-4180647
- 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-3634794
- VMware vCenter Server 6.0.0 build-5960847
- VMware vCenter Server 6.0.0 build-7924803
- VMware vCenter Server 6.0.0 build-8803875
- VMware vCenter Server 6.0.0 build-9313458
- VMware vCenter Server 6.5.0 build-10964411
- VMware vCenter Server 6.5.0 build-15679215
- VMware vCenter Server 6.5.0 build-17590285
- 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-19261680
- VMware vCenter Server 6.5.0 build-20510539
- VMware vCenter Server 6.5.0 build-7119157
- VMware vCenter Server 6.7.0 build-10244857
- VMware vCenter Server 6.7.0 build-11727113
- VMware vCenter Server 6.7.0 build-13007421
- VMware vCenter Server 6.7.0 build-13639324
- VMware vCenter Server 6.7.0 build-14368073
- VMware vCenter Server 6.7.0 build-15129973
- VMware vCenter Server 6.7.0 build-15679289
- VMware vCenter Server 6.7.0 build-17137327

- 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-19832247
- 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-8170161
- VMware vCenter Server 6.7.0 build-9433931
- VMware vCenter Server 7.0.0 build-16620013
- VMware vCenter Server 7.0.0 build-16749670
- VMware vCenter Server 7.0.1 build-17491160
- VMware vCenter Server 7.0.2 build-17694817
- 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 7.0.3 build-18700403
- 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-20051473
- 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 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

Produtos suportados por este coletor de dados:

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
fundação					
1204					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Nome do nó	Implementado	Serviços da Web	
		OID Característica/Atributo	Estado Folga	Serviços da Web Protocolo Utilizado	Informações adicionais
Informações		Descrição da API	Implementado	Serviços da Web	
		Nome da API	Implementado	Serviços da Web	
		Versão da API	Implementado	Serviços da Web	
		Nome da API do cliente	Implementado	Serviços da Web	
		Versão da API do cliente	Implementado	Serviços da Web	
		Nome da fonte de dados	Implementado	Serviços da Web	Informações
		Data	Implementado	Serviços da Web	
		ID do originador	Implementado	Serviços da Web	

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
desempenho					

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/A tributo	Estado	Protocolo utilizado	Informações adicionais
----------------	------------------	-------------------------------------	---------------	--------------------------------	-----------------------------------

Produto	Categoria	Característica/Atributo	Estado	Protocolo utilizado	Informações adicionais
		Gravação da taxa de	Implementado	Serviços da Web	
		Taxa de transferência IP lida	Implementado	Serviços da Web	
		Taxa de transferência total	Implementado	Serviços da Web	Taxa de transferência IP total
		IpThroughput.wri te	Implementado	Serviços da Web	
		Utilização total da memória	Implementado	Serviços da Web	
		swapRate.inRate	Implementado	Serviços da Web	
		Taxa de swap	Implementado	Serviços da Web	
		Taxa de troca total	Implementado	Serviços da Web	
		Programar tempo de espera	Implementado	Serviços da Web	A aguardar o horário programado em percentagem

APIs de gerenciamento usadas por este coletor de dados:


API	Protocolo utilizado	Protocolo da camada de transporte utilizado	Portas de entrada usadas	Portas de saída usadas	Suporta autenticação	Requer apenas credenciais "só de leitura"	Suporta criptografia	Firewall amigável (portas estáticas)
API REST do VMware	Serviços da Web	HTTP/HTTPS	80/443		verdadeiro	verdadeiro	verdadeiro	verdadeiro

Referência e suporte

Solicitação de suporte

Você pode acessar as opções de suporte no Data Infrastructure Insights clicando em **Ajuda > suporte**. As opções de suporte disponíveis dependem do Data Infrastructure Insights Edition.

Cloud Insights Support NetApp Serial Number: 123456789011234567890 AWS Customer ID: AbCdEfGhI12345678990zyxWVU Support activation is required to enable support with NetApp through web ticket or phone. Activate Support at register.netapp.com . <input checked="" type="checkbox"/> Check this box to allow NetApp access to your instance of Cloud Insights.		Contact Us Need help with Cloud Insights? Technical Support: Open a Support Ticket Phone (P1) Chat Sales: Have questions regarding your subscription? Contact Sales .	
Knowledge Base Search through the Cloud Insights Knowledge Base to find helpful articles.	Documentation Center Visit the Cloud Insights Documentation Center to find step by step instructions to help you get the most out of Cloud Insights.	Communities Join the Cloud Insights Community to follow ongoing discussions or create a new one.	Feedback We value your input. Your feedback helps us improve Cloud Insights.
Learning Center Cloud Insights Course List: <ul style="list-style-type: none">Hybrid Cloud Resource ManagementCloud Insights FundamentalsCloud Resource ManagementCloud Secure		Cloud Education All-Access Pass: Visit and subscribe the Cloud Education All-Access Pass to get unlimited access to our best cloud learning resources.	Course Catalog: Browse the Learning Services Product Catalog to find all the courses that are relevant to you.
Proxy Settings Need to setup proxy exceptions? Click here to learn more.			



Ativação do direito de suporte

O Data Infrastructure Insights oferece suporte a autoatendimento e por e-mail quando executado no modo de avaliação. Depois de se inscrever no serviço, é altamente recomendável que você ative o direito de suporte. A ativação do direito de suporte permite-lhe aceder ao suporte técnico através do chat online, do sistema de Bilheteira na Web e do telefone. O modo de suporte padrão é self-service até que o Registro seja concluído. [detalhes](#) Veja abaixo.

Durante o processo de assinatura inicial, sua instância do Data Infrastructure Insights gerará um número de série NetApp de 20 dígitos começando com "950". Este número de série do NetApp representa a assinatura do Insights de infraestrutura de dados associada à sua conta. Você deve Registrar o número de série do NetApp para ativar o direito de suporte. Oferecemos duas opções para Registro de suporte:

1. Usuário com conta SSO pré-existente do site de suporte da NetApp (NSS) (por exemplo, cliente atual da NetApp)

2. Novo cliente da NetApp sem conta SSO pré-existente do site de suporte da NetApp (NSS)

Opção 1: Etapas para um usuário com uma conta SSO pré-existente do site de suporte da NetApp (NSS)

Passos

1. Navegue até o site de Registro do NetApp <https://register.netapp.com>
2. Selecione "Eu já estou registrado como Cliente NetApp" e escolha *Insights de infraestrutura de dados* como linha de Produtos. Selecione seu provedor de faturamento (NetApp ou AWS) e forneça seu número de série e seu nome de assinatura do NetApp ou ID do cliente da AWS consultando o menu **Ajuda > suporte** na interface de usuário do Insights de infraestrutura de dados:

Cloud Insights Support

NetApp Serial Number: 95011122233344455512 **NetApp Subscription Name:** A-000012345

Support activation is required to enable support with NetApp through chat, ticket or phone. Activate Support at register.netapp.com.

Check this box to allow NetApp access to your instance of Cloud Insights.

3. Preencha o formulário de Registro de cliente existente e clique em **Enviar**.

Existing Customer Registration

The fields marked with * are mandatory

First Name*	<input type="text" value="Test"/>
Last Name*	<input type="text" value="Cloud2"/>
Company*	<input type="text" value="NetApp Inc. (VSA Only)"/>
Email Address*	<input type="text" value="ng-cloudvol-csd1@netapp.com"/>
Product Line*	<input type="text" value="Cloud Insights"/>
Billing Provider*	<input type="text" value="NetApp"/>
Cloud Insights Serial #*	<input type="text" value="e.g. 95012235021303893918"/>
NetApp Subscription Name*	<input type="text" value="e.g. A-S0000100"/>

[Add another Serial #](#)

4. Se não ocorrerem erros, o usuário será direcionado para uma página "Registro enviado com sucesso". O endereço de e-mail associado ao nome de usuário SSO do NSS usado para Registro receberá um e-mail dentro de alguns minutos informando "seu produto agora está qualificado para suporte".
5. Este é um Registro único para o número de série do Data Infrastructure Insights NetApp.

Opção 2: Etapas para um novo cliente da NetApp sem conta SSO pré-existente do site de suporte da NetApp (NSS)

Passos


1. Navegue até o site de Registro do NetApp <https://register.netapp.com>
2. Selecione "Eu não sou um Cliente NetApp registrado" e preencha as informações necessárias no formulário de exemplo abaixo:

New Customer Registration

IMPORTANT: After submitting, a confirmation email will be sent to the email address filled-in the form. Please click the validation link in that email to complete the registration.

The fields marked with * are mandatory

First Name*	<input type="text"/>
Last Name*	<input type="text"/>
Company*	<input type="text"/>
Email Address*	<input type="text"/>
Office Phone*	<input type="text"/>
Alternate Phone	<input type="text"/>
Address Line 1*	<input type="text"/>
Address Line 2	<input type="text"/>
Postal Code / City*	<input type="text"/>
State/Province / Country*	<input type="text"/> - Select - <input type="button" value="v"/>
NetApp Reference SN	<input type="text"/>
	<small>If you currently own a NetApp product, please provide the Serial Number for that product here in order to speed-up the validation process</small>
Product Line*	Cloud Insights <input type="button" value="v"/>
Billing Provider *	NetApp <input type="button" value="v"/>
Cloud Insights Serial # * <input type="button" value="i"/>	<input type="text" value="e.g. 95012235021303893918"/>
NetApp Subscription Name * <input type="button" value="i"/>	<input type="text" value="e.g. A-S0000100"/>
	Add another Serial #

Security check:
Enter the characters shown in the image to verify your 

1. Selecione *Data Infrastructure Insights* como linha de Produtos. Selecione seu provedor de faturamento (NetApp ou AWS) e forneça seu número de série e seu nome de assinatura do NetApp ou ID do cliente da AWS consultando o menu **Ajuda > suporte** na interface de usuário do Insights de infraestrutura de dados:

Cloud Insights Support

NetApp Serial Number:
95011122233344455512

NetApp Subscription Name:
A-000012345

Support activation is required to enable support with NetApp through chat, ticket or phone. Activate Support at register.netapp.com.

Check this box to allow NetApp access to your instance of Cloud Insights.

2. Se não ocorrerem erros, o usuário será direcionado para uma página "Registro enviado com sucesso". O endereço de e-mail associado ao nome de usuário SSO do NSS usado para Registro receberá um e-mail dentro de algumas horas informando "seu produto agora está qualificado para suporte".
3. Como um novo cliente da NetApp, você também precisará criar uma conta de usuário do site de suporte da NetApp (NSS) para futuros Registros e acesso ao portal de suporte para bate-papo de suporte técnico e tíquetes na Web. Este link está localizado em <https://mysupport.netapp.com/eservice/public/now.do>. Você pode fornecer seu número de série recém-registrado Data Infrastructure Insights para agilizar o processo.
4. Este é um Registro único para o número de série do Data Infrastructure Insights NetApp.

Obtenção de informações de suporte

O NetApp fornece suporte para Insights de infraestrutura de dados de várias maneiras. Amplas opções gratuitas de suporte autônomo estão disponíveis 24 horas por dia, 7 dias por semana, como artigos da base de conhecimento (KB) ou da comunidade NetApp. Para os usuários que estão inscritos* no Data Infrastructure Insights, o suporte técnico está disponível por telefone ou na web ticketing. Uma conta SSO do site de suporte da NetApp (NSS) é necessária para o ticket da Web juntamente com o gerenciamento de casos.

*O suporte está disponível na Edição básica, desde que todos os seus sistemas de armazenamento NetApp sejam cobertos pelo menos no nível de suporte Premium.

Muitas ofertas do NetApp incluem o Data Infrastructure Insights Basic Edition como parte do pacote. Se pretender atualizar para a Premium Edition, contacte o seu representante de vendas.

Suporte self-service:

Estas opções de suporte estão disponíveis no modo de avaliação e estão disponíveis gratuitamente 24x7:

- <https://kb.NetApp.com/Special:Pesquisa> na nuvem[base de conhecimento]

Clique nos links nesta seção leva você para a base de conhecimento da NetApp, onde você pode pesquisar por artigos relevantes, como fazer e muito mais.

- **"Documentação"**

Clicar no link Documentação leva você a este centro de documentação.

- **"Comunidade"**

Clicar no link da comunidade leva você à comunidade de insights da infraestrutura de dados da NetApp,

onde você pode se conectar com colegas e especialistas.

Há também um link para [xref:./"Feedback"](#) nos ajudar a melhorar os insights da infraestrutura de dados.

Suporte por assinatura

Além das opções de suporte autônomo acima, se você tiver uma assinatura do Insights de infraestrutura de dados ou suporte pago para produtos ou serviços monitorados da NetApp, poderá trabalhar com um engenheiro de suporte da NetApp para resolver seu problema.



Você deve se Registrar para [ative o suporte](#) obter os produtos de nuvem da NetApp. Para se Registrar, vá para NetApp ["Registro de suporte de serviços de dados em nuvem"](#) .

É altamente recomendável que você marque a caixa para permitir que um engenheiro de suporte da NetApp acesse seu locatário do Insights de infraestrutura de dados durante sua sessão de suporte. Isso permitirá que o engenheiro solucione o problema e o ajudará a resolvê-lo rapidamente. Quando o problema for resolvido ou a sessão de suporte tiver terminado, pode desmarcar a caixa.

Você pode solicitar suporte por qualquer um dos seguintes métodos. Você precisa ter uma assinatura ativa do Data Infrastructure Insights para usar essas opções de suporte:

- **"Telefone"**
- **"Ticket de suporte"**
- **Chat** - você estará conectado com a equipe de suporte da NetApp para assistência (somente dias úteis). O bate-papo está disponível na opção de menu **Ajuda > Chat ao vivo**, no canto superior direito de qualquer tela Data Infrastructure Insights.

Você também pode solicitar suporte de vendas clicando no **"Contato de vendas"** link.

O número de série do Data Infrastructure Insights fica visível no serviço no menu **Ajuda > suporte**. Se você tiver problemas ao acessar o serviço e tiver registrado um número de série no NetApp anteriormente, também poderá visualizar sua lista de números de série do Insights de infraestrutura de dados no site de suporte da NetApp da seguinte forma:

- Faça login no [mysupport.NetApp.com](https://mysupport.netapp.com)
- Na guia **Produtos > Meus produtos**, use a família de produtos "SaaS Data Infrastructure Insights" para localizar todos os seus números de série registrados:

View Installed Systems

Selection Criteria

- Select: Then, enter Value:
- Enter the entire value, or use asterisk (*) for wildcard searches. (Wildcard search does not apply to Serial Numbers)
Wildcard searches may take some time.
Enter the Cluster Serial Number value without dashes.

- OR -

- Search Type*: Product Family (optional):
- City (optional): State/Province (optional):
- Postal Code (optional): Country (optional):

Details

If you see any discrepancies or errors in the information shown below, please submit [Feedback](#) and be sure to include the serial nu

Matriz de suporte do Data Infrastructure Insights Data Collector

Você pode exibir ou baixar informações e detalhes sobre coletores de dados suportados no "[Data Infrastructure Insights Data Collector Support Matrix](#), função "externo".

Centro de Aprendizagem

Independentemente da sua subscrição, **Ajuda > suporte** tem ligações para várias ofertas de cursos da Universidade da NetApp para o ajudar a tirar o máximo partido das informações sobre a infraestrutura de dados. Veja-os!

Referência do coletor de dados - infraestrutura

Referência específica do fornecedor

Os tópicos nesta seção fornecem informações de referência específicas do fornecedor. Na maioria dos casos, configurar um coletor de dados é simples. Em alguns casos, você pode precisar de informações ou comandos adicionais para configurar corretamente o coletor de dados.

Clique em um **vendor** no menu à esquerda para ver as informações de seus coletores de dados.

Configurando o coletor de dados do Amazon EC2

O Data Infrastructure Insights usa o coletor de dados do Amazon EC2 para adquirir dados de inventário e desempenho de instâncias do EC2.

Requisitos

Para coletar dados de dispositivos Amazon EC2, você deve ter as seguintes informações:

- Você deve ter um dos seguintes:

- A função **IAM** da sua conta na nuvem do Amazon EC2, se estiver usando a Autenticação de função do IAM. A função IAM só se aplica se a sua unidade de aquisição estiver instalada em uma instância da AWS.
- A ID **IAM Access Key** e a chave de acesso secreta para sua conta na nuvem do Amazon EC2, se estiver usando a autenticação IAM Access Key.
- Tem de ter o privilégio "List Organization" (organização de lista)
- Porta 443 HTTPS
- As instâncias EC2 podem ser reportadas como uma máquina virtual ou (menos naturalmente) um host. Os volumes do EBS podem ser reportados como um VirtualDisk usado pela VM, bem como um datastore que fornece a capacidade para o VirtualDisk.

As chaves de acesso consistem em uma ID de chave de acesso (por exemplo, AKIAIOSFODNN7EXAMPLE) e uma chave de acesso secreta (por exemplo, wJalrXUtnFEMI/K7MDENG/bPxrRfiCYEXAMPLEKEY). Use as chaves de acesso para assinar solicitações programáticas que você faz para o EC2 se você usar as operações de API de SDKs, REST ou Query do Amazon EC2. Essas chaves são fornecidas com seu contrato da Amazon.

Configuração

Insira os dados nos campos do coletor de dados de acordo com a tabela abaixo:

Campo	Descrição
Região da AWS	Escolha a região da AWS
Função IAM	Para uso somente quando adquirido em uma AU na AWS. Consulte abaixo para obter mais informações Função IAM sobre .
ID da chave de acesso do AWS IAM	Insira o ID da chave de acesso do AWS IAM. Necessário se você não usar a função IAM.
Chave de acesso secreta do AWS IAM	Insira a chave de acesso secreta do AWS IAM. Necessário se você não usar a função IAM.
Eu entendo que a AWS me cobra por solicitações de API	Verifique isso para verificar se a AWS cobra por solicitações de API feitas pela sondagem Data Infrastructure Insights.

Configuração avançada

Campo	Descrição
Incluir Regiões extra	Especifique regiões adicionais a serem incluídas na sondagem.
Função de conta cruzada	Função para acessar recursos em diferentes contas da AWS.
Intervalo de enquete de inventário (min)	A predefinição é 60
Escolha 'Excluir' ou 'incluir' para aplicar ao filtro de VMs por Tags	Especifique se deve incluir ou excluir VM por Tags ao coletar dados. Se a opção "incluir" estiver selecionada, o campo chave da etiqueta não pode estar vazio.

Campo	Descrição
Marque chaves e valores nos quais filtrar VMs	Clique em * Tag de filtro* para escolher quais VMs (e discos associados) incluir/excluir filtrando chaves e valores que correspondem a chaves e valores de tags na VM. A chave da etiqueta é necessária, o valor da etiqueta é opcional. Quando o valor Tag está vazio, a VM é filtrada desde que corresponda à chave Tag.
Intervalo de enquete de desempenho (seg)	A predefinição é 1800
Namespace das métricas do CloudWatch Agent	Namespace em EC2/EBS a partir do qual coletar dados. Observe que se os nomes das métricas padrão nesse namespace forem alterados, o Data Infrastructure Insights pode não conseguir coletar esses dados renomeados. Recomenda-se deixar os nomes das métricas padrão.

Chave de Acesso IAM

As chaves de acesso são credenciais de longo prazo para um usuário do IAM ou para o usuário raiz da conta da AWS. As chaves de acesso são usadas para assinar solicitações programáticas para a AWS CLI ou API da AWS (diretamente ou usando o AWS SDK).

As chaves de acesso consistem em duas partes: Uma ID de chave de acesso e uma chave de acesso secreta. Quando você usa a autenticação *IAM Access Key* (em vez da autenticação *IAM role*), você deve usar o ID da chave de acesso e a chave de acesso secreta juntos para autenticação de solicitações. Para obter mais informações, consulte a documentação da Amazon no "[Teclas de acesso](#)".

Função IAM

Ao usar a autenticação *função* do IAM (em vez da autenticação da chave de acesso do IAM), você deve garantir que a função criada ou especificada tenha as permissões apropriadas necessárias para acessar seus recursos.

Por exemplo, se você criar uma função do IAM chamada *InstanceEc2ReadOnly*, deverá configurar a política para conceder permissão de acesso à lista somente leitura do EC2 a todos os recursos do EC2 para essa função do IAM. Além disso, você deve conceder acesso ao STS (Security Token Service) para que essa função possa assumir funções entre contas.

Depois de criar uma função do IAM, você pode anexá-la ao criar uma nova instância do EC2 ou qualquer instância existente do EC2.

Depois de anexar a função IAM *InstanceEc2ReadOnly* a uma instância do EC2, você poderá recuperar a credencial temporária por meio de metadados de instância pelo nome da função IAM e usá-la para acessar recursos da AWS por qualquer aplicativo executado nessa instância do EC2.

Para obter mais informações, consulte a documentação da Amazon no "[Funções do IAM](#)".

Observação: A função IAM só pode ser usada quando a Unidade de aquisição estiver sendo executada em uma instância da AWS.

Mapeamento de tags da Amazon para anotações do Data Infrastructure Insights

O coletor de dados do Amazon EC2 inclui uma opção que permite preencher anotações do Data Infrastructure

Insights com tags configuradas no EC2. As anotações devem ser nomeadas exatamente como as tags EC2. O Data Infrastructure Insights sempre preencherá anotações de tipo texto com o mesmo nome e fará uma "melhor tentativa" para preencher anotações de outros tipos (número, boolean, etc.). Se a anotação for de um tipo diferente e o coletor de dados não a preencher, pode ser necessário remover a anotação e recriá-la como um tipo de texto.

Observe que a AWS diferencia maiúsculas de minúsculas, enquanto o Data Infrastructure Insights diferencia maiúsculas de minúsculas. Então, se você criar uma anotação chamada "PROPRIETÁRIO" no Data Infrastructure Insights e tags chamadas "PROPRIETÁRIO", "proprietário" e "proprietário" em EC2, todas as EC2 variações de "proprietário" serão mapeadas para a anotação "PROPRIETÁRIO" do Cloud Insight.

Incluir Regiões extra

Na seção AWS Data Collector **Configuração avançada**, você pode definir o campo **incluir regiões extras** para incluir regiões adicionais, separadas por vírgula ou ponto e vírgula. Por padrão, esse campo é definido como **US-***, que é coletado em todas as regiões da AWS dos EUA. Para coletar em *todas* regiões, defina este campo como ***.***. Se o campo **incluir regiões extras** estiver vazio, o coletor de dados coletará os ativos especificados no campo **região AWS** conforme especificado na seção **Configuração**.

Coleta de contas AWS Child

O Data Infrastructure Insights dá suporte à coleta de contas filhas para a AWS em um único coletor de dados da AWS. A configuração para essa coleção é executada no ambiente AWS:

- Você deve configurar cada conta filho para ter uma função da AWS que permita que o ID da conta principal acesse os detalhes do EC2 da conta crianças.
- Cada conta filho deve ter o nome da função configurado como a mesma cadeia de caracteres.
- Insira esta cadeia de caracteres de nome de função na seção Data Infrastructure Insights AWS Data Collector **Configuração avançada**, no campo **função de conta cruzada**.
- A conta em que o coletor está instalado precisa ter *delegar acesso administrador* Privileges. Consulte "[Documentação do AWS](#)" para obter mais informações.

Prática recomendada: É altamente recomendável atribuir a política predefinida da AWS *AmazonEC2ReadOnlyAccess* à conta principal do EC2. Além disso, o usuário configurado na fonte de dados deve ter pelo menos a política predefinida *AWSOrganizationsReadOnlyAccess* atribuída, a fim de consultar a AWS.

Consulte o seguinte para obter informações sobre como configurar seu ambiente para permitir que o Data Infrastructure Insights colete de contas filhas da AWS:

["Tutorial: Delegar acesso em contas da AWS usando funções do IAM"](#)

["Configuração da AWS: Fornecendo acesso a um usuário do IAM em outra conta da AWS que você possui"](#)

["Criando uma função para delegar permissões a um usuário do IAM"](#)

Solução de problemas

Informações adicionais sobre este Coletor de dados podem ser encontradas "[Suporte](#)" na página ou no "[Matriz de suporte do Data Collector](#)".

Coletor de dados do Amazon FSX para NetApp ONTAP

Esse coletor de dados adquire dados de inventário e desempenho do Amazon FSX for NetApp ONTAP. Esse coletor de dados será disponibilizado de forma incremental em todas as regiões de serviço Data Infrastructure Insights. Entre em Contato com seu representante de vendas se você não vir o ícone deste coletor no ambiente Data Infrastructure Insights.



Esse coletor de Insights de infraestrutura de dados requer um usuário ONTAP com uma função *filesystem-scoped*. Consulte a documentação da AWS "[Papéis e regras](#)" para obter as opções disponíveis. Neste momento, a AWS suporta apenas um tipo de função de usuário com escopo de sistema de arquivos, que é *fsxadmin*. Esta é a função apropriada a ser usada para o coletor Data Infrastructure Insights. O usuário também deve ter todas as três aplicações atribuídas a ele: HTTP, ontapi, ssh.

Terminologia

O Insights de infraestrutura de dados adquire dados de inventário e desempenho do coletor de dados do FSX-NetApp. Para cada tipo de ativo adquirido, a terminologia mais comum usada para o ativo é mostrada. Ao visualizar ou solucionar problemas desse coletor de dados, tenha em mente a seguinte terminologia:

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
Cluster	Armazenamento
LUN	Volume
Volume	Volume interno

Terminologia do FSX-NetApp

Os termos a seguir se aplicam a objetos ou referências que você pode encontrar nas Landing pages de ativos de armazenamento do FSX-NetApp. Muitos desses termos também se aplicam a outros coletores de dados.

Armazenamento

- Modelo – Uma lista delimitada por vírgulas dos nomes de modelo únicos e discretos dentro deste cluster.
- Fornecedor – AWS
- Número de série – o número de série da matriz.
- IP – geralmente serão os IP (s) ou nome de host (s) conforme configurado na fonte de dados.
- Capacidade bruta – soma de base 2 de todo o armazenamento SSD atribuído ao sistema de arquivos FSX.
- Latência – uma representação do que o host enfrenta cargas de trabalho, tanto na leitura quanto na gravação. Idealmente, o Data Infrastructure Insights está fornecendo esse valor diretamente, mas isso geralmente não é o caso. Em vez do array que oferece isso, o Data Infrastructure Insights geralmente está executando um cálculo ponderado por IOPs derivado das estatísticas individuais de volumes internos.
- Taxa de transferência – agregada a partir de volumes internos. Gerenciamento – isso pode conter um hiperlink para a interface de gerenciamento do dispositivo. Criado programaticamente pela fonte de dados Data Infrastructure Insights como parte dos relatórios de inventário.

Pool de storage

- Armazenamento – em que storage esse pool vive. Obrigatório.
- Tipo – um valor descritivo de uma lista de uma lista enumerada de possibilidades. Mais comumente será "agregado" ou "RAID Group".
- Capacidade – os valores aqui são a capacidade lógica usada, utilizável e a capacidade total lógica, e a porcentagem usada entre eles.
- IOPS – a soma de IOPs de todos os volumes alocados nesse pool de armazenamento.
- Taxa de transferência – a taxa de transferência soma de todos os volumes alocados neste pool de armazenamento.

Requisitos

A seguir estão os requisitos para configurar e usar este coletor de dados:

- Você deve ter acesso a uma conta com a função "fsxadmin", com três aplicativos atribuídos a ela - ssh, ontapi, http
- Os detalhes da conta incluem nome de usuário e senha.
- Requisitos do porto: 443

Configuração

Campo	Descrição
IP de gerenciamento de NetApp	Endereço IP ou nome de domínio totalmente qualificado do cluster NetApp
Nome de utilizador	Nome de usuário para cluster NetApp
Palavra-passe	Palavra-passe para cluster NetApp

Métricas avançadas

Esse coletor de dados coleta as seguintes métricas avançadas do armazenamento FSX for NetApp ONTAP:

- fpolicy
- nfsv3
- nfsv3:nó
- nfsv4
- nfsv4_1
- nfsv4_1:nó
- nfsv4:nó
- policy_group
- qtree
- volume
- workload_volume

Observe que os comandos da CLI e API do FSX recuperam alguns valores de capacidade que o Data

Infrastructure Insights ZAPI não coleta, portanto, certos valores de capacidade (como aqueles para pools de armazenamento) podem ser diferentes no Data Infrastructure Insights do que no FSX em si.

Solução de problemas

Algumas coisas para tentar se você encontrar problemas com este coletor de dados:

Inventário

Problema:	Tente isto:
Receber 401 resposta HTTP ou 13003 código de erro ZAPI e ZAPI retorna "insuficiente Privileges" ou "não autorizado para este comando"	Verifique o nome de usuário e a senha e o Privileges/permissões do usuário.
ZAPI retorna "a função de cluster não é cluster_mgmt LIF"	A UA precisa falar com o IP de gerenciamento de cluster. Verifique o IP e mude para um IP diferente, se necessário
O comando ZAPI falha após a tentativa	AAU tem problema de comunicação com o cluster. Verifique a rede, o número da porta e o endereço IP. O usuário também deve tentar executar um comando da linha de comando da máquina AU.
Falha ao conectar-se ao ZAPI via HTTP	Verifique se a porta ZAPI aceita texto simples. Se AU tentar enviar texto simples para um soquete SSL, a comunicação falha.
A comunicação falha com SSLException	Au está tentando enviar SSL para uma porta de texto simples em um arquivador. Verifique se a porta ZAPI aceita SSL ou se usa uma porta diferente.
Erro de conexão adicional: A resposta ZAPI tem o código de erro 13001, "banco de dados não está aberto" o código de erro ZAPI é 60 e a resposta contém "API não terminou no tempo" resposta ZAPI contém "inicializar_sessão() ambiente NULL retornado o código de erro ZAPI é 14007 e a resposta contém "nó não está saudável"	Verifique a rede, o número da porta e o endereço IP. O usuário também deve tentar executar um comando da linha de comando da máquina AU.

Informações adicionais podem ser encontradas na ["Suporte"](#) página ou no ["Matriz de suporte do Data Collector"](#).

Configurando o coletor de dados de computação do Azure

O Data Infrastructure Insights usa o coletor de dados de computação do Azure para adquirir dados de inventário e desempenho de instâncias de computação do Azure.

Requisitos

Você precisa das seguintes informações para configurar este coletor de dados.

- Requisito de porta: 443 HTTPS
- URI de redirecionamento do Azure OAuth 2,0 (login.microsoftonline.com)
- IP REST do Gerenciamento do Azure (management.azure.com)

- IP do Azure Resource Manager (management.core.windows.net)
- ID da aplicação principal do serviço do Azure (Cliente) (função de leitor necessária)
- Chave de autenticação principal do serviço Azure (senha do usuário)
- Você precisa configurar uma conta do Azure para a descoberta do Data Infrastructure Insights.

Depois que a conta estiver configurada corretamente e você Registrar o aplicativo no Azure, você terá as credenciais necessárias para descobrir a instância do Azure com o Data Infrastructure Insights. O link a seguir descreve como configurar a conta para descoberta. <https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal>

Configuração

Insira os dados nos campos do coletor de dados de acordo com a tabela abaixo:

Campo	Descrição
ID da aplicação principal do serviço do Azure (Cliente) (função de leitor necessária)	ID de início de sessão no Azure. Requer acesso à função Reader.
ID de locatário do Azure	ID de locatário da Microsoft
Chave de autenticação principal do serviço Azure	Chave de autenticação de login
Eu entendo que a Microsoft me cobra por solicitações de API	Verifique isso para verificar se a Microsoft cobra solicitações de API feitas pela polling do Insight.

Configuração avançada

Campo	Descrição
Intervalo de enquete de inventário (min)	A predefinição é 60
Escolha 'Excluir' ou 'incluir' para aplicar ao filtro de VMs por Tags	Especifique se deve incluir ou excluir VM por Tags ao coletar dados. Se a opção "incluir" estiver selecionada, o campo chave da etiqueta não pode estar vazio.
Marque chaves e valores nos quais filtrar VMs	Clique em * Tag de filtro* para escolher quais VMs (e discos associados) incluir/excluir filtrando chaves e valores que correspondem a chaves e valores de tags na VM. A chave da etiqueta é necessária, o valor da etiqueta é opcional. Quando o valor Tag está vazio, a VM é filtrada desde que corresponda à chave Tag.
Intervalo de enquete de desempenho (seg)	A predefinição é 300

Solução de problemas

Informações adicionais sobre este Coletor de dados podem ser encontradas "[Suporte](#)" na página ou no "[Matriz de suporte do Data Collector](#)".

Broadcom

Coletor de dados do consultor de rede Brocade

O Insights de infraestrutura de dados usa o coletor de dados do consultor de rede da Brocade para adquirir dados de inventário e desempenho de switches Brocade.

Terminologia

Informações de infraestrutura de dados adquire as seguintes informações de inventário do coletor de dados do consultor de rede da Brocade. Para cada tipo de ativo adquirido pelo Data Infrastructure Insights, a terminologia mais comum usada para esse ativo é mostrada. Ao visualizar ou solucionar problemas desse coletor de dados, tenha em mente a seguinte terminologia:

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
Interrutor	Interrutor
Porta	Porta
Malha virtual, malha física	Malha
Comutador lógico	Comutador lógico

Nota: Estes são apenas mapeamentos de terminologia comuns e podem não representar todos os casos para este coletor de dados.

Requisitos

Para configurar este coletor de dados, são necessários os seguintes itens:

- A Unidade de aquisição do Data Infrastructure Insights initará conexões à porta TCP 443 no servidor BNA. O servidor BNA deve estar executando a versão 14.2.1 ou superior.
- Endereço IP do servidor do consultor de rede Brocade
- Nome de usuário e senha para uma conta de administrador
- Requisito de porta: HTTP/HTTPS 443

Configuração

Campo	Descrição
IP do servidor do consultor de rede Brocade	Endereço IP do servidor do Network Advisor
Nome de utilizador	Nome de utilizador do comutador
Nome de utilizador	Nome de usuário do administrador
Palavra-passe	Senha do administrador

Configuração avançada

Campo	Descrição
Tipo de ligação	HTTPS (porta padrão 443) ou HTTP (porta padrão 80)

Campo	Descrição
Substituir porta de ligação	Se estiver em branco, use a porta padrão no campo tipo de conexão; caso contrário, insira a porta de conexão a ser usada
Palavra-passe	Palavra-passe para o interruptor
Intervalo de pesquisa de inventário (min)	A predefinição é 40
Gateway de acesso de relatório	Verifique para incluir dispositivos no modo Gateway de acesso
Intervalo de enquete de desempenho (seg)	A predefinição é 1800

Solução de problemas

Algumas coisas para tentar se você encontrar problemas com este coletor de dados:

Inventário

Problema:	Tente isto:
Receba uma mensagem informando que mais de 1 nó está conectado à porta do Gateway de acesso ou que o coletor de dados não consegue detetar o dispositivo Gateway de acesso.	Verifique se o dispositivo NPV está funcionando corretamente e se todas as WWNs conectadas são esperadas. Não adquira diretamente o dispositivo NPV. Em vez disso, a aquisição do switch de malha central coletará os dados do dispositivo NPV.

Informações adicionais podem ser encontradas na ["Suporte"](#) página ou no ["Matriz de suporte do Data Collector"](#).

Coletor de dados do switch Brocade FC

O Insights de infraestrutura de dados usa a fonte de dados do switch FC Brocade (SSH) para descobrir o inventário de dispositivos de switch Brocade ou rebranded que executam o firmware do sistema operacional fatorado (FOS) 4,2 e posterior. Os dispositivos nos modos de switch FC e Gateway de acesso são suportados.

Terminologia

O Data Infrastructure Insights adquire as seguintes informações de inventário do coletor de dados do switch Brocade FC. Para cada tipo de ativo adquirido pelo Data Infrastructure Insights, a terminologia mais comum usada para esse ativo é mostrada. Ao visualizar ou solucionar problemas desse coletor de dados, tenha em mente a seguinte terminologia:

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
Interruptor	Interruptor
Porta	Porta
Malha virtual, malha física	Malha
Zona	Zona

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
Comutador lógico	Comutador lógico
Volume virtual	Volume
Zona LSAN	Zona IVR

Nota: Estes são apenas mapeamentos de terminologia comuns e podem não representar todos os casos para este coletor de dados.

Requisitos

- A Unidade de aquisição de informações de infraestrutura de dados (AU) iniciará conexões com a porta TCP 22 nos switches Brocade para coletar dados de inventário. A AU também iniciará conexões com a porta UDP 161 para coleta de dados de desempenho.
- Deve haver conectividade IP para todos os switches na malha. Se você selecionar a caixa de seleção descobrir todos os switches na malha, o Data Infrastructure Insights identificará todos os switches da malha. No entanto, ela precisará de conectividade IP com esses switches adicionais para detectá-los.
- Globalmente, a mesma conta é necessária em todos os switches da malha. Você pode usar PuTTY (emulador de terminal de código aberto) para confirmar o acesso.
- As portas 161 e 162 devem estar abertas para todos os switches na malha para polling de desempenho SNMP.
- Cadeia de Comunidade somente leitura SNMP

Configuração

Campo	Descrição
IP do switch	Endereço IP ou nome de domínio totalmente qualificado do servidor EFC
Nome de utilizador	Nome de utilizador do comutador
Palavra-passe	Palavra-passe para o interruptor
SNMP	Versão SNMP
SNMP Community String	String de comunidade SNMP somente leitura usada para acessar o switch
Nome de utilizador SNMP	Nome de utilizador SNMP
Palavra-passe SNMP	Palavra-passe SNMP

Configuração avançada

Campo	Descrição
Nome da malha	Nome do tecido a ser informado pelo coletor de dados. Deixe em branco para relatar o nome da tela como WWN.
Intervalo de enquete de inventário (min)	Intervalo entre sondagens de inventário. A predefinição é 15.

Campo	Descrição
Dispositivos excluídos	Lista separada por vírgulas de IDs de dispositivo a excluir da sondagem
Domínios Admin ativos	Selecione se estiver usando domínios Admin
Recuperar dados MPR	Selecione para adquirir dados de roteamento do roteador multiprotocolo.
Ativar trapping	Selecione para ativar a aquisição ao receber uma trap SNMP do dispositivo. Se você selecionar Ativar trapping, você também deve ativar o SNMP.
Tempo mínimo entre armadilhas (seg)	Tempo mínimo entre tentativas de aquisição desencadeadas por armadilhas. A predefinição é 10.
Descubra todos os switches na malha	Selecione para descobrir todos os switches na malha
Escolha favorecendo HBA vs. Aliases de zona	Escolha se prefere HBA ou aliases de zona
Intervalo de enquete de desempenho (seg)	Intervalo entre sondagens de desempenho. A predefinição é 300.
Protocolo Auth SNMP	Protocolo de autenticação SNMP (apenas SNMP v3)
Palavra-passe de privacidade SNMP	Palavra-passe de privacidade SNMP (apenas SNMP v3)
Geometrias SNMP	Número de tentativas de tentativa SNMP

Solução de problemas

Algumas coisas para tentar se você encontrar problemas com este coletor de dados:

Inventário

Problema:	Tente isto:
A aquisição de inventário da fonte de dados Brocade falha com o erro: <date> <time> ERROR [com.onaro.SANscreen.acquisition.framework.datasour ce.BaseDataSource] erro 2 de 2: <datasource name> [erro interno] - não é possível gerar o modelo para <IP> de dispositivo. Erro ao detetar prompt ([Nome do dispositivo <name>]: Não é possível gerar o modelo para o <IP> do dispositivo. Aviso de detecção de erro)	O problema pode ser causado quando o switch Brocade leva muito tempo para retornar com um prompt, excedendo o tempo limite padrão de 5 segundos. Nas configurações de Configuração Avançada do coletor de dados em Insights de infraestrutura de dados, tente aumentar o tempo limite de espera da faixa <i>SSH (seg)</i> para um valor mais alto.
Erro: "Dados Infrastructure Insights receberam função de chassi inválida"	Verifique se o usuário configurado nesta fonte de dados recebeu a permissão de função de chassi.
Erro: "Endereço IP do chassis incorreto"	Altere a configuração da fonte de dados para usar o endereço IP do chassis.

Problema:	Tente isto:
Receba uma mensagem informando que mais de 1 nó está conectado à porta do Gateway de acesso	Verifique se o dispositivo NPV está funcionando corretamente e se todas as WWNs conectadas são esperadas. Não adquira diretamente o dispositivo NPV. Em vez disso, a aquisição do switch de malha central coletará os dados do dispositivo NPV.
A coleção de desempenho falha com "tempo limite durante o envio de solicitação SNMP".	Dependendo das variáveis de consulta e da configuração do switch, algumas consultas podem exceder o tempo limite padrão. "Saiba mais" .

Informações adicionais podem ser encontradas na ["Suporte"](#) página ou no ["Matriz de suporte do Data Collector"](#).

Coletor de DADOS REST do Brocade FOS

O Insights de infraestrutura de dados usa o coletor REST do Brocade FOS para descobrir o inventário e o desempenho dos dispositivos de switch Brocade que executam o firmware 8,2 e posterior do FabricOS.

Observação: O nível padrão DE "usuário" DO FOS não é suficientemente poderoso para que o Data Infrastructure Insights visualize todos os aspectos lógicos de um dispositivo - precisamos de uma conta de usuário com a "função de chassi" ativada, bem como permissões em todas as estruturas virtuais configuradas em um switch.

Aqui está um exemplo de como você pode criar uma conta de usuário "menos privilégio" para uso do Data Infrastructure Insights em uma sessão SSH para um dispositivo FOS:

```
UserConfig --add NetAppCIUser -r user -l 1-128 -c user -p Qwerty!
```

Isso criará um usuário "NetAppCIUser" com uma senha de "Qwerty!". Esse usuário tem a função "usuário" (-r) em todas as 128 malhas virtuais possíveis (-l). Esse usuário também tem a função "chassis" necessária (-c) com acesso ao nível do usuário atribuído.

Por padrão, este coletor tentará descobrir todos os dispositivos FOS que fazem parte de todas as malhas das quais o switch faz parte.

Terminologia

O Insights de infraestrutura de dados adquire as seguintes informações de inventário do coletor de DADOS REST do Brocade FOS. Para cada tipo de ativo adquirido pelo Data Infrastructure Insights, a terminologia mais comum usada para esse ativo é mostrada. Ao visualizar ou solucionar problemas desse coletor de dados, tenha em mente a seguinte terminologia:

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
Interrutor	Interrutor
Porta	Porta
Malha virtual, malha física	Malha
Zona	Zona
Computador lógico	Computador lógico

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
Zona LSAN	Zona IVR

Nota: Estes são apenas mapeamentos de terminologia comuns e podem não representar todos os casos para este coletor de dados.

Requisitos

- Deve haver conectividade TCP para todos os switches na malha. Esse tipo de coletor de dados experimentará perfeitamente HTTP e HTTPS para cada dispositivo na malha. Se você selecionar a caixa de seleção *descobrir todos os switches na estrutura*, o Data Infrastructure Insights identificará todos os switches na malha; no entanto, ele precisará de conectividade TCP a esses switches adicionais para detectá-los.
- Globalmente, a mesma conta é necessária em todos os switches da malha. Pode utilizar a interface Web do dispositivo para confirmar o acesso.

Configuração

Campo	Descrição
IP do switch	Endereço IP ou nome de domínio totalmente qualificado do switch FOS
Nome de utilizador	Nome de utilizador do computador
Palavra-passe	Palavra-passe para o interruptor

Configuração avançada

Campo	Descrição
Dispositivos excluídos	Lista separada por vírgulas dos endereços do dispositivo IPv4 a excluir da sondagem.
Intervalo de enquete de inventário (min)	Intervalo entre sondagens de inventário. A predefinição é 60.
Descubra todos os switches na malha	Selecione para descobrir todos os switches na malha.
Escolha favorecendo HBA vs. Aliases de zona	Escolha se prefere HBA ou aliases de zona.
Tipo de ligação	HTTP ou HTTPS.
Observe que essa configuração somente altera o IC de protocolo que tenta usar primeiro por dispositivo - IC tentará o protocolo oposto automaticamente se o padrão falhar	Substituir a porta TCP
Especifique uma porta se não estiver usando o padrão.	Intervalo de enquete de desempenho (seg)

Solução de problemas

Algumas coisas para tentar se você encontrar problemas com este coletor de dados:

Inventário

Problema:	Tente isto:
O recurso Teste me avisa que um protocolo está inacessível	Um determinado dispositivo Brocade FOS 8,2 só vai querer falar em HTTP ou HTTPS - se um switch tiver um certificado digital instalado, o switch irá lançar erros HTTP se alguém tentar se comunicar com ele com HTTP não criptografado versus HTTPS. O recurso de teste tenta a comunicação com HTTP e HTTPS - se o Teste disser que um protocolo passa, você pode salvar o coletor com segurança e não se preocupar que o outro protocolo não foi bem-sucedido - o coletor tentará ambos os protocolos durante a coleta, e só falhará se nenhum deles funcionar.
Erro: "Dados Infrastructure Insights receberam função de chassi inválida"	Verifique se o usuário configurado nesta fonte de dados recebeu a permissão de função de chassi.
Erro: "Endereço IP do chassis incorreto"	Altere a configuração da fonte de dados para usar o endereço IP do chassis.
Inventário falha com um 403 proibido	Isso pode ser simplesmente credenciais ruins, ou pode ser indicativo de que você está tentando usar uma função insuficientemente poderosa - lembre-se de que os usuários de nível "usuário" NÃO têm o direito de "função de chassi" necessário, ou visualizar o acesso a telas virtuais não padrão.

Informações adicionais podem ser encontradas na ["Suporte"](#) página ou no ["Matriz de suporte do Data Collector"](#).

Coletor de dados dos switches Cisco MDS Fabric

O Data Infrastructure Insights usa o coletor de dados dos switches Cisco MDS Fabric para descobrir o inventário dos switches Cisco MDS Fabric e uma variedade de switches FCoE Cisco Nexus nos quais o serviço FC está ativado.

Além disso, você pode descobrir muitos modelos de dispositivos Cisco rodando no modo NPV com este coletor de dados.

Terminologia

O Data Infrastructure Insights adquire as seguintes informações de inventário do coletor de dados do switch Cisco FC. Para cada tipo de ativo adquirido pelo Data Infrastructure Insights, a terminologia mais comum usada para esse ativo é mostrada. Ao visualizar ou solucionar problemas desse coletor de dados, tenha em mente a seguinte terminologia:

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
Interrutor	Interrutor
Porta	Porta
VSAN	Malha

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
Zona	Zona
Comutador lógico	Comutador lógico
Entrada do servidor de nomes	Entrada do servidor de nomes
Zona de Roteamento Inter-VSAN (IVR)	Zona IVR

Nota: Estes são apenas mapeamentos de terminologia comuns e podem não representar todos os casos para este coletor de dados.

Requisitos

- Um endereço IP de um switch na malha ou switches individuais
- Detecção de chassis, para permitir a descoberta de malha
- Se estiver usando SNMP V2, string de comunidade somente leitura
- A porta 161 é utilizada para aceder ao dispositivo

Configuração

Campo	Descrição
IP do comutador Cisco	Endereço IP ou nome de domínio totalmente qualificado do switch
Versão SNMP	Selecione V1, V2 ou V3. V2 ou posterior é necessário para a aquisição de desempenho.
SNMP Community String	String de comunidade SNMP somente leitura usada para acessar o switch (não aplicável para SNMP v3)
Nome de utilizador	Nome de utilizador do comutador (apenas SNMP v3)
Palavra-passe	Palavra-passe utilizada para o interruptor (apenas SNMPv3)

Configuração avançada

Campo	Descrição
Intervalo de enquete de inventário (min)	Intervalo entre pesquisas de inventário (padrão de 40 minutos)
Protocolo Auth SNMP	Protocolo de autenticação SNMP (apenas SNMPv3)
Protocolo de privacidade SNMP	Protocolo de privacidade SNMP (apenas SNMPv3)
Palavra-passe de privacidade SNMP	Palavra-passe de privacidade SNMP
Geometrias SNMP	Número de tentativas de tentativa SNMP
Tempo limite SNMP (ms)	Tempo limite SNMP (padrão de 5000 ms)
Ativar trapping	Selecione para ativar o trapping. Se você ativar o trapping, você também deve ativar notificações SNMP.

Campo	Descrição
Tempo mínimo entre armadilhas (seg)	Tempo mínimo entre tentativas de aquisição acionadas por armadilhas (padrão de 10 segundos)
Descubra todos os switches de malha	Selecione para descobrir todos os switches na malha
Dispositivos excluídos	Lista separada por vírgulas de IPs de dispositivos a excluir da sondagem
Dispositivos incluídos	Lista separada por vírgulas de IPs de dispositivos a incluir na sondagem
Verifique o tipo de dispositivo	Selecione para aceitar apenas os dispositivos que se anunciam explicitamente como dispositivos Cisco
Primeiro tipo de Alias	Forneça uma primeira preferência para a resolução do alias. Escolha a partir do seguinte: Device Alais este é um nome amigável para uma porta WWN (pWWN) que pode ser usado em todos os comandos de configuração, conforme necessário. Todos os switches da família Cisco MDS 9000 suportam Serviços de Alias de dispositivos distribuídos (aliases de dispositivos). Nenhum não relate nenhum alias. Descrição da porta Uma descrição para ajudar a identificar a porta em uma lista de portas. Alias de zona (todos) Um nome amigável para uma porta que pode ser usado apenas para a configuração ativa. Este é o padrão.
Segundo tipo Alias	Forneça uma segunda preferência para a resolução do alias
Terceiro tipo de Alias	Forneça uma terceira preferência para a resolução do alias
Ative o suporte do modo Proxy SANTAP	Selecione se o switch Cisco está usando SANTAP no modo proxy. Se você estiver usando o EMC RecoverPoint, você provavelmente está usando o SANTAP.
Intervalo de enquete de desempenho (seg)	Intervalo entre sondagens de desempenho (padrão 300 segundos)

Solução de problemas

Algumas coisas para tentar se você encontrar problemas com este coletor de dados:

Inventário

Problema:	Tente isto:
Erro: Falha ao descobrir chassis - não foram detetados interruptores	<ul style="list-style-type: none"> • Faça ping no dispositivo com o IP configurado • Faça login no dispositivo usando o Gerenciador de dispositivos Cisco GUI • Faça login no dispositivo usando CLI • Tente executar o SNMP Walk

Problema:	Tente isto:
Erro: O dispositivo não é um switch Cisco MDS	<ul style="list-style-type: none"> • Certifique-se de que o IP de origem de dados configurado para o dispositivo está correto • Faça login no dispositivo usando a GUI do Gerenciador de dispositivos Cisco • Faça login no dispositivo usando a CLI
Erro: O Data Infrastructure Insights não consegue obter o WWN do switch.	Este pode não ser um switch FC ou FCoE e, como tal, pode não ser suportado. Certifique-se de que o IP/FQDN configurado na fonte de dados seja realmente um switch FC/FCoE.
Erro: Foram encontrados mais de um nós conectados à porta do switch NPV	Desativar a aquisição direta do interruptor NPV
Erro: Não foi possível ligar ao interruptor	<ul style="list-style-type: none"> • Certifique-se de que o dispositivo ESTÁ LIGADO • Verifique o endereço IP e a porta de escuta • Ping o dispositivo • Faça login no dispositivo usando a GUI do Gerenciador de dispositivos Cisco • Faça login no dispositivo usando a CLI • Executar caminhada SNMP

Desempenho

Problema:	Tente isto:
Erro: Aquisição de desempenho não suportada pelo SNMP v1	<ul style="list-style-type: none"> • Editar origem de dados e desativar o desempenho do comutador • Modificar a origem de dados e configuração do comutador para usar SNMP v2 ou superior

Informações adicionais podem ser encontradas na ["Suporte"](#) página ou no ["Matriz de suporte do Data Collector"](#).

Coletor de dados Cohesity SmartFiles

Esse coletor baseado em API REST adquirirá um cluster Cohesity, descobrindo as "visualizações" (como volumes internos do Data Infrastructure Insights), os vários nós, além de coletar métricas de performance.

Configuração

Campo	Descrição
Cohesity Cluster IP	Endereço IP do cluster Cohesity
Nome de utilizador	Nome de utilizador para o cluster Cohesity
Palavra-passe	Senha usada para o cluster Cohesity

Configuração avançada

Campo	Descrição
Porta TCP	Porta usada para comunicação TCP com o cluster Cohesity
Intervalo de enquete de inventário (min)	Intervalo entre sondagens de inventário. O padrão é 60 minutos.
Intervalo de enquete de desempenho (min)	Intervalo entre sondagens de desempenho. O padrão é 900 segundos.

Solução de problemas

Informações adicionais podem ser encontradas na ["Suporte"](#) página ou no ["Matriz de suporte do Data Collector"](#).

Dell

Coletor de dados da série XC da Dell EMC

O Data Infrastructure Insights usa esse coletor de dados para descobrir informações de inventário e desempenho para os storages de armazenamento da série XC da Dell EMC.

Configuração

Campo	Descrição
Endereço IP externo do prisma	Endereço IP do servidor XC
Nome de utilizador	Nome de usuário para o servidor XC
Palavra-passe	Senha usada para o servidor XC

Configuração avançada

Campo	Descrição
Porta TCP	Porta usada para comunicação TCP com o servidor XC
Intervalo de enquete de inventário (min)	Intervalo entre sondagens de inventário. O padrão é 60 minutos.
Intervalo de enquete de desempenho (min)	Intervalo entre sondagens de desempenho. O padrão é 300 segundos.

Solução de problemas

Informações adicionais podem ser encontradas na ["Suporte"](#) página ou no ["Matriz de suporte do Data Collector"](#).

Dell EMC

Coletor de dados DELL EMC Data Domain

Este coletor de dados reúne informações de inventário e desempenho dos sistemas de armazenamento de dados de deduplicação Dell EMC Data Domain. Para configurar esse coletor de dados, há instruções de configuração específicas e recomendações de uso que você deve seguir.

Terminologia

O Data Infrastructure Insights adquire as seguintes informações de inventário do coletor de dados do Data Domain. Para cada tipo de ativo adquirido pelo Data Infrastructure Insights, a terminologia mais comum usada para esse ativo é mostrada. Ao visualizar ou solucionar problemas desse coletor de dados, tenha em mente a seguinte terminologia:

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
Disco	Disco
Array	Armazenamento
Porta FC	Porta
Sistema de ficheiros	Volume interno
Cota	Cota
Compartilhamento NFS e CIFS	Partilha de ficheiros

Nota: Estes são apenas mapeamentos de terminologia comuns e podem não representar todos os casos para este coletor de dados.

Requisitos

Você precisa das seguintes informações para configurar este coletor de dados:

- Endereço IP do dispositivo domínio de dados
- Nome de usuário somente leitura e senha para o armazenamento do domínio de dados
- Porta SSH 22

Configuração

Campo	Descrição
Endereço IP	O endereço IP ou o nome de domínio totalmente qualificado da matriz de armazenamento Data Domain
Nome de utilizador	O nome de usuário para a matriz de armazenamento Data Domain
Palavra-passe	A palavra-passe para a matriz de armazenamento Data Domain

Configuração avançada

Campo	Descrição
Intervalo de enquete de inventário (min)	Intervalo entre sondagens de inventário. A predefinição é 20.
Porta SSH	Porta de serviço SSH

Solução de problemas

Informações adicionais sobre este Coletor de dados podem ser encontradas ["Suporte"](#) na página ou no ["Matriz de suporte do Data Collector"](#).

Configurar o coletor de dados EMC ECS

Este coletor de dados adquire dados de inventário e desempenho dos sistemas de armazenamento EMC ECS. Para a configuração, o coletor de dados requer um endereço IP ou nome de host do cluster ECS e um nome de usuário e senha.



O Dell EMC ECS é medido a uma taxa bruta de TB para Unidade gerenciada diferente. Cada 40 TB de capacidade ECS não formatada é cobrada como 1 ["Unidade gerenciada \(MU\)"](#).

Terminologia

O Data Infrastructure Insights adquire as seguintes informações de inventário do coletor de dados ECS. Para cada tipo de ativo adquirido, a terminologia mais comum usada para esse ativo é mostrada. Ao visualizar ou solucionar problemas desse coletor de dados, tenha em mente a seguinte terminologia:

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
Cluster	Armazenamento
Locatário	Pool de storage
Balde	Volume interno
Disco	Disco

Nota: Estes são apenas mapeamentos de terminologia comuns e podem não representar todos os casos para este coletor de dados.

Requisitos

- Um endereço IP ou nome de host do cluster ECS
- Um nome de utilizador e uma palavra-passe para o sistema ECS
- Porta 4443 (HTTPS). Requer conectividade de saída à porta TCP 4443 no sistema ECS.

Configuração

Campo	Descrição
Anfitrião ECS	Endereço IP ou nome de domínio totalmente qualificado do sistema ECS
Porta de host ECS	Porta utilizada para comunicação com o ECS Host

Campo	Descrição
ID de utilizador ECS	ID de utilizador para ECS
Palavra-passe	Palavra-passe utilizada para ECS

Configuração avançada

Campo	Descrição
Intervalo de enquete de inventário (min)	O padrão é 360 minutos.

Solução de problemas

Algumas coisas para tentar se você encontrar problemas com este coletor de dados:

Inventário

Problema:	Tente isto:
Erro: Falha na autenticação do utilizador.	Certifique-se de que as suas credenciais para este dispositivo estão corretas.

Desempenho

Problema:	Tente isto:
Erro: Não foram recolhidos dados suficientes.	<ul style="list-style-type: none"> • Verifique o carimbo de data/hora da coleção no arquivo de log e modifique o intervalo de polling em conformidade • aguarde mais tempo
Erro: O intervalo de polling de desempenho é muito grande.	Verifique o timestamp da coleção no arquivo de log e modifique o intervalo de polling em conformidade

Informações adicionais podem ser encontradas na ["Suporte"](#) página ou no ["Matriz de suporte do Data Collector"](#).

Coletor de dados Dell EMC PowerScale

O Data Infrastructure Insights usa o coletor de dados SSH PowerScale (anteriormente Isilon) da Dell EMC para adquirir dados de inventário e desempenho do armazenamento nas com escalabilidade horizontal do PowerScale.

Terminologia

O Data Infrastructure Insights adquire as seguintes informações de inventário desse coletor de dados. Para cada tipo de ativo adquirido pelo Data Infrastructure Insights, a terminologia mais comum usada para esse ativo é mostrada. Ao visualizar ou solucionar problemas desse coletor de dados, tenha em mente a seguinte terminologia:

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
Condução	Disco

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
Cluster	Armazenamento
Nó	Nó de storage
Sistema de ficheiros	Volume interno

Nota: Estes são apenas mapeamentos de terminologia comuns e podem não representar todos os casos para este coletor de dados.

Requisitos

Você precisa das seguintes informações para configurar este coletor de dados:

- Permissões de administrador para o armazenamento PowerScale
- Endereço IP do cluster PowerScale
- Acesso SSH à porta 22

Configuração

Campo	Descrição
Endereço IP	O endereço IP ou o nome de domínio totalmente qualificado do cluster PowerScale
Nome de utilizador	Nome de utilizador para o cluster PowerScale
Palavra-passe	Palavra-passe utilizada para o cluster PowerScale

Configuração avançada

Campo	Descrição
Intervalo de enquete de inventário (min)	Intervalo entre sondagens de inventário. A predefinição é 20.
Intervalo de enquete de desempenho (seg)	Intervalo entre sondagens de desempenho. A predefinição é 300.
Porta SSH	Porta de serviço SSH. A predefinição é 22.

Solução de problemas

Algumas coisas para tentar se você encontrar problemas com este coletor de dados:

Inventário

Problema:	Tente isto:
"Credenciais de login inválidas" com mensagens de erro "comandos não habilitados para administração baseada em funções exigem acesso de usuário raiz"	* Verifique se o usuário tem permissões para executar os seguintes comandos no dispositivo: > versão isi osrelease > isi status -q > isi status -n > isi devices -d %s > isi license * Verifique se as credenciais usadas no assistente correspondem às credenciais do dispositivo

Problema:	Tente isto:
"Erro interno" com mensagens de erro "a execução do Command <Your command> falhou com permissão: Problema de permissão de execução do comando sudo"	Verifique se o usuário tem permissões sudo para executar o seguinte comando no dispositivo

Informações adicionais podem ser encontradas na ["Suporte"](#) página ou no ["Matriz de suporte do Data Collector"](#).

Coletor de DADOS REST Dell EMC Isilon / PowerScale

O Data Infrastructure Insights usa o coletor de DADOS REST do Dell EMC Isilon / PowerScale para adquirir dados de inventário e desempenho do armazenamento Dell EMC Isilon ou PowerScale. Este coletor suporta matrizes executando OneFS 8,0.0 ou mais.

Terminologia

O Data Infrastructure Insights adquire as seguintes informações de inventário desse coletor de dados. Para cada tipo de ativo adquirido pelo Data Infrastructure Insights, a terminologia mais comum usada para esse ativo é mostrada. Ao visualizar ou solucionar problemas desse coletor de dados, tenha em mente a seguinte terminologia:

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
Condução	Disco
Cluster	Armazenamento
Nó	Nó de storage
Sistema de arquivos OneFS	Volume interno
Sistema de arquivos OneFS	Pool de storage
Qtree	Qtree

Nota: Estes são apenas mapeamentos de terminologia comuns e podem não representar todos os casos para este coletor de dados.

Requisitos

Você precisa das seguintes informações para configurar este coletor de dados:

- Uma conta de usuário e senha. Essa conta **NÃO** precisa ser admin/root, mas **VOCÊ DEVE** conceder um número substancial de Privileges somente leitura à sua conta de serviço - consulte a tabela abaixo
- Endereço IP / Nome de domínio totalmente qualificado do cluster Dell EMC Isilon / PowerScale
- Acesso HTTPS à porta 8080
- Cluster Isilon / PowerScale executando OneFS 8.0.0 ou superior

Nome do privilégio	Descrição	r (leitura) ou rw (leitura e gravação)
ISI_PRIV_LOGIN_PAPI	API da plataforma	r
ISI_PRIV_SYS_TIME	Tempo	r
ISI_PRIV_AUTH	Auth	r
ISI_PRIV_ROLE	Privilégio	r
ISI_PRIV_DEVICES	Dispositivos	r
ISI_PRIV_EVENT	Evento	r
ISI_PRIV_HDFS	HDFS	r
ISI_PRIV_NDMP	NDMP	r
ISI_PRIV_NETWORK	Rede	r
ISI_PRIV_NFS	NFS	r
ISI_PRIV_PAPI_CONFIG	Configure a API da plataforma	r
ISI_PRIV_QUOTA	Cota	r
ISI_PRIV_SMARTPOOLS	SmartPools	r
ISI_PRIV_SMB	SMB	r
ISI_PRIV_STATISTICS	Estatísticas	r
ISI_PRIV_SWIFT	Rápido	r
ISI_PRIV_JOB_ENGINE	Motor de trabalho	r

Configuração

Campo	Descrição
Endereço IP de Isilon	O endereço IP ou nome de domínio totalmente qualificado do armazenamento Isilon
Nome de utilizador	Nome de utilizador para o Isilon
Palavra-passe	Senha usada para o Isilon

Configuração avançada

Campo	Descrição
Porta HTTPS	A predefinição é 8080.
Intervalo de enquete de inventário (min)	Intervalo entre sondagens de inventário. A predefinição é 20.
Intervalo de enquete de desempenho (seg)	Intervalo entre sondagens de desempenho. A predefinição é 300.

Solução de problemas

Algumas coisas para tentar se você encontrar problemas com este coletor de dados:

Inventário

Problema:	Tente isto:
"Credenciais de login inválidas" com mensagens de erro "comandos não habilitados para administração baseada em funções exigem acesso de usuário raiz"	* Verifique se o usuário tem permissões para executar os seguintes comandos no dispositivo: > versão isi osrelease > isi status -q > isi status -n > isi devices -d %s > isi license * Verifique se as credenciais usadas no assistente correspondem às credenciais do dispositivo
"Erro interno" com mensagens de erro "a execução do Command <Your command> falhou com permissão: Problema de permissão de execução do comando sudo"	Verifique se o usuário tem permissões sudo para executar o seguinte comando no dispositivo

Informações adicionais podem ser encontradas na ["Suporte"](#) página ou no ["Matriz de suporte do Data Collector"](#).

Coletor de dados Dell EMC PowerStore

O coletor de dados EMC PowerStore reúne informações de inventário do armazenamento EMC PowerStore. Para a configuração, o coletor de dados requer o endereço IP dos processadores de armazenamento e um nome de usuário e senha somente leitura.

O coletor de dados EMC PowerStore reúne as relações de replicação de volume para volume que o PowerStore coordena em outros arrays de armazenamento. O Data Infrastructure Insights mostra um storage array para cada cluster do PowerStore e coleta dados de inventário para nós e portas de storage nesse cluster. Nenhum pool de armazenamento ou dados de volume são coletados.

Terminologia

O Data Infrastructure Insights adquire as seguintes informações de inventário desse coletor de dados. Para cada tipo de ativo adquirido pelo Data Infrastructure Insights, a terminologia mais comum usada para esse ativo é mostrada. Ao visualizar ou solucionar problemas desse coletor de dados, tenha em mente a seguinte terminologia:

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
host	host
host_volume_mapping	host_volume_mapping
Hardware (ele tem unidades sob "extra_details" objeto): Drives	Disco
Aparelho	StoragePool
Cluster	Storage array
Nó	StorageNode

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
fc_port	Porta
volume	Volume
Internalvolume	file_system (sistema_ficheiro)

Nota: Estes são apenas mapeamentos de terminologia comuns e podem não representar todos os casos para este coletor de dados.

Requisitos

As seguintes informações são necessárias para configurar este coletor de dados:

- Endereço IP ou nome de domínio totalmente qualificado do processador de armazenamento
- Nome de utilizador e palavra-passe só de leitura

Configuração

Campo	Descrição
Gateway(s) PowerStore	Endereços IP ou nomes de domínio totalmente qualificados do armazenamento PowerStore
Nome de utilizador	Nome de utilizador para PowerStore
Palavra-passe	Palavra-passe utilizada para PowerStore

Configuração avançada

Campo	Descrição
Porta HTTPS	A predefinição é 443
Intervalo de enquete de inventário (minutos)	Intervalo entre sondagens de inventário. O padrão é 60 minutos.

A coleção de desempenho PowerStore do Cloud Insight utiliza os dados de origem de granularidade de 5 minutos do PowerStore. Como tal, o Data Infrastructure Insights pesquisa esses dados a cada cinco minutos, e isso não é configurável.

Solução de problemas

Informações adicionais sobre este Coletor de dados podem ser encontradas ["Suporte"](#) na página ou no ["Matriz de suporte do Data Collector"](#).

Coletor de dados Dell EMC RecoverPoint

O principal caso de uso do coletor de dados EMC RecoverPoint é descobrir relações de replicação de volume para volume que o dispositivo de armazenamento RecoverPoint facilita. Este coletor também irá descobrir o próprio aparelho RecoverPoint. Observe que a Dell/EMC vende uma solução de backup VMware para VMs--"RecoverPoint for VMs"--que não é suportada por este coletor

Para a configuração, o coletor de dados requer o endereço IP dos processadores de armazenamento e um nome de usuário e senha somente leitura.

O coletor de dados EMC RecoverPoint reúne as relações de replicação de volume para volume que o RecoverPoint coordena entre outros arrays de armazenamento. O Data Infrastructure Insights mostra um storage array para cada cluster do RecoverPoint e coleta dados de inventário de nós e portas de storage nesse cluster. Nenhum pool de armazenamento ou dados de volume são coletados.

Requisitos

As seguintes informações são necessárias para configurar este coletor de dados:

- Endereço IP ou nome de domínio totalmente qualificado do processador de armazenamento
- Nome de utilizador e palavra-passe só de leitura
- Acesso à API REST via porta 443

Configuração

Campo	Descrição
Endereço do RecoverPoint	Endereço IP ou nome de domínio totalmente qualificado do cluster RecoverPoint
Nome de utilizador	Nome de utilizador para o cluster RecoverPoint
Palavra-passe	Palavra-passe utilizada para o cluster RecoverPoint

Configuração avançada

Campo	Descrição
Porta TCP	Porta TCP utilizada para ligar ao cluster RecoverPoint
Intervalo de enquete de inventário (minutos)	Intervalo entre sondagens de inventário. O padrão é 20 minutos.
Clusters excluídos	Lista separada por vírgulas de IDs ou nomes de cluster a excluir ao fazer polling.

Solução de problemas

Informações adicionais sobre este Coletor de dados podem ser encontradas ["Suporte"](#) na página ou no ["Matriz de suporte do Data Collector"](#).

Coletor de dados Dell EMC ScaleIO / PowerFlex

O coletor de dados ScaleIO/PowerFlex coleta informações de inventário do armazenamento ScaleIO e PowerFlex. Para configuração, esse coletor de dados requer o endereço de gateway ScaleIO/PowerFlex e um nome de usuário e senha de administrador.

Terminologia

O Data Infrastructure Insights adquire as seguintes informações de inventário do coletor de dados ScaleIO/PowerFlex. Para cada tipo de ativo adquirido pelo Data Infrastructure Insights, a terminologia mais

comum usada para esse ativo é mostrada. Ao visualizar ou solucionar problemas desse coletor de dados, tenha em mente a seguinte terminologia:

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
Cluster MDM (Meta Data Manager)	Armazenamento
SDS (servidor de dados ScaleIO/PowerFlex)	Nó de storage
Pool de storage	Pool de storage
Volume	Volume
Dispositivo	Disco

Nota: Estes são apenas mapeamentos de terminologia comuns e podem não representar todos os casos para este coletor de dados.

Requisitos

- Acesso somente leitura à conta de usuário Admin
- Requisito de porta: Porta HTTPS 443

Configuração

Campo	Descrição
Gateway(s) ScaleIO/PowerFlex	Endereços IP ou FQDNs de gateways ScaleIO/PowerFlex, separados por vírgula (,) ou ponto e vírgula (;)
Nome de utilizador	Nome de usuário Admin usado para fazer login no dispositivo ScaleIO/PowerFlex
Palavra-passe	Palavra-passe utilizada para iniciar sessão no dispositivo ScaleIO/PowerFlex

Configuração avançada

Clique na caixa de verificação Inventário para ativar a recolha de inventário.

Campo	Descrição
Porta de HTTPS	443
Intervalo de pesquisa de inventário (min)	A predefinição é 60.
Tempo limite da ligação (seg.)	A predefinição é 60.

Solução de problemas

Informações adicionais podem ser encontradas na ["Suporte"](#) página ou no ["Matriz de suporte do Data Collector"](#).

Configurando o coletor de dados EMC Unity

O coletor de dados Dell EMC Unity (anteriormente VNXe) fornece suporte de inventário

para matrizes de armazenamento unificadas VNXe. O Data Infrastructure Insights atualmente oferece suporte aos protocolos iSCSI e nas.

Requisitos

- O coletor de dados Unity é baseado na CLI; você deve instalar o Unisphere para Unity CLI (uemcli.exe) na unidade de aquisição onde reside o coletor de dados VNXe.
- O uemcli.exe usa HTTPS como protocolo de transporte, portanto, a unidade de aquisição precisará ser capaz de iniciar conexões HTTPS com o Unity.
- Endereço IP ou nome de domínio totalmente qualificado do dispositivo Unity
- Você deve ter pelo menos um usuário somente leitura para uso pelo coletor de dados.
- HTTPS na porta 443 é necessário
- O coletor de dados EMC Unity fornece suporte nas e iSCSI para inventário; volumes de canal de fibra serão descobertos, mas o Data Infrastructure Insights não relata portas de mapeamento, mascaramento ou armazenamento FC.

Terminologia

O Data Infrastructure Insights adquire as seguintes informações de inventário do coletor de dados Unity. Para cada tipo de ativo adquirido pelo Data Infrastructure Insights, a terminologia mais comum usada para esse ativo é mostrada. Ao visualizar ou solucionar problemas desse coletor de dados, tenha em mente a seguinte terminologia:

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
Disco	Disco
Storage array	Armazenamento
Processador	Nó de storage
Pool de storage	Pool de storage
Informações gerais do bloco iSCSI, VMware VMFS	Partilhar
Sistema remoto de replicação	Sincronização
Nó iSCSI	Nó de destino iSCSI
Iniciador iSCSI	Iniciador iSCSI Target

Nota: Estes são apenas mapeamentos de terminologia comuns e podem não representar todos os casos para esta fonte de dados.

Configuração

Campo	Descrição
Armazenamento Unity	Endereço IP ou nome de domínio totalmente qualificado do dispositivo Unity
Nome de utilizador	Nome de usuário do dispositivo Unity
Palavra-passe	Senha para o dispositivo Unity

Campo	Descrição
Caminho completo para o executável UEMCLI	Caminho completo para a pasta que contém o executável <i>uemcli.exe</i>

Configuração avançada

Campo	Descrição
Intervalo de enquete de inventário (min)	Intervalo entre sondagens de inventário. O padrão é 40 minutos
Porta Unity CLI	Porta usada para o Unity CLI
Intervalo de pesquisa de desempenho (seg)	A predefinição é 300.

Solução de problemas

Algumas coisas para tentar se você encontrar problemas com este coletor de dados:

Inventário

Problema:	Tente isto:
"Falha ao executar utilitário externo" com mensagens de erro "Falha ao encontrar o executável do Unisphere uemcli"	* Verifique o endereço IP, nome de usuário e senha corretos * Confirme se a Unisphere CLI está instalada na Unidade de aquisição do Data Infrastructure Insights * Confirme se o diretório de instalação da Unisphere CLI está correto na configuração da fonte de dados * Confirme se o IP do VNXe está correto na configuração da fonte de dados. Na Unidade de aquisição do Data Infrastructure Insights, abra um CMD e mude para o diretório de instalação configurado: Tente fazer uma conexão com o dispositivo VNXe digitando: <code>Uemcli -d <Your IP> -u <Your ID> /sys/general show</code>

Informações adicionais podem ser encontradas na ["Suporte"](#) página ou no ["Matriz de suporte do Data Collector"](#).

Coletor de dados da família de dispositivos Dell EMC VMAX e Powermax

O Data Infrastructure Insights descobre arrays de armazenamento EMC VMAX e Powermax usando comandos `symcli` do Solutions Enabler em conjunto com um servidor Solutions Enabler existente no seu ambiente. O servidor Solutions Enabler existente tem conectividade com o storage array VMAX/Powermax por meio do acesso aos volumes do gatekeeper.

Requisitos

Antes de configurar esse coletor de dados, você deve garantir que o Data Infrastructure Insights tenha conectividade TCP à porta 2707 no servidor Solutions Enabler existente. O Data Infrastructure Insights descobre todos os arrays Symmetrix que são "locais" para este servidor, como visto na saída `"symcfg list"` desse servidor.

- O aplicativo EMC Solutions Enabler (CLI) com provedor SMI-S deve ser instalado no servidor da Unidade de aquisição e a versão deve corresponder ou ser anterior à versão em execução no Solutions Enabler Server.
- É necessário um ficheiro devidamente configurado. Este arquivo define nomes de serviço para servidores Solutions Enabler, bem como o método de acesso (SECURE / NOSECURE /ANY).
- Se você precisar de latência de leitura/gravação no nível do nó de storage, o Fornecedor SMI-S deve se comunicar com uma instância em execução do aplicativo UNISPHERE for VMAX.
- Endereço IP do servidor Managing Solutions Enabler
- Permissões de administrador no servidor Solutions Enabler (se)
- Nome de utilizador e palavra-passe apenas de leitura para o software se
- O aplicativo UNISPHERE para VMAX deve estar executando e coletando estatísticas para os arrays EMC VMAX e Powermax sstorage gerenciados pela instalação do Fornecedor SMI-S.
- Validação de acesso para desempenho: Em um navegador da Web em sua Unidade de aquisição, vá para *Nome de host* `https://<SMI-S ou IP>:5989/ecomconfig` onde "Nome de host ou IP SMI-S" é o endereço IP ou nome de host do seu servidor SMI-S. Este URL é para um portal administrativo para o serviço EMC SMI-S (também conhecido como "ECOM") - você receberá um pop-up de login.
- As permissões devem ser declaradas no arquivo de configuração daemon do servidor Solutions Enabler, geralmente encontrado aqui: `/var/symapi/config/daemon_users`

Aqui está um arquivo de exemplo com as permissões cisys adequadas.

```

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 stordaeomon
control
###      operations (e.g., shutdown).
#####
#####
# smith          storrdfd
cisys storapid <all>

```

Terminologia

O Data Infrastructure Insights adquire as seguintes informações de inventário da fonte de dados EMC VMAX/Powermax. Para cada tipo de ativo adquirido, a terminologia mais comum usada para esse ativo é mostrada. Ao visualizar ou solucionar problemas desse coletor de dados, tenha em mente a seguinte terminologia:

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
Disco	Disco
Grupo de discos	Grupo de discos

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
Armazenamento	Storage de array
Diretor	Nó de storage
Pool de dispositivos, pool de recursos de armazenamento (SRP)	Pool de storage
Dispositivo TDev	Volume

Nota: Estes são apenas mapeamentos de terminologia comuns e podem não representar todos os casos para este coletor de dados.

Configuração

Observação: se a autenticação de usuário SMI-S não estiver ativada, os valores padrão no coletor de dados do Data Infrastructure Insights serão ignorados.

Campo	Descrição
Nome do serviço	Nome do serviço conforme especificado no arquivo <i>netcnfg</i>
Caminho completo para CLI	Caminho completo para a pasta que contém o Symmetrix CLI
Endereço IP do host SMI-S	Endereço IP do host SMI-S.

Configuração avançada

Campo	Descrição
Intervalo de enquete de inventário (min)	Intervalo entre sondagens de inventário. O padrão é 40 minutos.
Escolha 'Excluir' ou 'incluir' para especificar uma lista	Especifique se deve incluir ou excluir a lista de matrizes abaixo ao coletar dados.
Lista de dispositivos de filtro de inventário	Lista separada por vírgulas de IDs de dispositivo para incluir ou excluir

Campo	Descrição
Cache de conexão	Escolha o método de cache de conexão: * LOCAL significa que o serviço de aquisição Cloud Insights está sendo executado no servidor de ativação de soluções, que tem conectividade Fibre Channel com os arrays Symmetrix que você procura descobrir e tem acesso aos volumes do gatekeeper. Isso pode ser visto em algumas configurações da Unidade de aquisição Remota (RAU). * Remote_CACHED é o padrão e deve ser usado na maioria dos casos. Isso usa as configurações de arquivo NETCNFG para se conectar usando IP ao servidor Solutions Enabler, que deve ter conectividade Fibre Channel com os arrays Symmetrix que você busca descobrir e ter acesso aos volumes do Gatekeeper. * Caso as opções Remote_CACHED façam com que os comandos CLI falhem, use a OPÇÃO REMOTA. Tenha em mente que ele vai retardar o processo de aquisição (possivelmente para horas ou até mesmo dias em casos extremos). As configurações de arquivo NETCNFG ainda são usadas para uma conexão IP com o servidor Solutions Enabler que tem conectividade Fibre Channel com os arrays Symmetrix sendo descobertos. Observação: esta configuração não altera o comportamento do Data Infrastructure Insights em relação aos arrays listados como REMOTOS pela saída "symcfg list". O Data Infrastructure Insights coleta dados somente em dispositivos mostrados como LOCAIS por este comando.
Protocolo SMI-S.	Protocolo utilizado para ligar ao fornecedor SMI-S. Também exibe a porta padrão usada.
Substituir a porta SMIS	Se estiver em branco, use a porta padrão no campo tipo de conexão; caso contrário, insira a porta de conexão a ser usada
Nome de utilizador SMI-S.	Nome de utilizador para o anfitrião do fornecedor SMI-S.
Palavra-passe SMI-S.	Nome de utilizador para o anfitrião do fornecedor SMI-S.
Intervalo de polling de desempenho (seg)	Intervalo entre sondagens de desempenho (padrão 1000 segundos)
Toque em 'Excluir' ou 'incluir' para especificar uma lista	Especifique se deve incluir ou excluir a lista de matrizes abaixo ao coletar dados de desempenho
Lista de dispositivos de filtro de desempenho	Lista separada por vírgulas de IDs de dispositivo para incluir ou excluir

Solução de problemas

Algumas coisas para tentar se você encontrar problemas com este coletor de dados:

Problema:	Tente isto:
Erro: O recurso solicitado não está licenciado no momento	Instale a licença do servidor SYMAPI.
Erro: Nenhum dispositivo foi encontrado	Certifique-se de que os dispositivos Symmetrix estejam configurados para serem gerenciados pelo servidor Solutions Enabler: - Executar <code>symcfg list -v</code> para ver a lista de dispositivos Symmetrix configurados.
Erro: Um serviço de rede solicitado não foi encontrado no arquivo de serviço	Certifique-se de que o nome do serviço do Solutions Enabler esteja definido no arquivo <code>netcnfg</code> para o Solutions Enabler. Esse arquivo geralmente está localizado em SYMAPI na instalação do cliente do Solutions Enabler.
Erro: O handshake cliente/servidor remoto falhou	Verifique os arquivos <code>storsrvd.log*</code> mais recentes no host Solutions Enabler que estamos tentando descobrir.
Erro: O nome comum no certificado do cliente não é válido	Edite o arquivo <code>hosts</code> no servidor Solutions Enabler para que o nome do host da Unidade de aquisição resolva para o endereço IP conforme relatado no <code>storsrvd.log</code> no servidor Solutions Enabler.
Erro: A função não conseguiu obter memória	Certifique-se de que há memória livre suficiente disponível no sistema para executar o Solutions Enabler
Erro: O Solutions Enabler não conseguiu fornecer todos os dados necessários.	Investigue o status de integridade e o perfil de carga do Solutions Enabler
Erro: • O comando CLI " <code>symcfg list -tdev</code> " pode retornar dados incorretos quando coletados com o Solutions Enabler 7.x de um servidor Solutions Enabler 8.x. • O comando CLI " <code>symcfg list -srp</code> " pode retornar dados incorretos quando coletados com o Solutions Enabler 8.1.0 ou anterior de um servidor Solutions Enabler 8,3 ou posterior.	Certifique-se de que você está usando a mesma versão principal do Solutions Enabler
Estou vendo erros de coleta de dados com a mensagem: "Código desconhecido"	Você poderá ver essa mensagem se as permissões não forem declaradas no arquivo de configuração do daemon do servidor Solutions Enabler (veja Requisitos acima). Isto pressupõe que a versão do cliente se corresponde à versão do servidor se. Esse erro também pode ocorrer se o usuário <code>cisys</code> (que executa comandos Solutions Enabler) não tiver sido configurado com as permissões de daemon necessárias no arquivo de configuração <code>/var/symapi/config/daemon_users</code> . Para corrigir isso, edite o arquivo <code>/var/symapi/config/daemon_users</code> e verifique se o usuário <code>cisys</code> tem permissão <code><all></code> especificada para o daemon <code>storapid</code> . Exemplo: 14:11:25 no tail <code>/var/symapi/config/daemon_users ... cisys storapid <all></code>

Informações adicionais podem ser encontradas na "[Suporte](#)" página ou no "[Matriz de suporte do Data](#)"

Collector".

Coletor de dados Dell EMC VNX Block Storage (Navicli)

O Data Infrastructure Insights usa o coletor de dados Dell EMC VNX Block Storage (NaviSec) (anteriormente CLARiiON) para adquirir dados de inventário e desempenho.

Terminologia

O Data Infrastructure Insights adquire as seguintes informações de inventário do coletor de dados EMC VNX Block Storage. Para cada tipo de ativo adquirido pelo Data Infrastructure Insights, a terminologia mais comum usada para esse ativo é mostrada. Ao visualizar ou solucionar problemas desse coletor de dados, tenha em mente a seguinte terminologia:

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
Disco	Disco
Armazenamento	Armazenamento
Processador de armazenamento	Nó de storage
Este pool, RAID Group	Pool de storage
LUN	Volume

Nota: Estes são apenas mapeamentos de terminologia comuns e podem não representar todos os casos para esta fonte de dados.

Requisitos

Os seguintes requisitos devem ser atendidos para coletar dados:

- Um endereço IP de cada processador de armazenamento de bloco VNX
- Nome de usuário e senha do Navisphere somente leitura para os storages de armazenamento de bloco VNX
- O NaviSecCli deve ser instalado no Data Infrastructure Insights AU
- Validação de acesso: Execute o NaviSecCLI a partir do Data Infrastructure Insights AU para cada array usando o nome de usuário e a senha.
- Requisitos do porto: 80, 443
- A versão NaviSecCLI deve corresponder com o código FLARE mais recente em sua matriz
- Para obter desempenho, o registo de estatísticas tem de estar ativado.

Sintaxe de interface de linha de comando Navisphere

```
naviseccli.exe -h <IP address> -user <user> -password <password> -scope,use 0 for global scope> -port [use 443 by default] comando
```

Configuração

Campo	Descrição
Endereço IP de armazenamento de bloco VNX	Endereço IP ou nome de domínio totalmente qualificado do armazenamento de blocos VNX
Nome de utilizador	Nome utilizado para iniciar sessão no dispositivo de armazenamento de bloco VNX.
Palavra-passe	Palavra-passe utilizada para iniciar sessão no dispositivo de armazenamento de bloco VNX.
Caminho CLI para naviseccli.exe	Caminho completo para a pasta que contém o executável <i>naviseccli.exe</i>

Configuração avançada

Campo	Descrição
Intervalo de enquete de inventário (min)	Intervalo entre sondagens de inventário. O padrão é de 40 minutos.
Âmbito de aplicação	O escopo seguro do cliente. O padrão é Global.
Intervalo de enquete de desempenho (seg)	Intervalo entre sondagens de desempenho. O padrão é 300 segundos.

Solução de problemas

Algumas coisas para tentar se você encontrar problemas com este coletor de dados:

Inventário

Problema:	Tente isto:
<p>Erro:</p> <ul style="list-style-type: none"> • O agente não está em execução • Falha ao encontrar naviseccli • Falha ao executar qualquer comando 	<ul style="list-style-type: none"> • Confirme se o Navisphere CLI está instalado na Unidade de aquisição do Cloud Insight • Você não selecionou a opção "usar cliente seguro" no assistente de configuração do coletor de dados e não tem uma versão não segura do Navisphere CLI instalada. • Confirme se o diretório de instalação do Navisphere CLI está correto na configuração do coletor de dados • Confirme se o IP do armazenamento de blocos VNX está correto na configuração do coletor de dados: • Na unidade de aquisição do Data Infrastructure Insights: <ul style="list-style-type: none"> ◦ Abra um cmd. ◦ Altere o diretório para o diretório de instalação configurado ◦ Tente fazer uma conexão com o dispositivo de armazenamento de bloco VNX digitando "navicli -h ip getagent" (substitua o ip pelo IP real)
<p>Erro: 4,29 emc235848 emc241018 getall falhou ao analisar informações de alias do host</p>	<p>Isso provavelmente é causado por um problema de corrupção do FLARE 29 do banco de dados do iniciador do host no próprio array. Consulte os artigos da base de conhecimento EMC: emc235848, emc241018. Você também pode verificar https://now.netapp.com/Knowledgebase/solutionarea.asp?id=kb58128</p>
<p>Erro: Não foi possível recuperar meta LUNs. Erro ao executar o Java -jar navicli.jar</p>	<ul style="list-style-type: none"> • Modificar a configuração do coletor de dados para usar o cliente seguro (recomendado) • Instale o navicli.jar no caminho CLI para navicli.exe OU naviseccli.exe • Nota: O navicli.jar está obsoleto a partir do EMC Navisphere versão 6,26 • O navicli.jar pode estar disponível no http://powerlink.emc.com
<p>Erro: Os pools de armazenamento não reportam discos no processador de serviço no endereço IP configurado</p>	<p>Configure o coletor de dados com ambos os IPs do processador de serviço, separados por uma vírgula</p>

Problema:	Tente isto:
Erro: Erro de incompatibilidade de revisão	<ul style="list-style-type: none"> • Isso geralmente é causado pela atualização do firmware no dispositivo de armazenamento de bloco VNX, mas não pela atualização da instalação do Navicli.exe. Isso também pode ser causado por ter dispositivos diferentes com firmwares diferentes, mas apenas uma CLI instalada (com uma versão de firmware diferente). • Verifique se o dispositivo e o host estão executando versões idênticas do software: <ul style="list-style-type: none"> ◦ Na Unidade de aquisição do Data Infrastructure Insights, abra uma janela de linha de comando ◦ Altere o diretório para o diretório de instalação configurado ◦ Faça uma conexão com o dispositivo CLARiiON digitando "navicli -h <ip> getagent" ◦ Procure o número da versão nas primeiras linhas. Exemplo: "Agente Rev: 6.16.2 (0,1)" ◦ Procure e compare a versão na primeira linha. Exemplo: "Navisphere CLI Revisão 6.07.00.04.07"
Erro: Configuração não suportada - sem portas Fibre Channel	O dispositivo não está configurado com nenhuma porta Fibre Channel. Atualmente, apenas configurações de FC são compatíveis. Verifique se esta versão/firmware é suportada.

Informações adicionais podem ser encontradas na ["Suporte"](#) página ou no ["Matriz de suporte do Data Collector"](#).

Coletor de dados Dell EMC VNX File (antigo Celerra Unified Storage System)

Este coletor de dados adquire informações de inventário do sistema de armazenamento de ficheiros VNX. Para configuração, este coletor de dados requer o endereço IP dos processadores de armazenamento e um nome de usuário e senha somente leitura.

Terminologia

O Data Infrastructure Insights adquire as seguintes informações de inventário do coletor de dados do arquivo VNX. Para cada tipo de ativo adquirido pelo Data Infrastructure Insights, a terminologia mais comum usada para esse ativo é mostrada. Ao visualizar ou solucionar problemas desse coletor de dados, tenha em mente a seguinte terminologia:

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
Celerra Network Server/Celerra Storage Pool	Pool de storage

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
Sistema de ficheiros	Volume interno
Transferência de dados	Controlador
Sistema de arquivos montado em um controlador de dados	Partilha de ficheiros
Exportações de CIFS e NFS	Partilhar
Volume do disco	LUN de back-end

Nota: Estes são apenas mapeamentos de terminologia comuns e podem não representar todos os casos para este coletor de dados.

Requisitos

Você precisa do seguinte para configurar este coletor de dados:

- O endereço IP do processador de armazenamento
- Nome de utilizador e palavra-passe só de leitura
- Porta SSH 22

Configuração

Campo	Descrição
Endereço IP do ficheiro VNX	Endereço IP ou nome de domínio totalmente qualificado do dispositivo VNX File
Nome de utilizador	Nome utilizado para iniciar sessão no dispositivo ficheiro VNX
Palavra-passe	Palavra-passe utilizada para iniciar sessão no dispositivo ficheiro VNX

Configuração avançada

Campo	Descrição
Intervalo de enquete de inventário (minutos)	Intervalo entre sondagens de inventário. O padrão é 20 minutos.

Solução de problemas

Algumas coisas para tentar se você encontrar problemas com este coletor de dados:

Inventário

Problema:	Tente isto:
Erro: Não é possível prosseguir com a atualização DART em andamento	Solução possível: Pausar o coletor de dados e aguardar que a atualização DART seja concluída antes de tentar outra solicitação de aquisição.

Informações adicionais podem ser encontradas na ["Suporte"](#) página ou no ["Matriz de suporte do Data Collector"](#).

Configurando o coletor de dados unificado VNX da Dell EMC

Para configuração, o coletor de dados Dell EMC VNX Unified (SSH) requer o endereço IP da Estação de Controle e um nome de usuário e senha somente leitura.

Terminologia

O Data Infrastructure Insights adquire as seguintes informações de inventário desse coletor de dados. Para cada tipo de ativo adquirido pelo Data Infrastructure Insights, a terminologia mais comum usada para esse ativo é mostrada. Ao visualizar ou solucionar problemas desse coletor de dados, tenha em mente a seguinte terminologia:

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
Disco	Disco
Pasta de disco	Grupo de discos
Sistema de arquivos	Volume interno
Armazenamento	Armazenamento
Processador de armazenamento	Nó de storage
Pool de armazenamento, grupo RAID	Pool de storage
LUN	Volume
Transferência de dados	Controlador
Sistema de arquivos montado em um controlador de dados	Partilha de ficheiros
Exportações de CIFS e NFS	Partilhar
Volume do disco	LUN de back-end

Requisitos

Você precisa do seguinte para configurar o coletor de dados VNX (SSH):

- Endereço IP VNX e credenciais para a Estação de Controle Celerra.
- Nome de utilizador e palavra-passe só de leitura.
- O coletor de dados é capaz de executar comandos Navicli/NaviSecCLI contra o array backend utilizando as cabeças nas DART os

Configuração

Campo	Descrição
Endereço IP VNX	Endereço IP ou nome de domínio totalmente qualificado da Estação de Controle VNX
Nome de utilizador	Nome de utilizador para a Estação de controlo VNX

Campo	Descrição
Palavra-passe	Palavra-passe para a Estação de controlo VNX

Configuração avançada

Campo	Descrição
Intervalo de enquete de inventário (min)	Intervalo entre sondagens de inventário. O padrão é 40 minutos.
Intervalo de enquete de desempenho (seg).	Intervalo entre sondagens de desempenho. O padrão é 300 segundos.

Solução de problemas

Informações adicionais sobre este Coletor de dados podem ser encontradas ["Suporte"](#) na página ou no ["Matriz de suporte do Data Collector"](#).

Configurando o coletor de dados EMC VPLEX

Este coletor de dados adquire dados de inventário e desempenho dos sistemas de armazenamento EMC VPLEX. Para a configuração, o coletor de dados requer um endereço IP do servidor VPLEX e uma conta de domínio de nível administrativo.



A coleta de desempenho do Data Infrastructure Insights de clusters Vplex exige que o serviço de arquivamento de performance esteja operacional, a fim de preencher os arquivos .CSV e os logs que o Data Infrastructure Insights recupera por meio de cópias de arquivos baseadas em SCP. A NetApp observou que muitas atualizações da estação de gerenciamento/atualização de firmware da Vplex deixarão essa funcionalidade não operacional. Os clientes que planejam essas atualizações podem querer perguntar proativamente à Dell/EMC se sua atualização planejada deixará essa funcionalidade inoperável e, em caso afirmativo, como podem reabilitá-la para minimizar as lacunas na visibilidade do desempenho? O código de desempenho Vplex do Cloud Insight avaliará em cada enquete se todos os arquivos esperados existem e se eles estão sendo atualizados corretamente. Se estiverem ausentes ou obsoletos, o Data Infrastructure Insights registrará falhas na coleta de performance.

Terminologia

A Insightst adquire as seguintes informações de inventário do coletor de dados VPLEX. Para cada tipo de ativo adquirido, a terminologia mais comum usada para esse ativo é mostrada. Ao visualizar ou solucionar problemas desse coletor de dados, tenha em mente a seguinte terminologia:

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
Cluster	Armazenamento
Motor	Nó de storage
Dispositivo, extensão do sistema	Pool de storage de back-end
Volume virtual	Volume
Porta Front-end, porta back-end	Porta

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
Dispositivo distribuído	Sincronização de armazenamento
Vista de armazenamento	Mapa de volume, Máscara de volume
Volume de armazenamento	LUN de back-end
ITLs	Caminho de back-end

Nota: Estes são apenas mapeamentos de terminologia comuns e podem não representar todos os casos para este coletor de dados.

Requisitos

- Um endereço IP da consola de gestão VPLEX
- Conta de domínio de nível administrativo para o servidor VPLEX
- Porta 443 (HTTPS). Requer conectividade de saída à porta TCP 443 na estação de gerenciamento VPLEX.
- Para desempenho, nome de usuário e senha somente leitura para acesso ssh/scp.
- Para o desempenho, a porta 22 é necessária.

Configuração

Campo	Descrição
Endereço IP da consola de gestão VPLEX	Endereço IP ou nome de domínio totalmente qualificado do Console de Gerenciamento VPLEX
Nome de utilizador	Nome de usuário para VPLEX CLI
Palavra-passe	Palavra-passe utilizada para VPLEX CLI
Endereço IP remoto de desempenho	Endereço IP remoto de desempenho da consola de gestão VPLEX
Nome de utilizador remoto do desempenho	Desempenho Nome de usuário remoto do VPLEX Management Console
Palavra-passe remota de desempenho	Palavra-passe remota de desempenho do VPLEX Management Console

Configuração avançada

Campo	Descrição
Porta de comunicação	Porta usada para VPLEX CLI. A predefinição é 443.
Intervalo de enquete de inventário (min)	O padrão é 20 minutos.
Número de tentativas de conexão	A predefinição é 3.
Intervalo de enquete de desempenho (seg)	Intervalo entre sondagens de desempenho. O padrão é 600 segundos.
Número de geometrias	A predefinição é 2.

Solução de problemas

Algumas coisas para tentar se você encontrar problemas com este coletor de dados:

Inventário

Problema:	Tente isto:
Erro: Falha na autenticação do utilizador.	Certifique-se de que as suas credenciais para este dispositivo estão corretas.

Desempenho

Problema:	Tente isto:
Erro: O desempenho VPLEX para a versão abaixo de 5,3 não é suportado.	Atualize VPLEX para 5,3 ou superior
Erro: Não foram recolhidos dados suficientes.	• Verifique o carimbo de data/hora da coleção no arquivo de log e modifique o intervalo de polling em conformidade • aguarde mais tempo
Erro: Arquivos de log perpétuos não estão sendo atualizados.	Entre em Contato com o suporte da EMC para ativar a atualização dos arquivos de log perpétuos
Erro: O intervalo de polling de desempenho é muito grande.	Verifique o timestamp da coleção no arquivo de log e modifique o intervalo de polling em conformidade
Erro: O endereço IP remoto do Console de Gerenciamento VPLEX não está configurado.	Edite a fonte de dados para definir o endereço IP remoto de desempenho do VPLEX Management Console.
Erro: Nenhum dado de desempenho relatado pelo diretor	• Verifique se os monitores de desempenho do sistema estão sendo executados corretamente • entre em Contato com o suporte da EMC para habilitar a atualização dos arquivos de log do monitor de desempenho do sistema

Informações adicionais podem ser encontradas na "[Suporte](#)" página ou no "[Matriz de suporte do Data Collector](#)".

Coletor de dados Dell EMC XtremIO

O coletor de dados EMC XtremIO adquire dados de inventário e desempenho do sistema de armazenamento EMC XtremIO.

Requisitos

Para configurar o coletor de dados EMC XtremIO (HTTP), você deve ter:

- O endereço de host XMS (XMS) do XtremIO Management Server
- Uma conta com o administrador Privileges
- Acesso à porta 443 (HTTPS)

Terminologia

O Data Infrastructure Insights adquire as seguintes informações de inventário do coletor de dados EMC XtremIO. Para cada tipo de ativo adquirido pelo Data Infrastructure Insights, a terminologia mais comum usada para esse ativo é mostrada. Ao visualizar ou solucionar problemas desta fonte de dados, tenha em mente a seguinte terminologia:

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
Disco (SSD)	Disco
Cluster	Armazenamento
Controlador	Nó de storage
Volume	Volume
Mapa LUN	Mapa de volume
Iniciador FC de destino	Máscara de volume

Nota: Estes são apenas mapeamentos de terminologia comuns e podem não representar todos os casos para esta fonte de dados.

Requisitos

- O endereço IP do host XMS (XMS) do XtremIO Management Server
- Nome de usuário e senha do administrador para o XtremIO

Configuração

Campo	Descrição
Anfitrião XMS	Endereço IP ou nome de domínio totalmente qualificado do XtremIO Management Server
Nome de utilizador	Nome de usuário do XtremIO Management Server
Palavra-passe	Senha para o XtremIO Management Server

Configuração avançada

Campo	Descrição
Porta de TCP	Porta TCP usada para se conectar ao XTremIO Management Server. A predefinição é 443.
Intervalo de pesquisa de inventário (min)	Intervalo entre sondagens de inventário. O padrão é 60 minutos.
Intervalo de pesquisa de desempenho (seg)	Intervalo entre sondagens de desempenho. O padrão é 300 segundos.

Solução de problemas

Informações adicionais sobre este Coletor de dados podem ser encontradas ["Suporte"](#) na página ou no ["Matriz de suporte do Data Collector"](#).

Fujitsu ETERNUS Data Collector

O coletor de dados ETERNUS da Fujitsu adquire dados de inventário utilizando acesso de nível de administração ao sistema de armazenamento.

Terminologia

A Data Infrastructure Insights adquire as seguintes informações de inventário do armazenamento Fujitsu ETERNUS. Para cada tipo de ativo adquirido pelo Data Infrastructure Insights, a terminologia mais comum usada para esse ativo é mostrada. Ao visualizar ou solucionar problemas desse coletor de dados, tenha em mente a seguinte terminologia:

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
Disco	Disco
Armazenamento	Armazenamento
Thin Pool, pool de camadas flexível, grupo RAID	Pool de storage
Volume padrão, volume de dados Snap (SDV), volume de pool de dados Snap (SDPV), volume de provisionamento fino (TPV), volume de nível flexível (FTV), volume de distribuição ampla (WSV)	Volume
Adaptador de canal	Controlador

Nota: Estes são apenas mapeamentos de terminologia comuns e podem não representar todos os casos para este coletivismo de dados.

Requisitos

Para configurar este coletor de dados, são necessários os seguintes itens:

- Um endereço IP do armazenamento ETERNUS, que não pode ser delimitado por vírgulas
- Nome de usuário e senha no nível de administração SSH
- Porta 22
- Certifique-se de que a rolagem da página está desativada (clienv-show-more-scroll disable)

Configuração

Campo	Descrição
Endereço IP do armazenamento ETERNUS	Endereço IP do armazenamento ETERNUS
Nome de utilizador	Nome de utilizador para armazenamento ETERNUS
Palavra-passe	Palavra-passe para o armazenamento ETERNUS

Configuração avançada

Campo	Descrição
Intervalo de enquete de inventário (min)	O padrão é 20 minutos.

Solução de problemas

Algumas coisas para tentar se você encontrar problemas com este coletor de dados:

Inventário

Problema:	Tente isto:
"Erro ao recuperar dados" com mensagens de erro "Error finding prompt CLI" ou "Error finding prompt no final dos resultados do shell"	Provavelmente causado por: O sistema de armazenamento tem rolagem de página ativada. Solução possível: * Tente desativar a rolagem de página executando o seguinte comando: <code>Set clienv-show-more -scroll disable</code>
"Erro de conexão" com mensagens de erro "Falha ao instanciar uma conexão SSH ao armazenamento" ou "Falha ao instanciar uma conexão ao VirtualCenter"	Causas prováveis: * Credenciais incorretas. * Endereço IP incorreto. * Problema de rede. * O armazenamento pode estar inativo ou não responder. Soluções possíveis: * Verifique as credenciais e o endereço IP inseridos. * Tente se comunicar com o armazenamento usando SSH Client.

Informações adicionais podem ser encontradas na ["Suporte"](#) página ou no ["Matriz de suporte do Data Collector"](#).

Coletor de dados do NetApp Google Compute

Esse coletor de dados suporta a coleta de inventário e desempenho das configurações da plataforma de nuvem do Google Compute. Este coletor procurará descobrir todos os recursos de computação em todos os projetos dentro de uma organização do Google. Se você tiver várias organizações do Google que deseja descobrir com o Data Infrastructure Insights, será necessário implantar um coletor de Insights de infraestrutura de dados por organização.

Requisitos da conta de serviço

- Você deve criar uma conta de serviço seguindo as instruções em ["Criando/gerenciando contas de serviço"](#). Essa conta de serviço é identificada por um ID exclusivo, conhecido como seu *ClientID*, que será usado como um nome de usuário.
- Além disso, crie uma chave de conta de serviço seguindo as instruções em ["Criando/gerenciando chaves de conta de serviço"](#). Essa chave pode ser baixada como um arquivo json, cujo conteúdo será usado como senha.
- A conta de serviço deve ter escopo para *Compute.readonly*, *monitoring.read* e *cloud-Platform*.

Configuração

Campo	Descrição
Código Organização	O ID da organização que você deseja descobrir com este coletor. Este campo é obrigatório se a sua conta de serviço for capaz de ver mais de uma organização
Escolha 'Excluir' ou 'incluir' para filtrar projetos do GCP por IDs	Se você quiser limitar quais recursos dos projetos são trazidos para o Data Infrastructure Insights.

Campo	Descrição
IDs de projeto	A lista de IDs de projeto que você deseja filtrar dentro ou fora da descoberta, dependendo do valor do valor "escolha 'Excluir'....". A lista padrão está vazia
ID do cliente	ID do cliente para a configuração do Google Cloud Platform
Copie e cole o conteúdo do seu arquivo de credencial do Google aqui	Copie suas credenciais do Google para a conta do Cloud Platform para este campo

Configuração avançada

Campo	Descrição
Intervalo de enquete de inventário (min)	O padrão é de 60 minutos
Escolha 'Excluir' ou 'incluir' para aplicar ao filtro de VMs por rótulos	Especifique se deseja incluir ou excluir VM por rótulos ao coletar dados. Se "incluir" estiver selecionado, o campo chave de rótulo não pode estar vazio.
Rotule chaves e valores nos quais filtrar VMs	Clique em * rótulo de filtro* para escolher quais VMs (e discos associados) incluir/excluir filtrando chaves e valores que correspondem a chaves e valores de rótulos na VM. A chave da etiqueta é necessária, o valor da etiqueta é opcional. Quando o valor de rótulo está vazio, a VM é filtrada desde que corresponda à chave de rótulo.
Intervalo de enquete de desempenho (seg)	O padrão é de 1800 segundos

Solução de problemas

Informações adicionais sobre este Coletor de dados podem ser encontradas ["Suporte"](#) na página ou no ["Matriz de suporte do Data Collector"](#).

HP Enterprise

Coletor de dados HP Enterprise Alletra 9000 / Primera Storage

O Data Infrastructure Insights usa o coletor de dados HP Enterprise Alletra 9000 / HP Enterprise Primera (anteriormente 3PAR) para descobrir inventário e desempenho.

Terminologia

O Data Infrastructure Insights adquire as seguintes informações de inventário desse coletor de dados. Para cada tipo de ativo adquirido pelo Data Infrastructure Insights, a terminologia mais comum usada para esse ativo é mostrada. Ao visualizar ou solucionar problemas desse coletor de dados, tenha em mente a seguinte terminologia:

Campo	Descrição
Disco físico	Disco
Sistema de storage	Armazenamento

Campo	Descrição
Nó do controlador	Nó de storage
Grupo de provisionamento comum	Pool de storage
Volume virtual	Volume

Nota: Estes são apenas mapeamentos de terminologia comuns e podem não representar todos os casos para este coletor de dados.

Requisitos

Para configurar este coletor de dados, são necessários os seguintes itens:

- Endereço IP ou FQDN do cluster InServ
- Para inventário, nome de usuário somente leitura e senha para o servidor StoreServ
- Para obter desempenho, leia-escreva o nome de usuário e a senha para o servidor StoreServ
- Requisitos de porta: 22 (coleta de inventário), 5988 ou 5989 (coleta de desempenho) [Nota: O desempenho é suportado para o StoreServ os 3.x]
- Para a coleta de desempenho, confirme que SMI-S está habilitado fazendo login no array via SSH.

Configuração

Campo	Descrição
Endereço IP de armazenamento	Endereço IP de armazenamento ou nome de domínio totalmente qualificado do cluster StoreServ
Nome de utilizador	Nome de usuário para o servidor StoreServ
Palavra-passe	Senha usada para o servidor StoreServ
Nome de utilizador SMI-S.	Nome de utilizador para o anfitrião do fornecedor SMI-S.
Palavra-passe SMI-S.	Palavra-passe utilizada para o anfitrião do fornecedor SMI-S.

Configuração avançada

Campo	Descrição
Intervalo de enquete de inventário (min)	Intervalo entre sondagens de inventário. O padrão é 40 minutos.
Conetividade SMI-S	Protocolo utilizado para ligar ao fornecedor SMI-S.
Substituir a porta padrão SMI-S.	Se estiver em branco, use a porta padrão da conetividade SMI-S; caso contrário, insira a porta de conexão a ser usada
Intervalo de enquete de desempenho (seg)	Intervalo entre sondagens de desempenho. O padrão é 300 segundos.

Solução de problemas

Algumas coisas para tentar se você encontrar problemas com este coletor de dados:

Inventário

Problema:	Tente isto:
o comando "showsys" não retorna nenhum resultado.	Execute "showsys" e "showversion -a" a partir da linha de comando e verifique se a versão é suportada pelo array.

Desempenho

Problema:	Tente isto:
Falha ao ligar ou iniciar sessão. Falha na inicialização do fornecedor.	Um nome de array all-numeric pode causar problemas com o servidor SMI-S. Tente alterar o nome do array.
O usuário SMI-S configurado não tem nenhum domínio	Conceda Privileges de domínio apropriado ao usuário SMI-S configurado
O Data Infrastructure Insights afirma que não pode se conectar/fazer login ao serviço SMI-S.	Confirme se não há firewall entre a AU de IC e a matriz que bloquearia a AU de IC de fazer conexões TCP para 5988 ou 5989. Uma vez que isso é feito, e se você confirmou que não há firewall, você deve SSH para o array, e usar o comando "showcim" para confirmar. Verifique se: * O serviço está ativado * HTTPS está ativado * a porta HTTPS deve ser 5989 se todos forem assim, você pode tentar "startcim" e, em seguida, um "startcim" para reiniciar o CIM (ou seja, o serviço SMI-S).

Informações adicionais podem ser encontradas na ["Suporte"](#) página ou no ["Matriz de suporte do Data Collector"](#).

Coletor de dados HP Enterprise Command View

O coletor de dados HP Enterprise Command View Advanced Edition suporta a descoberta de matrizes XP e P9500 através do servidor CVAE (Command View Advanced Edition). O Data Infrastructure Insights se comunica com o CVAE usando a API Command View padrão para coletar dados de inventário e desempenho.

Terminologia

O Data Infrastructure Insights adquire as seguintes informações de inventário do coletor de dados HP Enterprise Command View. Para cada tipo de ativo adquirido pelo Data Infrastructure Insights, a terminologia mais comum usada para esse ativo é mostrada. Ao visualizar ou solucionar problemas desse coletor de dados, tenha em mente a seguinte terminologia:

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
PDEV	Disco

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
Pool Diário	Grupo de discos
Storage array	Armazenamento
Controlador de porta	Nó de storage
Grupo de array, DP Pool	Pool de storage
Unidade lógica, LDEV	Volume

Nota: Estes são apenas mapeamentos de terminologia comuns e podem não representar todos os casos para este coletor de dados.

Requisitos de inventário

Você deve ter o seguinte para coletar dados de inventário:

- Endereço IP do servidor CVAE
- Nome de usuário e senha somente leitura para o software CVAE e Privileges peer
- Exigência do porto: 2001

Requisitos de desempenho

Os seguintes requisitos devem ser atendidos para coletar dados de desempenho:

- Desempenho do HDS USP, USP V e VSP
 - O Monitor de desempenho deve ser licenciado.
 - O interruptor de monitorização tem de estar ativado.
 - A ferramenta de exportação (Export.exe) deve ser copiada para a AU Data Infrastructure Insights e extraída para um local. No CI Linux AUS, certifique-se de que "cisys" tenha permissões de leitura e execução.
 - A versão da ferramenta de exportação deve corresponder à versão do microcódigo da matriz de destino.
- Desempenho AMS:
 - O Monitor de desempenho deve ser licenciado.
 - O utilitário CLI do Storage Navigator Modular 2 (SNM2) deve ser instalado no Data Infrastructure Insights AU.
- Requisitos de rede
 - As Ferramentas de exportação são baseadas em Java e usam RMI para falar com o array. Essas ferramentas podem não ser compatíveis com firewall, pois podem negociar dinamicamente as portas TCP de origem e destino em cada invocação. Além disso, as ferramentas de exportação de diferentes matrizes de modelos podem se comportar de forma diferente em toda a rede - consulte a HPE para obter os requisitos do seu modelo

Configuração

Campo	Descrição
Servidor de visualização de comandos	Endereço IP ou nome de domínio totalmente qualificado do servidor Command View
Nome de utilizador	Nome de usuário do servidor Command View.
Palavra-passe	Senha usada para o servidor Command View.
DISPOSITIVOS - VSP G1000 (R800), VSP (R700), HUS VM (HM700) E ARMAZENAMENTOS USP	Lista de dispositivos para armazenamentos VSP G1000 (R800), VSP (R700), HUS VM (HM700) e USP. Cada armazenamento requer: * IP da matriz: Endereço IP do armazenamento * Nome do utilizador: Nome do utilizador para o armazenamento * Palavra-passe: Palavra-passe para o armazenamento * pasta que contém ficheiros JAR do utilitário de exportação
SNM2Devices - armazenamentos WMS/SMS/AMS	Lista de dispositivos para armazenamentos WMS/SMS/AMS. Cada armazenamento requer: * IP da matriz: Endereço IP do armazenamento * caminho CLI do Navegador de armazenamento: SNM2 caminho CLI * Autenticação de conta válida: Selecione para escolher autenticação de conta válida * Nome de utilizador: Nome de utilizador para o armazenamento * Palavra-passe: Palavra-passe para o armazenamento
Escolha o Tuning Manager para desempenho	Substituir outras opções de desempenho
Host do Tuning Manager	Endereço IP ou nome de domínio totalmente qualificado do gerenciador de ajuste
Porta do Gestor de sintonização	Porta usada para Tuning Manager
Nome de utilizador do Gestor de sintonização	Nome de usuário para Tuning Manager
Palavra-passe do Gestor de sintonização	Senha para Tuning Manager

Nota: No HDS USP, USP V e VSP, qualquer disco pode pertencer a mais de um grupo de matrizes.

Configuração avançada

Campo	Descrição
Porta do servidor de visualização de comandos	Porta usada para o Command View Server
HTTPS ativado	Selecione para ativar HTTPS
Intervalo de enquete de inventário (min)	Intervalo entre sondagens de inventário. A predefinição é 40.
Escolha 'Excluir' ou 'incluir' para especificar uma lista	Especifique se deve incluir ou excluir a lista de matrizes abaixo ao coletar dados.
Excluir ou incluir dispositivos	Lista separada por vírgulas de ID de dispositivo ou nomes de matriz para incluir ou excluir
Consultar Gestor anfitrião	Selecione para consultar o gestor de anfitrião

Intervalo de polling de desempenho (seg)	Intervalo entre sondagens de desempenho. A predefinição é 300.
--	--

Solução de problemas

Algumas coisas para tentar se você encontrar problemas com este coletor de dados:

Inventário

Problema:	Tente isto:
Erro: O usuário não tem permissão suficiente	Use uma conta de usuário diferente que tenha mais privilégios ou aumente o privilégio de conta de usuário configurada no coletor de dados
Erro: A lista de armazenamentos está vazia. Os dispositivos não estão configurados ou o usuário não tem permissão suficiente	* Use DeviceManager para verificar se os dispositivos estão configurados. * Use uma conta de usuário diferente que tenha mais privilégios ou aumente o privilégio da conta de usuário
Erro: A matriz de armazenamento HDS não foi atualizada durante alguns dias	Investigue por que esse array não está sendo atualizado no HP CommandView AE.

Desempenho

Problema:	Tente isto:
Erro: * Erro ao executar o utilitário de exportação * erro ao executar comando externo	* Confirme se Export Utility está instalado na Unidade de aquisição do Data Infrastructure Insights * Confirme se a localização do Utilitário de exportação está correta na configuração do coletor de dados * Confirme se o IP do array USP/R600 está correto na configuração do coletor de dados * Confirme se o nome do usuário e a senha estão corretos na configuração do coletor de dados * Confirme se runWin.bat
Erro: O login da ferramenta de exportação falhou para o IP de destino	* Confirmar que o nome de utilizador/palavra-passe está correto * criar uma ID de utilizador principalmente para este coletor de dados HDS * confirmar que nenhum outro coletor de dados está configurado para adquirir esta matriz
Erro: Ferramentas de exportação registradas "não é possível obter intervalo de tempo para monitoramento".	* Confirmar que o monitoramento de desempenho está habilitado no array. * Tente invocar as ferramentas de exportação fora do Data Infrastructure Insights para confirmar que o problema está fora do Data Infrastructure Insights.
Erro: * Erro de configuração: Matriz de armazenamento não suportada pelo Utilitário de exportação * erro de configuração: Matriz de armazenamento não suportada pela CLI Modular do Storage Navigator	* Configurar apenas matrizes de armazenamento suportadas. * Use "Filtrar lista de dispositivos" para excluir matrizes de armazenamento não suportadas.

Problema:	Tente isto:
Erro: * Erro ao executar comando externo * erro de configuração: Matriz de armazenamento não reportada pelo Inventário * erro de configuração:pasta de exportação não contém arquivos jar	* Verifique a localização do utilitário de exportação. * Verifique se a matriz de armazenamento em questão está configurada no servidor Command View * defina o intervalo de enquete de desempenho como múltiplo de 60 segundos.
Erro: * Error Storage Navigator CLI * erro ao executar o comando auperform * erro ao executar comando externo	* Confirme que a CLI Modular do Storage Navigator está instalada na Unidade de aquisição de dados Insights da infraestrutura de dados * Confirme que a localização da CLI Modular do Storage Navigator está correta na configuração do coletor de dados * Confirme que a versão da CLI Modular do Storage Navigator é compatível com a versão de micro-código da matriz de armazenamento configurada no coletor de dados * da Unidade de aquisição de dados Insights da infraestrutura de dados, abra um diretório de dados, abra o seguinte para fazer uma conexão de cliente configurada para executar uma conexão do storage auteref.exe.
Erro: Erro de configuração: Storage Array não reportado pelo Inventário	Verifique se a matriz de armazenamento em questão está configurada no servidor Command View
Erro: * Nenhuma matriz é registrada com o Storage Navigator Modular 2 CLI * a matriz não está registrada com o Storage Navigator Modular 2 CLI * erro de configuração: Matriz de armazenamento não registrada com o StorageNavigator Modular CLI	* Abra o prompt de comando e mude o diretório para o caminho configurado * execute o comando * Executar o comando "auunitref" * confirmar que a saída do comando contém detalhes da matriz com IP * se a saída não contém os detalhes da matriz, em seguida, Registrar a matriz com Storage Navigator CLI: - Abrir prompt de comando e alterar diretório para o caminho configurado - execute o comando "set - Execute o comando "auunitaddauto -ip". Substitua o ip por IP real

Informações adicionais podem ser encontradas na "[Suporte](#)" página ou no "[Matriz de suporte do Data Collector](#)".

Coletor de dados HPE Alletra 6000

O coletor de dados HP Enterprise Alletra 6000 (anteriormente ágil) suporta dados de inventário e desempenho para matrizes de armazenamento Alletra 6000.

Terminologia

O Data Infrastructure Insights adquire as seguintes informações de inventário desse coletor. Para cada tipo de ativo adquirido pelo Data Infrastructure Insights, a terminologia mais comum usada para esse ativo é mostrada. Ao visualizar ou solucionar problemas desse coletor de dados, tenha em mente a seguinte terminologia:

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
Array	Armazenamento

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
Disco	Disco
Volume	Volume
Piscina	Pool de storage
Iniciador	Alias do host de storage
Controlador	Nó de storage
Interface Fibre Channel	Controlador

Nota: Estes são apenas mapeamentos de terminologia comuns e podem não representar todos os casos para este coletor de dados.

Requisitos

Você deve ter o seguinte para coletar dados de inventário e configuração da matriz de armazenamento:

- A matriz deve ser instalada e configurada e acessível a partir do cliente através do seu nome de domínio totalmente qualificado (FQDN) ou endereço IP de gerenciamento de matriz.
- O array deve estar executando NimbleOS 2,3.x ou posterior.
- Você deve ter um nome de usuário e senha válidos para o array com pelo menos função de nível "Operador". A função "convidado" não tem acesso suficiente para compreender as configurações do iniciador.
- A porta 5392 deve estar aberta no array.

Você deve ter o seguinte para coletar dados de desempenho da matriz de armazenamento:

- O array deve estar executando NimbleOS 4.0.0 ou posterior
- O array deve ter volumes configurados. A única API de performance que o NimbleOS tem é para volumes, e quaisquer estatísticas de relatórios Data Infrastructure Insights são derivados das estatísticas sobre volumes

Configuração

Campo	Descrição
Endereço IP de gerenciamento de matriz	Nome de domínio totalmente qualificado (FQDN) ou endereço IP de gerenciamento de matriz.
Nome de utilizador	Nome de usuário para o array
Palavra-passe	Senha para o array

Configuração avançada

Campo	Descrição
Porta	Porta usada pela API REST do Nimble. A predefinição é 5392.
Intervalo de enquete de inventário (min)	Intervalo entre sondagens de inventário. O padrão é 60 minutos.

Observação: O intervalo padrão de enquete de desempenho é de 300 segundos e não pode ser alterado. Este é o único intervalo suportado pelo HPE Alletra 6000.

Sistemas de dados Hitachi

Coletor de dados Hitachi Vantara Command Suite

O coletor de dados Hitachi Vantara Command Suite suporta o servidor HiCommand Device Manager. O Data Infrastructure Insights se comunica com o servidor HiCommand Device Manager usando a API padrão HiCommand.

Terminologia

O Data Infrastructure Insights adquire as seguintes informações de inventário do coletor de dados do Hitachi Vantara Command Suite. Para cada tipo de ativo adquirido pelo Data Infrastructure Insights, a terminologia mais comum usada para esse ativo é mostrada. Ao visualizar ou solucionar problemas desse coletor de dados, tenha em mente a seguinte terminologia:

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
PDEV	Disco
Pool Diário	Grupo de discos
Storage array	Armazenamento
Controlador de porta	Nó de storage
Grupo de array, HDS Pool	Pool de storage
Unidade lógica, LDEV	Volume

Nota: Estes são apenas mapeamentos de terminologia comuns e podem não representar todos os casos para este coletor de dados.

Armazenamento

Os termos a seguir se aplicam a objetos ou referências que você pode encontrar nas páginas iniciais de ativos de armazenamento HDS. Muitos desses termos também se aplicam a outros coletores de dados.

- Nome – vem diretamente do atributo "nome" do HDS HiCommand Device Manager através da chamada API XML GetStorageArray
- Modelo - vem diretamente do atributo arrayType do HDS HiCommand Device Manager através da chamada API XML GetStorageArray
- Fornecedor – HDS
- Família - vem diretamente do atributo "arrayFamily" do HDS HiCommand Device Manager através da chamada API XML GetStorageArray
- IP – este é o endereço IP de gerenciamento da matriz, não uma lista exaustiva de todos os endereços IP da matriz
- Capacidade bruta – um valor de base2 que representa a soma da capacidade total de todos os discos neste sistema, independentemente da função de disco.

Pool de storage

Os termos a seguir se aplicam a objetos ou referências que você pode encontrar nas páginas iniciais de ativos do pool de armazenamento HDS. Muitos desses termos também se aplicam a outros coletores de dados.

- Tipo: O valor aqui será um dos seguintes:
 - Reservado – se esse pool for dedicado para outros fins que não volumes de dados, ou seja, journaling, instantâneos
 - Provisionamento de thin – se este for um pool HDP
 - RAID Group – você provavelmente não verá isso por alguns motivos:

O Data Infrastructure Insights adota uma postura forte para evitar a dupla capacidade de contagem a todo custo. No HDS, normalmente é necessário construir grupos RAID a partir de discos, criar volumes de pool nesses grupos RAID e construir pools (muitas vezes HDP, mas poderia ser um propósito especial) a partir desses volumes de pool. Se o Data Infrastructure Insights reportasse tanto os grupos RAID subjacentes como os estão, como os pools, a soma de sua capacidade bruta excederia consideravelmente a soma dos discos.

Em vez disso, o coletor de dados HDS Command Suite do Data Infrastructure Insights reduz arbitrariamente o tamanho dos grupos RAID pela capacidade dos volumes de pool. Isso pode fazer com que os Insights de infraestrutura de dados não relatem o RAID Group. Além disso, quaisquer grupos RAID resultantes são sinalizados de forma a que não sejam visíveis na WebUI do Data Infrastructure Insights, mas fluem para a DWH (Data Infrastructure Insights Data Warehouse). O objetivo dessas decisões é evitar a confusão da interface do usuário para coisas que a maioria dos usuários não se importa – se seu array HDS tiver grupos RAID com 50MB livre, você provavelmente não pode usar esse espaço livre para qualquer resultado significativo.

- Nó - N/A, pois os pools do HDS não estão vinculados a nenhum nó específico
- Redundância - o nível RAID do pool. Possivelmente vários valores para um pool HDP composto por vários tipos de RAID
- % De capacidade - a porcentagem utilizada do conjunto para utilização de dados, com o GB utilizado e o tamanho de GB lógico total do conjunto
- Capacidade sobre-comprometida - um valor derivado, afirmando "a capacidade lógica deste pool é supersubscrita por esta porcentagem em virtude da soma dos volumes lógicos que excedem a capacidade lógica do pool por esta porcentagem"
- Instantâneo - mostra a capacidade reservada para uso de snapshot neste pool

Nó de storage

Os termos a seguir se aplicam a objetos ou referências que você pode encontrar nas páginas iniciais de ativos de nó de armazenamento HDS. Muitos desses termos também se aplicam a outros coletores de dados.

- Nome – o nome do diretor de front-end (FED) ou do adaptador de canal em matrizes monolíticas, ou o nome do controlador em uma matriz modular. Um determinado array do HDS terá 2 ou mais nós de storage
- Volumes – a tabela volume mostrará qualquer volume mapeado para qualquer porta pertencente a esse nó de armazenamento

Requisitos de inventário

Você deve ter o seguinte para coletar dados de inventário:

- Endereço IP do servidor HiCommand Device Manager
- Nome de usuário e senha somente leitura para o software Gerenciador de dispositivos HiCommand e Privileges peer
- Requisitos de porta: 2001 (http) ou 2443 (https)
- Faça login no software HiCommand Device Manager usando nome de usuário e senha
- Verifique o acesso ao Gerenciador de dispositivos HiCommand
http://<HiCommand_Device_Manager_IP>:2001/Service/StorageManager

Requisitos de desempenho

Os seguintes requisitos devem ser atendidos para coletar dados de desempenho:

- Desempenho do HDS USP, USP V e VSP
 - O Monitor de desempenho deve ser licenciado.
 - O interruptor de monitorização tem de estar ativado.
 - A ferramenta de exportação (Export.exe) deve ser copiada para a AU Data Infrastructure Insights.
 - A versão da ferramenta de exportação deve corresponder à versão do microcódigo da matriz de destino.
- Desempenho AMS:
 - A NetApp recomenda fortemente a criação de uma conta de serviço dedicada nos storages AMS para Insights de infraestrutura de dados a serem usados para recuperar dados de desempenho. O Navegador de armazenamento permite apenas uma conta de usuário um login simultâneo na matriz. Ter o Data Infrastructure Insights usar a mesma conta de usuário que os scripts de gerenciamento ou o HiCommand pode fazer com que o Data Infrastructure Insights, scripts de gerenciamento ou o HiCommand não consigam se comunicar com o array devido ao limite de login de uma conta de usuário concorrente
 - O Monitor de desempenho deve ser licenciado.
 - O utilitário CLI do Storage Navigator Modular 2 (SNM2) precisa ser instalado no Data Infrastructure Insights AU.

Configuração

Campo	Descrição
Servidor HiCommand	Endereço IP ou nome de domínio totalmente qualificado do servidor HiCommand Device Manager
Nome de utilizador	Nome de usuário do servidor HiCommand Device Manager.
Palavra-passe	Senha usada para o servidor HiCommand Device Manager.

Campo	Descrição
DISPOSITIVOS - VSP G1000 (R800), VSP (R700), HUS VM (HM700) E ARMAZENAMENTOS USP	Lista de dispositivos para armazenamentos VSP G1000 (R800), VSP (R700), HUS VM (HM700) e USP. Cada armazenamento requer: * IP da matriz: Endereço IP do armazenamento * Nome do utilizador: Nome do utilizador para o armazenamento * Palavra-passe: Palavra-passe para o armazenamento * pasta que contém ficheiros JAR do utilitário de exportação
SNM2Devices - armazenamentos WMS/SMS/AMS	Lista de dispositivos para armazenamentos WMS/SMS/AMS. Cada armazenamento requer: * IP da matriz: Endereço IP do armazenamento * caminho CLI do Navegador de armazenamento: SNM2 caminho CLI * Autenticação de conta válida: Selecione para escolher autenticação de conta válida * Nome de utilizador: Nome de utilizador para o armazenamento * Palavra-passe: Palavra-passe para o armazenamento
Escolha o Tuning Manager para desempenho	Substituir outras opções de desempenho
Host do Tuning Manager	Endereço IP ou nome de domínio totalmente qualificado do gerenciador de ajuste
Substituir a porta do Gestor de sintonização	Se estiver em branco, use a porta padrão no campo Choose Tuning Manager for Performance (escolher Gerenciador de sintonização para desempenho). Caso contrário, insira a porta a ser usada
Nome de utilizador do Gestor de sintonização	Nome de usuário para Tuning Manager
Palavra-passe do Gestor de sintonização	Senha para Tuning Manager

Nota: No HDS USP, USP V e VSP, qualquer disco pode pertencer a mais de um grupo de matrizes.

Configuração avançada

Campo	Descrição
Tipo de ligação	HTTPS ou HTTP, também exibe a porta padrão
Porta do servidor HiCommand	Porta usada para o Gerenciador de dispositivos HiCommand
Intervalo de enquete de inventário (min)	Intervalo entre sondagens de inventário. A predefinição é 40.
Escolha 'Excluir' ou 'incluir' para especificar uma lista	Especifique se deve incluir ou excluir a lista de matrizes abaixo ao coletar dados.
Filtrar lista de dispositivos	Lista separada por vírgulas de números de série do dispositivo para incluir ou excluir
Intervalo de enquete de desempenho (seg)	Intervalo entre sondagens de desempenho. A predefinição é 300.
Tempo limite de exportação em segundos	Tempo limite do utilitário de exportação. A predefinição é 300.

Solução de problemas

Algumas coisas para tentar se você encontrar problemas com este coletor de dados:

Inventário

Problema:	Tente isto:
Erro: O usuário não tem permissão suficiente	Use uma conta de usuário diferente que tenha mais privilégios ou aumente o privilégio de conta de usuário configurada no coletor de dados
Erro: A lista de armazenamentos está vazia. Os dispositivos não estão configurados ou o usuário não tem permissão suficiente	* Use DeviceManager para verificar se os dispositivos estão configurados. * Use uma conta de usuário diferente que tenha mais privilégios ou aumente o privilégio da conta de usuário
Erro: A matriz de armazenamento HDS não foi atualizada durante alguns dias	Investigue por que razão esta matriz não está a ser atualizada no HDS HiCommand.

Desempenho

Problema:	Tente isto:
Erro: * Erro ao executar o utilitário de exportação * erro ao executar comando externo	* Confirme se Export Utility está instalado na Unidade de aquisição do Data Infrastructure Insights * Confirme se a localização do Utilitário de exportação está correta na configuração do coletor de dados * Confirme se o IP do array USP/R600 está correto na configuração do coletor de dados * Confirme se o nome do usuário e a senha estão corretos na configuração do coletor de dados * Confirme se runWin.bat
Erro: O login da ferramenta de exportação falhou para o IP de destino	* Confirmar que o nome de utilizador/palavra-passe está correto * criar uma ID de utilizador principalmente para este coletor de dados HDS * confirmar que nenhum outro coletor de dados está configurado para adquirir esta matriz
Erro: Ferramentas de exportação registradas "não é possível obter intervalo de tempo para monitoramento".	* Confirmar que o monitoramento de desempenho está habilitado no array. * Tente invocar as ferramentas de exportação fora do Data Infrastructure Insights para confirmar que o problema está fora do Data Infrastructure Insights.
Erro: * Erro de configuração: Matriz de armazenamento não suportada pelo Utilitário de exportação * erro de configuração: Matriz de armazenamento não suportada pela CLI Modular do Storage Navigator	* Configurar apenas matrizes de armazenamento suportadas. * Use "Filtrar lista de dispositivos" para excluir matrizes de armazenamento não suportadas.
Erro: * Erro ao executar comando externo * erro de configuração: Matriz de armazenamento não reportada pelo Inventário * erro de configuração:pasta de exportação não contém arquivos jar	* Verifique a localização do utilitário de exportação. * Verifique se a matriz de armazenamento em questão está configurada no servidor HiCommand * defina o intervalo de enquete de desempenho como múltiplo de 60 segundos.

Problema:	Tente isto:
Erro: * Error Storage Navigator CLI * erro ao executar o comando auperform * erro ao executar comando externo	* Confirme que a CLI Modular do Storage Navigator está instalada na Unidade de aquisição de dados Insights da infraestrutura de dados * Confirme que a localização da CLI Modular do Storage Navigator está correta na configuração do coletor de dados * Confirme que a versão da CLI Modular do Storage Navigator é compatível com a versão de micro-código da matriz de armazenamento configurada no coletor de dados * da Unidade de aquisição de dados Insights da infraestrutura de dados, abra um diretório de dados, abra o seguinte para fazer uma conexão de cliente configurada para executar uma conexão do storage auteref.exe.
Erro: Erro de configuração: Storage Array não reportado pelo Inventário	Verifique se o Storage Array em questão está configurado no servidor HiCommand
Erro: * Nenhuma matriz é registrada com o Storage Navigator Modular 2 CLI * a matriz não está registrada com o Storage Navigator Modular 2 CLI * erro de configuração: Matriz de armazenamento não registrada com o StorageNavigator Modular CLI	* Abra o prompt de comando e mude o diretório para o caminho configurado * execute o comando * Executar o comando "auunitref" * confirmar que a saída do comando contém detalhes da matriz com IP * se a saída não contém os detalhes da matriz, em seguida, Registrar a matriz com Storage Navigator CLI: - Abrir prompt de comando e alterar diretório para o caminho configurado - execute o comando "set - Executar comando "auunitaddauto -IP <ip>". Substitua o <ip> pelo IP correto.

Informações adicionais podem ser encontradas na "[Suporte](#)" página ou no "[Matriz de suporte do Data Collector](#)".

Configurar o coletor de dados Hitachi Vantara nas

O coletor de dados Hitachi Vantara nas é um coletor de dados de inventário e configuração que suporta a descoberta de clusters HDS nas. O Data Infrastructure Insights é compatível com a descoberta de compartilhamentos NFS e CIFS, sistemas de arquivos (volumes internos) e vãos (pools de storage).

Terminologia

O Data Infrastructure Insights adquire as seguintes informações de inventário do coletor de dados HNAS. Para cada tipo de ativo adquirido pelo Data Infrastructure Insights, a terminologia mais comum usada para esse ativo é mostrada. Ao visualizar ou solucionar problemas desse coletor de dados, tenha em mente a seguinte terminologia:

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
Nível	Grupo de discos
Cluster	Armazenamento
Nó	Nó de storage

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
Extensão	Pool de storage
Unidade do sistema	LUN de back-end
Sistema de ficheiros	Volume interno

Nota: Estes são apenas mapeamentos de terminologia comuns e podem não representar todos os casos para este coletor de dados.

Requisitos

- Endereço IP do dispositivo
- Porta 22, protocolo SSH
- Nome de utilizador e palavra-passe - nível de privilégio: Supervisor
- Nota: Este coletor de dados é baseado em SSH, então a AU que o hospeda deve ser capaz de iniciar sessões SSH para TCP 22 no próprio HNAS, ou a Unidade de Gerenciamento de sistemas (SMU) à qual o cluster está conetado.

Configuração

Campo	Descrição
Host HNAS	Endereço IP ou nome de domínio totalmente qualificado do HNAS Management Host
Nome de utilizador	Nome de usuário para HNAS CLI
Palavra-passe	Senha usada para HNAS CLI

Configuração avançada

Campo	Descrição
Intervalo de enquete de inventário (min)	Intervalo entre sondagens de inventário. O padrão é 30 minutos.

Solução de problemas

Algumas coisas para tentar se você encontrar problemas com este coletor de dados:

Inventário

Problema:	Tente isto:
"Erro ao conetar-se" com mensagens de erro "erro ao configurar canal de shell:" ou "erro ao abrir canal de shell"	Provavelmente causado por problemas de conectividade de rede ou SSH está mal configurado. Confirme a conexão com o cliente SSH alternativo
"Timeout" ou "erro ao recuperar dados" com mensagens de erro "Command: XXX expirou."	* Tente o comando com o cliente SSH alternativo * aumente o tempo limite

Problema:	Tente isto:
"Erro ao conectar " ou "credenciais de login inválidas" com mensagens de erro "não foi possível se comunicar com o dispositivo:"	* Verificar endereço IP * verificar nome de usuário e senha * confirmar conexão com cliente SSH alternativo

Informações adicionais podem ser encontradas na "[Suporte](#)" página ou no "[Matriz de suporte do Data Collector](#)".

Coletor de dados do Hitachi Ops Center

Esse coletor de dados usa o conjunto integrado de aplicativos do Hitachi Ops Center para acessar dados de inventário e desempenho de vários dispositivos de armazenamento. Para descoberta de inventário e capacidade, a instalação do Ops Center deve incluir os componentes "Common Services" e "Administrator". Para a coleta de desempenho, você deve também ter o "Analyzer" implantado.

Terminologia

O Data Infrastructure Insights adquire as seguintes informações de inventário desse coletor de dados. Para cada tipo de ativo adquirido pelo Data Infrastructure Insights, a terminologia mais comum usada para esse ativo é mostrada. Ao visualizar ou solucionar problemas desse coletor de dados, tenha em mente a seguinte terminologia:

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
Sistemas de storage	Armazenamento
Volume	Volume
Grupos de paridade	Pool de armazenamento (RAID), grupos de discos
Disco	Disco
Pool de storage	Pool de armazenamento (fino, SNAP)
Grupos de paridade externa	Pool de armazenamento (back-end), grupos de discos
Porta	Nó de storage → nó do controlador → porta
Grupos de acolhimento	Mapeamento de volume e Masking
Pares de volume	Sincronização de armazenamento

Nota: Estes são apenas mapeamentos de terminologia comuns e podem não representar todos os casos para este coletor de dados.

Requisitos de inventário

Você deve ter o seguinte para coletar dados de inventário:

- Endereço IP ou nome do host do servidor Ops Center que hospeda o componente "Common Services"
- Conta de usuário root/sysadmin e senha que existem em todos os servidores que hospedam componentes do Ops Center. A HDS não implementou suporte à API REST para uso por usuários LDAP/SSO até o Ops Center 10,8

Requisitos de desempenho

Os seguintes requisitos devem ser atendidos para coletar dados de desempenho:

O módulo "Analyzer" do HDS Ops Center deve ser instalado Storage Arrays devem estar alimentando o módulo "Analyzer" do Ops Center

Configuração

Campo	Descrição
Endereço IP do Centro de operações Hitachi	Endereço IP ou nome de domínio totalmente qualificado do servidor Ops Center que hospeda o componente "Serviços comuns"
Nome de utilizador	Nome de usuário do servidor do Ops Center.
Palavra-passe	Senha usada para o servidor do Ops Center.

Configuração avançada

Campo	Descrição
Tipo de ligação	O padrão é HTTPS (porta 443)
Substituir a porta TCP	Especifique a porta a ser usada se não for a padrão
Intervalo de enquete de inventário (min)	Intervalo entre sondagens de inventário. A predefinição é 40.
Escolha 'Excluir' ou 'incluir' para especificar uma lista	Especifique se deve incluir ou excluir a lista de matrizes abaixo ao coletar dados.
Filtrar lista de dispositivos	Lista separada por vírgulas de números de série do dispositivo para incluir ou excluir
Intervalo de enquete de desempenho (seg)	Intervalo entre sondagens de desempenho. A predefinição é 300.

Informações adicionais podem ser encontradas na ["Suporte"](#) página ou no ["Matriz de suporte do Data Collector"](#).

Infinidat InfiniBox coletor de dados

O coletor de dados Infinidat InfiniBox (HTTP) é usado para coletar informações de inventário do sistema de armazenamento Infinidat InfiniBox.

Terminologia

O Data Infrastructure Insights adquire as seguintes informações de inventário do coletor de dados Infinidat InfiniBox. Para cada tipo de ativo adquirido pelo Data Infrastructure Insights, a terminologia mais comum usada para esse ativo é mostrada. Ao visualizar ou solucionar problemas desse coletor de dados, tenha em mente a seguinte terminologia:

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
Pool de storage	Pool de storage

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
Nó	Controlador
Sistema de ficheiros	Volume interno
Sistema de ficheiros	Partilha de ficheiros
Exportações do sistema de arquivos	Partilhar

Requisitos

A seguir estão os requisitos ao configurar este coletor de dados.

- Endereço IP ou FQDN do nó de gerenciamento InfiniBox
- ID de usuário e senha do administrador
- Porta 443 via API REST

Configuração

Campo	Descrição
Host InfiniBox	Endereço IP ou nome de domínio totalmente qualificado do nó de gerenciamento InfiniBox
Nome de utilizador	Nome de usuário para InfiniBox Management Node
Palavra-passe	Senha para o nó de gerenciamento InfiniBox

Configuração avançada

Campo	Descrição
Porta TCP	Porta TCP usada para se conectar ao InfiniBox Server. A predefinição é 443.
Intervalo Poll Stock	Intervalo entre sondagens de inventário. O padrão é 60 minutos.

Solução de problemas

Informações adicionais sobre este Coletor de dados podem ser encontradas ["Suporte"](#) na página ou no ["Matriz de suporte do Data Collector"](#).

Coletor de dados Huawei OceanStor

O Data Infrastructure Insights usa o coletor de dados OceanStor (REST/HTTPS) da Huawei para descobrir o inventário e o desempenho para o armazenamento OceanStor e OceanStor Dorado da Huawei.

Terminologia

A Data Infrastructure Insights adquire as seguintes informações de inventário e desempenho do OceanStor da Huawei. Para cada tipo de ativo adquirido pelo Data Infrastructure Insights, a terminologia mais comum usada

para esse ativo é mostrada. Ao visualizar ou solucionar problemas desse coletor de dados, tenha em mente a seguinte terminologia:

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
Pool de storage	Pool de storage
Sistema de ficheiros	Volume interno
Controlador	Nó de storage
Porta FC (mapeada)	Mapa de volume
Iniciador FC do host (mapeado)	Máscara de volume
Compartilhamento NFS/CIFS	Partilhar
iSCSI Link Target	Nó de destino iSCSI
Iniciador de ligação iSCSI	Nó do iniciador iSCSI
Disco	Disco
LUN	Volume

Requisitos

Os seguintes requisitos são necessários para configurar este coletor de dados:

- Endereço IP do dispositivo
- Credenciais para acessar o gerenciador de dispositivos OceanStor
- A porta 8088 deve estar disponível

Configuração

Campo	Descrição
Endereço IP do host OceanStor	Endereço IP ou nome de domínio totalmente qualificado do OceanStor Device Manager
Nome de utilizador	Nome utilizado para iniciar sessão no OceanStor Device Manager
Palavra-passe	Palavra-passe utilizada para iniciar sessão no OceanStor Device Manager

Configuração avançada

Campo	Descrição
Porta TCP	Porta TCP usada para se conectar ao OceanStor Device Manager. A predefinição é 8088.
Intervalo de enquete de inventário (min)	Intervalo entre sondagens de inventário. O padrão é 60 minutos.
Intervalo de pesquisa de desempenho (seg).	O padrão é 300 segundos.

Solução de problemas

Informações adicionais sobre este Coletor de dados podem ser encontradas "[Suporte](#)" na página ou no "[Matriz de suporte do Data Collector](#)".

IBM

Coletor de dados IBM Cleversafe

O Data Infrastructure Insights usa esse coletor de dados para descobrir dados de inventário e desempenho para sistemas de armazenamento IBM Cleversafe.



O IBM Cleversafe é medido a uma taxa bruta diferente de TB para Unidade gerenciada. A cada 40 TB de capacidade não formatada do IBM Cleversafe é cobrada como 1 "[Unidade gerenciada \(MU\)](#)".

Terminologia

O Data Infrastructure Insights adquire as seguintes informações de inventário do coletor de dados IBM Cleversafe. Para cada tipo de ativo adquirido pelo Data Infrastructure Insights, a terminologia mais comum usada para esse ativo é mostrada. Ao visualizar ou solucionar problemas desse coletor de dados, tenha em mente a seguinte terminologia:

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
Pool de storage	Pool de storage
Recipiente	Volume interno
Recipiente	Partilha de ficheiros
Compartilhamento NFS	Partilhar

Nota: Estes são apenas mapeamentos de terminologia comuns e podem não representar todos os casos para este coletor de dados.

Requisitos

- O endereço IP dos serviços de dados externos para o cluster
- Nome de usuário e senha do administrador
- Porta 9440

Configuração

Campo	Descrição
IP ou nome do host do gerente	Endereço IP ou nome do host do nó de gerenciamento
Nome de utilizador	Nome de usuário para a conta de usuário com super usuário ou função de administrador do sistema
Palavra-passe	Senha para a conta de usuário com super usuário ou função de administrador do sistema

Configuração avançada

Campo	Descrição
Intervalo de pesquisa de inventário (min)	Intervalo entre sondagens de inventário.
Tempo limite da conexão HTTP (seg)	Tempo limite HTTP em segundos.

Solução de problemas

Informações adicionais sobre este Coletor de dados podem ser encontradas "[Suporte](#)" na página ou no "[Matriz de suporte do Data Collector](#)".

Coletor de dados IBM CS

O Data Infrastructure Insights usa esse coletor de dados para descobrir dados de inventário e desempenho para sistemas de armazenamento IBM CS.

Terminologia

O Data Infrastructure Insights adquire as seguintes informações de inventário do coletor de dados do IBM CS. Para cada tipo de ativo adquirido pelo Data Infrastructure Insights, a terminologia mais comum usada para esse ativo é mostrada. Ao visualizar ou solucionar problemas desse coletor de dados, tenha em mente a seguinte terminologia:

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
Pool de storage	Pool de storage
Recipiente	Volume interno
Recipiente	Partilha de ficheiros
Compartilhamento NFS	Partilhar

Nota: Estes são apenas mapeamentos de terminologia comuns e podem não representar todos os casos para este coletor de dados.

Requisitos

- O endereço IP dos serviços de dados externos para o cluster
- Nome de usuário e senha do administrador
- Porta 9440

Configuração

Campo	Descrição
Endereço IP externo do prisma	O endereço IP dos serviços de dados externos para o cluster
Nome de utilizador	Nome de usuário para a conta de administrador
Palavra-passe	Palavra-passe para a conta de administrador

Configuração avançada

Campo	Descrição
Porta de TCP	Porta TCP usada para se conectar ao array IBM CS. A predefinição é 9440.
Intervalo de pesquisa de inventário (min)	Intervalo entre sondagens de inventário. O padrão é 60 minutos.
Intervalo de pesquisa de desempenho (seg)	Intervalo entre sondagens de desempenho. O padrão é 300 segundos.

Solução de problemas

Informações adicionais sobre este Coletor de dados podem ser encontradas "[Suporte](#)" na página ou no "[Matriz de suporte do Data Collector](#)".

Coletor de dados IBM System Storage DS8000 Series

O coletor de dados IBM DS (CLI) suporta a aquisição de dados de inventário e desempenho para dispositivos DS6xxx e DS8xxx.

Os dispositivos DS3xxx, DS4xxx e DS5xxx são suportados pelo "[Coletor de dados NetApp e-Series](#)". Você deve consultar a matriz de suporte do Data Infrastructure Insights para modelos e versões de firmware compatíveis.

Terminologia

O Data Infrastructure Insights adquire as seguintes informações de inventário do coletor de dados IBM DS. Para cada tipo de ativo adquirido pelo Data Infrastructure Insights, a terminologia mais comum usada para esse ativo é mostrada. Ao visualizar ou solucionar problemas desse coletor de dados, tenha em mente a seguinte terminologia:

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
Módulo de unidade de disco	Disco
Imagem de armazenamento	Armazenamento
Fundo de extensão	Nó de storage
Volume de bloco fixo	Volume
Iniciador FC do host (mapeado)	Máscara de volume

Nota: Estes são apenas mapeamentos de terminologia comuns e podem não representar todos os casos para esta coleta de dados.

Requisitos

Você precisa do seguinte para configurar este coletor de dados:

- Endereço IP de cada DS array
- Nome de utilizador e palavra-passe apenas de leitura em cada DS array
- Software de terceiros instalado no Data Infrastructure Insights AU: IBM *dscli*

- Validação de acesso: Execute os comandos *dscli* usando o nome de usuário e a senha
- Requisitos de porta: 80, 443 e 1750

Configuração

Campo	Descrição
Storage DS	Endereço IP ou nome de domínio totalmente qualificado do dispositivo DS
Nome de utilizador	Nome de usuário para a CLI DS
Palavra-passe	Senha para a CLI DS
<i>dscli</i> caminho executável	Caminho completo para o executável <i>dscli</i>

Configuração avançada

Campo	Descrição
Intervalo de enquete de inventário (min)	Intervalo entre pesquisas de inventário (min). A predefinição é 40.
Nome de exibição do armazenamento	Nome do storage array do IBM DS
Inventário Excluir dispositivos	Lista separada por vírgulas de números de série do dispositivo a excluir da coleção de inventário
Intervalo de enquete de desempenho (seg)	A predefinição é 300.
Tipo de filtro de desempenho	Incluir: Dados coletados apenas de dispositivos na lista. Excluir: Nenhum dado desses dispositivos é coletado
Lista de dispositivos de filtro de desempenho	Lista separada por vírgulas de IDs de dispositivo para incluir ou excluir da coleção de desempenho

Solução de problemas

Algumas coisas para tentar se você encontrar problemas com este coletor de dados:

Inventário

Problema:	Tente isto:
Erro contendo: CMUC00192E, CMUC00191E ou CMUC00190E	* Verifique as credenciais e o endereço IP inseridos. * Tente se comunicar com o array através do console de gerenciamento da Web <a href="https://<ip>:8452/DS8000/Console">https://<ip>:8452/DS8000/Console . Substitua o <ip> pelo IP configurado pelo coletor de dados.

Problema:	Tente isto:
Erro: * Não é possível executar o programa * erro executando o comando	* Da Unidade de aquisição do Data Infrastructure Insights abra um arquivo CMD * abra o arquivo CLI.CFG no diretório inicial da CLI/lib e verifique a propriedade JAVA_INSTALL, edite o valor para corresponder ao seu ambiente * Exibir versão Java instalada nesta máquina, digitando: "java -version" * Ping o endereço IP do dispositivo IBM Storage especificado no comando CLI emitido. * Se todos os itens acima funcionaram bem, então execute manualmente um comando CLI

Informações adicionais podem ser encontradas na ["Suporte"](#) página ou no ["Matriz de suporte do Data Collector"](#).

Configurando o coletor de dados IBM PowerVM

O coletor de dados IBM PowerVM (SSH) é usado para coletar informações sobre partições virtuais executadas em instâncias de hardware IBM POWER gerenciadas por um console de gerenciamento de hardware (HMC).

Terminologia

O Data Infrastructure Insights adquire informações de inventário das partições virtuais executadas em instâncias de hardware IBM POWER. Para cada tipo de ativo adquirido, a terminologia mais comum usada para o ativo é mostrada. Ao visualizar ou solucionar problemas desse coletor de dados, tenha em mente a seguinte terminologia:

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
hdisk	Disco virtual
Sistema gerenciado	Host
LPAR, servidor VIO	Máquina virtual
Grupo de volume	Armazenamento de dados
Volume físico	LUN

Nota: Estes são apenas mapeamentos de terminologia comuns e podem não representar todos os casos para este coletor de dados.

Requisitos

Os seguintes requisitos devem ser atendidos para configurar e usar este coletor de dados:

- Endereço IP do Console de Gerenciamento de hardware (HMC)
- Nome de usuário e senha que fornecem acesso ao hardware Management Console (HMC) por meio de SSH
- Requisito de porta SSH-22
- Visualize a permissão em todos os sistemas de gerenciamento e domínios de segurança de partição lógica

O usuário também deve ter permissão View em configurações HMC e a capacidade de coletar informações VPD para o agrupamento de segurança do console HMC. O usuário também deve ter permissão de acesso ao comando Virtual IO Server sob o agrupamento de segurança de partição lógica. É uma prática recomendada começar a partir de uma função de operador e depois remover todas as funções. Usuários somente leitura no HMC não têm Privileges para executar comandos proxied em hosts AIX.

- A prática recomendada da IBM é ter os dispositivos monitorados por dois ou mais HMCs. Esteja ciente de que isso pode fazer com que o OnCommand Insight relate dispositivos duplicados, portanto, é altamente recomendável adicionar dispositivos redundantes à lista "Excluir dispositivos" na Configuração Avançada para este coletor de dados.

Configuração

Campo	Descrição
Endereço IP do console de gerenciamento de hardware (HMC)	Endereço IP ou nome de domínio totalmente qualificado do PowerVM hardware Management Console
Utilizador HMC	Nome de usuário do Console de Gerenciamento de hardware
Palavra-passe	Senha usada para o Console de Gerenciamento de hardware

Configuração avançada

Campo	Descrição
Intervalo de enquete de inventário (min)	Intervalo entre sondagens de inventário. O padrão é 20 minutos.
Porta SSH	Porta usada para SSH para o PowerVM
Palavra-passe	Senha usada para o Console de Gerenciamento de hardware
Número de geometrias	Número de tentativas de tentativa de inventário
Excluir dispositivos	Lista separada por vírgulas de IDs de dispositivos ou nomes de exibição a serem excluídos

Solução de problemas

Informações adicionais sobre este Coletor de dados podem ser encontradas ["Suporte"](#) na página ou no ["Matriz de suporte do Data Collector"](#).

Configurando o coletor de dados do IBM SAN volume Controller

O coletor de dados IBM SAN volume Controller (SVC) coleta dados de inventário e desempenho usando SSH, suportando uma variedade de dispositivos que executam o sistema operacional SVC.

A lista de dispositivos suportados inclui modelos como o SVC, o v7000, o V5000 e o v3700. Consulte a matriz de suporte do Data Infrastructure Insights para ver os modelos e versões de firmware compatíveis.

Terminologia

O Data Infrastructure Insights adquire as seguintes informações de inventário do coletor de dados do IBM SVC. Para cada tipo de ativo adquirido pelo Data Infrastructure Insights, a terminologia mais comum usada para esse ativo é mostrada. Ao visualizar ou solucionar problemas desse coletor de dados, tenha em mente a seguinte terminologia:

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
Condução	Disco
Cluster	Armazenamento
Nó	Nó de storage
Grupo Mdisk	Pool de storage
VDisk	Volume
Mdisk	LUNs e caminhos de back-end

Nota: Estes são apenas mapeamentos de terminologia comuns e podem não representar todos os casos para este coletor de dados.

Requisitos de inventário

- Endereço IP de cada cluster SVC
- Porta 22 disponível
- Nome de utilizador e palavra-passe só de leitura

Requisitos de desempenho

- Console SVC, que é obrigatório para qualquer cluster SVC e necessário para o pacote de fundação de descoberta SVC.
- As credenciais exigirão nível de acesso administrativo apenas para copiar arquivos de desempenho de nós de cluster para o nó de configuração.
- Ative a coleta de dados conetando-se ao cluster SVC por SSH e executando: `Svctask startstats -interval 1`

Observação: Alternativamente, habilite a coleta de dados usando a interface do usuário de gerenciamento SVC.

Configuração

Campo	Descrição
Endereços IP do cluster	Endereços IP ou nomes de domínio totalmente qualificados do armazenamento SVC
Nome Utilizador Stock	Nome de usuário para a CLI SVC
Palavra-passe de inventário	Senha para a CLI SVC

Configuração avançada

Campo	Descrição
Intervalo de enquete de inventário (min)	Intervalo entre sondagens de inventário. O padrão é 40 minutos.
Intervalo de enquete de desempenho (seg)	Intervalo entre sondagens de desempenho. O padrão é 300 segundos.
Para limpar os arquivos de estatísticas despejados	Marque esta caixa de seleção para limpar os arquivos de estatísticas despejados

Solução de problemas

Algumas coisas para tentar se você encontrar problemas com este coletor de dados:

Problema:	Tente isto:
Erro: "O comando não pode ser iniciado porque não foi executado no nó de configuração."	O comando deve ser executado no nó de configuração.

Algumas coisas para tentar se você encontrar problemas com este coletor de dados:

Problema:	Tente isto:
Erro: "O comando não pode ser iniciado porque não foi executado no nó de configuração."	O comando deve ser executado no nó de configuração.

Informações adicionais sobre este Coletor de dados podem ser encontradas ["Suporte"](#) na página ou no ["Matriz de suporte do Data Collector"](#).

Configurando o coletor de dados IBM XIV/A9000

O coletor de dados IBM XIV e A9000 (CLI) usa a interface de linha de comando XIV para coletar dados de inventário enquanto a coleta de desempenho é realizada fazendo chamadas SMI-S para o array XIV/A9000, que executa um provedor SMI-S na porta 7778.

Terminologia

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
Disco	Disco
Sistema de storage	Armazenamento
Pool de storage	Pool de storage
Volume	Volume

Requisitos

Os seguintes requisitos devem ser atendidos para configurar e usar este coletor de dados:

- Requisito de porta: Porta TCP 7778
- Nome de utilizador e palavra-passe só de leitura

- A XIV CLI tem de ser instalada na AU

Requisitos de desempenho

Os seguintes são requisitos para a coleta de desempenho:

- Agente SMI-S 1,4 ou superior
- CIMService compatível com SMI-S rodando em array. A maioria dos arrays XIV tem um CIMServer instalado por padrão.
- O login de usuário deve ser fornecido para o CIMServer. O login deve ter acesso completo de leitura à configuração e propriedades do array.
- Namespace SMI-S. O padrão é root/ibm. Isso é configurável no CIMServer.
- Requisitos de porta: 5988 para HTTP, 5989 para HTTPS.
- Consulte o seguinte link sobre como criar uma conta para a coleção de desempenho SMI-S:
https://www.ibm.com/docs/en/products?topic=/com.ibm.tpc_V41.doc/fqz0_t_adding_cim_agent.html

Configuração

Campo	Descrição
Endereço IP XIV	Endereço IP ou nome de domínio totalmente qualificado do armazenamento XIV
Nome de utilizador	Nome de utilizador para o armazenamento XIV
Palavra-passe	Palavra-passe para o armazenamento XIV
Caminho completo para XIV diretório CLI	Caminho completo para a pasta que contém a XIV CLI
Endereço IP do host SMI-S	Endereço IP do host SMI-S.

Configuração avançada

Campo	Descrição
Intervalo de enquete de inventário (min)	Intervalo entre sondagens de inventário. O padrão é 40 minutos.
Protocolo SMI-S.	Protocolo utilizado para ligar ao fornecedor SMI-S. Também exibe a porta padrão.
Substituir a porta SMI-S.	Se estiver em branco, use a porta padrão no campo tipo de conexão; caso contrário, insira a porta de conexão a ser usada
Nome de utilizador	Nome de utilizador para o anfitrião do fornecedor SMI-S.
Palavra-passe	Palavra-passe para o anfitrião do fornecedor SMI-S.
Intervalo de enquete de desempenho (seg)	Intervalo entre sondagens de desempenho. O padrão é 300 segundos.

Solução de problemas

Informações adicionais sobre este Coletor de dados podem ser encontradas ["Suporte"](#) na página ou no ["Matriz de suporte do Data Collector"](#).

Coletor de dados Lenovo

O Data Infrastructure Insights usa o coletor de dados Lenovo para descobrir dados de inventário e desempenho para sistemas de armazenamento Lenovo HX.

Nota: Estes são apenas mapeamentos de terminologia comuns e podem não representar todos os casos para este coletor de dados.

Requisitos

- Endereço IP externo do prisma
- Nome de usuário e senha do administrador
- Requisito de porta TCP: 9440

Configuração

Campo	Descrição
Endereço IP externo do prisma	O endereço IP dos serviços de dados externos para o cluster
Nome de utilizador	Nome de usuário para a conta de administrador
Palavra-passe	Palavra-passe para a conta de administrador

Configuração avançada

Campo	Descrição
Porta de TCP	Porta TCP usada para conectar ao array. A predefinição é 9440.
Intervalo de pesquisa de inventário (min)	Intervalo entre sondagens de inventário. O padrão é 60 minutos.
Intervalo de pesquisa de desempenho (seg)	Intervalo entre sondagens de desempenho. O padrão é 300 segundos.

Solução de problemas

Informações adicionais sobre este Coletor de dados podem ser encontradas ["Suporte"](#) na página ou no ["Matriz de suporte do Data Collector"](#).

Microsoft

Configurar o coletor de dados Azure NetApp Files

O Data Infrastructure Insights usa o coletor de dados Azure NetApp Files para adquirir dados de inventário e performance.

Requisitos

Você precisa das seguintes informações para configurar este coletor de dados.

- Requisito de porta: 443 HTTPS
- IP REST do Gerenciamento do Azure (management.azure.com)
- ID de cliente principal do serviço Azure (conta de utilizador)
- Chave de autenticação principal do serviço Azure (senha do usuário)
- Você precisa configurar uma conta do Azure para a descoberta do Data Infrastructure Insights.

Depois que a conta estiver configurada corretamente e você Registrar o aplicativo no Azure, você terá as credenciais necessárias para descobrir a instância do Azure com o Data Infrastructure Insights. O link a seguir descreve como configurar a conta para descoberta:

<https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal>

Configuração

Insira os dados nos campos do coletor de dados de acordo com a tabela abaixo:

Campo	Descrição
ID Cliente Principal do Serviço Azure	ID de início de sessão no Azure
ID do Locatário do Azure	ID do Locatário do Azure
Chave de autenticação principal do serviço Azure	Chave de autenticação de login
Eu entendo que a Microsoft me cobra por solicitações de API	Verifique isso para verificar se a Microsoft cobra solicitações de API feitas pela polling do Insight.

Configuração avançada

Campo	Descrição
Intervalo de enquete de inventário (min)	A predefinição é 60

Solução de problemas

- As credenciais usadas pelo coletor de dados do ANF precisam ter acesso a todas as assinaturas do Azure que contenham volumes do ANF.
- Se o acesso ao Reader causar falha na coleção de desempenho, tente conceder acesso ao colaborador em um nível de grupo de recursos.

Informações adicionais sobre este Coletor de dados podem ser encontradas "[Suporte](#)" na página ou no "[Matriz de suporte do Data Collector](#)".

Coletor de dados Microsoft Hyper-V.

O coletor de dados Microsoft Hyper-V adquire dados de inventário e desempenho do ambiente de computação de servidor virtualizado. Este coletor de dados pode descobrir um host Hyper-V autônomo ou um cluster inteiro - criar um coletor por host ou cluster autônomo.

Terminologia

O Data Infrastructure Insights adquire as seguintes informações de inventário do Microsoft Hyper-V (WMI). Para cada tipo de ativo adquirido pelo Data Infrastructure Insights, a terminologia mais comum usada para esse ativo é mostrada. Ao visualizar ou solucionar problemas desse coletor de dados, tenha em mente a seguinte terminologia:

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
Disco rígido virtual	Disco virtual
Host	Host
Máquina virtual	Máquina virtual
Volumes compartilhados de cluster (CSV), volume da partição	Armazenamento de dados
Internet SCSI Device, Multi Path SCSI LUN	LUN
Porta Fibre Channel	Porta

Nota: Estes são apenas mapeamentos de terminologia comuns e podem não representar todos os casos para este coletor de dados.

Requisitos

Para configurar este coletor de dados, são necessários os seguintes itens:

- O Hyper-V requer a porta 5985 aberta para coleta de dados e acesso/gerenciamento remoto.
- Endereço IP ou FQDN do cluster ou hipervisor autônomo. Usar o nome de host ou IP do cluster flutuante é provavelmente a abordagem mais confiável em comparação com apontar o coletor em apenas um nó específico em um cluster.
- Conta de usuário de nível administrativo que funciona em todos os hipervisores no cluster.
- O WinRM precisa ser ativado e ouvir em todos os hipervisores
- Requisitos de porta: Porta 135 via WMI e portas TCP dinâmicas atribuídas 1024-65535 para Windows 2003 e anterior e 49152-65535 para Windows 2008.
- A resolução DNS deve ser bem-sucedida, mesmo que o coletor de dados seja apontado apenas para um endereço IP
- Cada hypervisor do Hyper-V deve ter a "Monitoração de recursos" ativada para cada VM, em cada host. Isso permite que cada hipervisor tenha mais dados disponíveis para o Data Infrastructure Insights em cada convidado. Se isso não for definido, menos métricas de desempenho serão adquiridas para cada convidado. Mais informações sobre a medição de recursos podem ser encontradas na documentação da Microsoft:

["Visão geral da Monitoração de recursos do Hyper-V"](#)

["Enable-VMResourceMetering \(Ativar-VMResourceMetering\)"](#)



O coletor de dados Hyper-V requer uma Unidade de aquisição do Windows.

Configuração

Campo	Descrição
Endereço IP do cluster ou FQDN do cluster flutuante	O endereço IP ou o nome de domínio totalmente qualificado para o cluster ou um hypervisor autônomo não agrupado
Nome de utilizador	Nome de usuário do administrador para o hypervisor
Palavra-passe	Palavra-passe para o hipervisor
Sufixo de domínio DNS	O sufixo hostname que combina com o hostname simples para renderizar o FQDN de um hypervisor

Configuração avançada

Campo	Descrição
Intervalo de enquete de inventário (min)	O padrão é 20 minutos.

Solução de problemas

Informações adicionais sobre este Coletor de dados podem ser encontradas ["Suporte"](#) na página ou no ["Matriz de suporte do Data Collector"](#).

NetApp

Coletor de dados NetApp Cloud Volumes ONTAP

Este coletor de dados suporta a coleta de inventário a partir de configurações do Cloud Volumes ONTAP.

Configuração

Campo	Descrição
Endereço IP de gerenciamento do NetApp	Endereço IP para Cloud Volumens ONTAP
Nome de utilizador	Nome de usuário para Cloud Volumes ONTAP
Palavra-passe	Senha para o usuário acima

Configuração avançada

Campo	Descrição
Tipo de ligação	HTTPS recomendado. Também mostra a porta padrão.
Substituir porta de comunicação	Porta a usar se não for padrão.
Intervalo de enquete de inventário (min)	O padrão é de 60 minutos.
Contagem de threads concorrente Stock	Número de threads simultâneos.
Forçar TLS para HTTPS	Forçar TLS em HTTPS

Campo	Descrição
Procurar automaticamente Netgroups	Procurar automaticamente Netgroups
Expansão do netgroup	Selecione Shell ou Arquivo
HTTP read timeout segundos	O padrão é de 30 segundos
Forçar respostas como UTF-8	Forçar respostas como UTF-8
Intervalo de enquete de desempenho (min)	O padrão é de 900 segundos.
Contagem de threads concorrente de desempenho	Número de threads simultâneos.
Coleta avançada de dados de contador	Verifique isso para que o Data Infrastructure Insights colete as métricas avançadas da lista abaixo.

Solução de problemas

Informações adicionais sobre este Coletor de dados podem ser encontradas ["Suporte"](#) na página ou no ["Matriz de suporte do Data Collector"](#).

NetApp Cloud volumes Services para coletor de dados da AWS

Esse coletor de dados dá suporte à coleta de inventário no NetApp Cloud volumes Services para configurações da AWS.

Configuração

Campo	Descrição
Região do Cloud volumes	Região do NetApp Cloud volumes Services para AWS
Chave API	Chave da API do Cloud volumes
Chave secreta	Chave secreta do Cloud volumes

Configuração avançada

Campo	Descrição
Intervalo de enquete de inventário (min)	O padrão é de 60 minutos

Solução de problemas

Algumas coisas para tentar se você encontrar problemas com este coletor de dados:

Problema:	Tente isto:
Recebi um erro semelhante a este: 'Falha ao executar solicitação: Conectar ao endpoint da região AWS>:8080 [endpoint da região AWS>/IP do endpoint da região AWS>] falhou: Conectar o tempo limite: OBTER endpoint da região do https://<AWS FQDN>:8080/v1/Storage/IPRanges HTTP/1,1'	O "proxy" usado pelo Data Infrastructure Insights para se comunicar com a Unidade de aquisição não se comunica entre o Data Infrastructure Insights e o próprio Data Collector. Aqui estão algumas coisas que você pode tentar: Certifique-se de que a unidade de aquisição é capaz de resolver o fqdn e alcançar a porta necessária. Confirme se um proxy não é necessário para alcançar o ponto final especificado na mensagem de erro. O curl pode ser usado para testar a comunicação entre a unidade de aquisição e o endpoint. Certifique-se de que você está não usando um Proxy para este teste. Curl -s -H accept:Application/json -H "content-type: Application/json" -H api-key: Chave do cliente usada nas credenciais do coletor de dados -H segredo-chave: Chave secreta do cliente usada nas credenciais do coletor de dados> -X GET https://<AWS endpoint regional>:8080/v1/Storage/IPRanges Veja isso " artigo da KB do NetApp ".

Informações adicionais sobre este Coletor de dados podem ser encontradas "[Suporte](#)" na página ou no "[Matriz de suporte do Data Collector](#)".

Coletor de dados do software de gerenciamento de dados NetApp ONTAP

Esse coletor de dados adquire dados de inventário e desempenho de sistemas de storage que executam o ONTAP usando chamadas de API somente leitura de uma conta do ONTAP. Esse coletor de dados também cria um Registro no Registro de aplicativos de cluster para acelerar o suporte.

Terminologia

O Data Infrastructure Insights adquire dados de inventário e desempenho do coletor de dados do ONTAP. Para cada tipo de ativo adquirido, a terminologia mais comum usada para o ativo é mostrada. Ao visualizar ou solucionar problemas desse coletor de dados, tenha em mente a seguinte terminologia:

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
Disco	Disco
Grupo RAID	Grupo de discos
Cluster	Armazenamento
Nó	Nó de storage
Agregado	Pool de storage
LUN	Volume
Volume	Volume interno

Terminologia de gerenciamento de dados do ONTAP

Os termos a seguir se aplicam a objetos ou referências que você pode encontrar nas páginas iniciais de ativos de storage do ONTAP Data Management. Muitos desses termos também se aplicam a outros coletores de dados.

Armazenamento

- Modelo – Uma lista delimitada por vírgulas dos nomes de modelo de nó único e discreto dentro deste cluster. Se todos os nós nos clusters forem do mesmo tipo de modelo, apenas um nome de modelo aparecerá.
- Fornecedor – mesmo nome do fornecedor que você veria se você estivesse configurando uma nova fonte de dados.
- Número de série – o número de série da matriz. Em sistemas de storage de arquitetura de cluster, como o ONTAP Data Management, esse número de série pode ser menos útil do que os números de série individuais "nós de storage".
- IP – geralmente serão os IP (s) ou nome de host (s) conforme configurado na fonte de dados.
- Versão de microcódigo – firmware.
- Capacidade bruta – soma de base 2 de todos os discos físicos no sistema, independentemente da sua função.
- Latência – uma representação do que o host enfrenta cargas de trabalho, tanto na leitura quanto na gravação. Idealmente, o Data Infrastructure Insights está fornecendo esse valor diretamente, mas isso geralmente não é o caso. Em vez do array que oferece isso, o Data Infrastructure Insights geralmente está executando um cálculo ponderado por IOPs derivado das estatísticas individuais de volumes internos.
- Taxa de transferência – agregada a partir de volumes internos. Gerenciamento – isso pode conter um hiperlink para a interface de gerenciamento do dispositivo. Criado programaticamente pela fonte de dados Data Infrastructure Insights como parte dos relatórios de inventário.

Pool de storage

- Armazenamento – em que storage esse pool vive. Obrigatório.
- Tipo – um valor descritivo de uma lista de uma lista enumerada de possibilidades. Mais comumente será "agregado" ou "RAID Group".
- Nó – se a arquitetura desse storage array for tal que os pools pertençam a um nó de armazenamento específico, seu nome será visto aqui como um hiperlink para sua própria página inicial.
- Usa Flash Pool – valor Sim/não – este pool baseado em SATA/SAS tem SSDs usados para aceleração de cache?
- Redundância – nível RAID ou esquema de proteção. RAID_DP é paridade dupla, RAID_TP é paridade tripla.
- Capacidade – os valores aqui são a capacidade lógica usada, utilizável e a capacidade total lógica, e a porcentagem usada entre eles.
- Capacidade sobrecomprometida – se, usando tecnologias de eficiência, você tiver alocado uma soma total de capacidades de volume ou volume interno maior que a capacidade lógica do pool de storage, o valor percentual aqui será maior que 0%.
- Snapshot – capacidades de snapshot usadas e totais, se a arquitetura do seu pool de armazenamento dedicar parte da sua capacidade a segmentos de áreas exclusivamente para snapshots. As configurações do ONTAP em MetroCluster provavelmente exibirão isso, enquanto outras configurações do ONTAP são menores.

- Utilização – um valor percentual que mostra a maior porcentagem de ocupado em disco de qualquer disco que contribui com a capacidade para esse pool de armazenamento. A utilização de disco não tem necessariamente uma forte correlação com o desempenho do array – a utilização pode ser alta devido a recompilações de disco, atividades de deduplicação, etc., na ausência de cargas de trabalho orientadas pelo host. Além disso, as implementações de replicação de muitos arrays podem aumentar a utilização de disco, sem serem exibidas como volume interno ou workload de volume.
- IOPS – a soma de IOPs de todos os discos que contribuem com capacidade para esse pool de storage. Taxa de transferência – a taxa de transferência soma de todos os discos que contribuem para a capacidade deste pool de armazenamento.

Nó de storage

- Armazenamento – em que storage array esse nó faz parte. Obrigatório.
- Parceiro HA – em plataformas onde um nó fará failover para um e apenas um outro nó, ele geralmente será visto aqui.
- Estado – saúde do nó. Disponível apenas quando o array estiver saudável o suficiente para ser inventariado por uma fonte de dados.
- Modelo – nome do modelo do nó.
- Versão – nome da versão do dispositivo.
- Número de série – o número de série do nó.
- Memória – memória base 2, se disponível.
- Utilização – no ONTAP, este é um índice de tensão do controlador de um algoritmo proprietário. Em cada pesquisa de desempenho, um número entre 0 e 100% será relatado que é o maior da contenção de disco WAFL ou da utilização média da CPU. Se você observar valores sustentados > 50%, isso é indicativo de subdimensionamento – potencialmente, um controlador/nó não é grande o suficiente ou não discos giratórios suficientes para absorver a carga de trabalho de gravação.
- IOPS – derivado diretamente das chamadas ZAPI do ONTAP no objeto do nó.
- Latência – derivada diretamente das chamadas ZAPI do ONTAP no objeto do nó.
- Taxa de transferência – derivada diretamente das chamadas ZAPI do ONTAP no objeto do nó.
- Processadores – contagem de CPU.

Requisitos

A seguir estão os requisitos para configurar e usar este coletor de dados:

- Você deve ter acesso a uma conta de administrador configurada para chamadas de API somente leitura.
- Os detalhes da conta incluem nome de usuário e senha.
- Requisitos do porto: 80 ou 443
- Permissões da conta:
 - Nome da função somente leitura para o aplicativo ontapi para o SVM padrão
 - Você pode exigir permissões de gravação opcionais adicionais. Consulte a Nota sobre permissões abaixo.
- Requisitos de licença do ONTAP:
 - Licença FCP e volumes mapeados/mascarados necessários para descoberta de Fibre Channel

Requisitos de permissão para coletar métricas de switch ONTAP

Insights de infraestrutura de dados tem a capacidade de coletar dados de switch de cluster do ONTAP como uma opção nas configurações do coletor [Configuração avançada](#). Além de habilitar isso no coletor de informações de infraestrutura de dados, você também deve **configurar o próprio sistema ONTAP** para fornecer "[informações do interruptor](#)" e garantir que os dados corretos [permissões](#) estejam definidos, a fim de permitir que os dados do switch sejam enviados para informações de infraestrutura de dados.

Configuração

Campo	Descrição
IP de gerenciamento de NetApp	Endereço IP ou nome de domínio totalmente qualificado do cluster NetApp
Nome de utilizador	Nome de usuário para cluster NetApp
Palavra-passe	Palavra-passe para cluster NetApp

Configuração avançada

Campo	Descrição
Tipo de ligação	Escolha HTTP (porta padrão 80) ou HTTPS (porta padrão 443). O padrão é HTTPS
Substituir porta de comunicação	Especifique uma porta diferente se você não quiser usar o padrão
Intervalo de enquete de inventário (min)	O padrão é de 60 minutos.
Para TLS para HTTPS	Permitir TLS apenas como protocolo ao usar HTTPS
Procurar automaticamente Netgroups	Ative as pesquisas automáticas de netgroup para regras de política de exportação
Expansão do netgroup	Estratégia de expansão do netgroup. Escolha <i>file</i> ou <i>shell</i> . O padrão é <i>shell</i> .
HTTP read timeout segundos	A predefinição é 30
Forçar respostas como UTF-8	Força o código coletor de dados a interpretar as respostas da CLI como estando em UTF-8
Intervalo de enquete de desempenho (seg)	O padrão é de 900 segundos.
Coleta avançada de dados de contador	Ative a integração com o ONTAP. Selecione esta opção para incluir os dados do Contador Avançado do ONTAP em enquetes. Escolha os contadores desejados na lista.

Campo	Descrição
Métricas de switch de cluster	Permita que o Data Infrastructure Insights colete dados do switch de cluster. Observe que, além de habilitá-lo no lado Insights de infraestrutura de dados, você também deve configurar o sistema ONTAP para fornecer "informações do interruptor" e garantir que os dados corretos permissões estejam definidos, a fim de permitir que os dados do switch sejam enviados para Insights de infraestrutura de dados. Consulte "uma nota sobre permissões" abaixo.

Métricas de potência do ONTAP

Vários modelos do ONTAP fornecem métricas de potência para Insights de infraestrutura de dados que podem ser usados para monitoramento ou alerta. As listas de modelos suportados e não suportados abaixo não são abrangentes, mas devem fornecer alguma orientação; em geral, se um modelo estiver na mesma família que um na lista, o suporte deve ser o mesmo.

Modelos suportados:

A200 A220 A250 A300 A320 A400 A700 A700S A800 A900 C190 FAS2240-4 FAS2552 FAS2650 FAS2720 FAS2750 FAS8200 FAS8300 FAS8700 FAS9000

Modelos não suportados:

FAS2620 FAS3250 FAS3270 FAS500f FAS6280 FAS/AFF 8020 FAS/AFF 8040 FAS/AFF 8060 FAS/AFF 8080

Uma Nota sobre permissões

Como vários painéis do ONTAP do Insights de infraestrutura de dados dependem de contadores avançados do ONTAP, você deve habilitar **coleta avançada de dados de contador** na seção Configuração avançada do coletor de dados.

Você também deve garantir que a permissão de gravação para a API do ONTAP esteja habilitada. Isso normalmente requer uma conta no nível do cluster com as permissões necessárias.

Para criar uma conta local para Insights de infraestrutura de dados no nível do cluster, faça login no ONTAP com o nome de usuário/senha do administrador de gerenciamento de cluster e execute os seguintes comandos no servidor ONTAP:

1. Antes de começar, você deve estar conectado ao ONTAP com uma conta *Administrador* e comandos de *nível de diagnóstico* devem estar ativados.
2. Crie uma função somente leitura usando os seguintes comandos.

```
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. Crie o usuário somente leitura usando o seguinte comando. Depois de executar o comando Create, você será solicitado a digitar uma senha para esse usuário.

```
security login create -username ci_user -application ontapi
-authentication-method password -role ci_readonly
```

Se a conta AD/LDAP for usada, o comando deve ser

```
security login create -user-or-group-name DOMAIN\aduser/adgroup
-application ontapi -authentication-method domain -role ci_readonly
Se estiver a recolher dados do comutador de cluster:
```

```
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
```

A função resultante e o login do usuário serão parecidos com o seguinte. Sua saída real pode variar:

```
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
```



Se o controle de acesso do ONTAP não estiver definido corretamente, as chamadas REST do Insights de infraestrutura de dados podem falhar, resultando em lacunas nos dados do dispositivo. Por exemplo, se você ativou-o no coletor Insights de infraestrutura de dados, mas não configurou as permissões no ONTAP, a aquisição falhará. Além disso, se a função for definida anteriormente no ONTAP e você estiver adicionando as habilidades da API REST, certifique-se de que *http* seja adicionado à função.

Solução de problemas

Algumas coisas para tentar se você encontrar problemas com este coletor de dados:

Inventário

Problema:	Tente isto:
Receber 401 resposta HTTP ou 13003 código de erro ZAPI e ZAPI retorna "insuficiente Privileges" ou "não autorizado para este comando"	Verifique o nome de usuário e a senha e o Privileges/permissões do usuário.
A versão do cluster é inferior a 8,1	A versão mínima suportada do cluster é 8,1. Atualize para a versão mínima suportada.
ZAPI retorna "a função de cluster não é cluster_mgmt LIF"	A UA precisa falar com o IP de gerenciamento de cluster. Verifique o IP e mude para um IP diferente, se necessário
Erro: "Os filers do modo 7 não são suportados"	Isso pode acontecer se você usar esse coletor de dados para descobrir o arquivador de modo 7D. Em vez disso, altere o IP para apontar para o cluster cdot.
O comando ZAPI falha após a tentativa	A AU tem problema de comunicação com o cluster. Verifique a rede, o número da porta e o endereço IP. O usuário também deve tentar executar um comando da linha de comando da máquina AU.
Falha ao conectar-se ao ZAPI via HTTP	Verifique se a porta ZAPI aceita texto simples. Se AU tentar enviar texto simples para um soquete SSL, a comunicação falha.
A comunicação falha com SSLException	Au está tentando enviar SSL para uma porta de texto simples em um arquivador. Verifique se a porta ZAPI aceita SSL ou se usa uma porta diferente.
Erro de conexão adicional: A resposta ZAPI tem o código de erro 13001, "banco de dados não está aberto" o código de erro ZAPI é 60 e a resposta contém "API não terminou no tempo" resposta ZAPI contém "inicializar_sessão() ambiente NULL retornado o código de erro ZAPI é 14007 e a resposta contém "nó não está saudável"	Verifique a rede, o número da porta e o endereço IP. O usuário também deve tentar executar um comando da linha de comando da máquina AU.

Desempenho

Problema:	Tente isto:
Erro "Falha ao coletar o desempenho do ZAPI"	Isso geralmente se deve ao fato de que o perf stat não está sendo executado. Tente o seguinte comando em cada nó: <pre>> system node systemshell -node * -command "spmctl -h cmd --stop; spmctl -h cmd --exec"</pre>

Informações adicionais podem ser encontradas na ["Suporte"](#) página ou no ["Matriz de suporte do Data Collector"](#).

Coletor de DADOS REST do NetApp ONTAP

Esse coletor de dados adquire inventário, logs do EMS e dados de desempenho de sistemas de armazenamento que executam o ONTAP 9.14,1 ou superior usando chamadas de API REST. Para sistemas ONTAP em versões anteriores, use o tipo coletor "NetApp ONTAP Data Management Software" baseado em ZAPI.



O coletor REST ONTAP pode ser usado como um substituto para o coletor baseado em ONTAPI anterior. Como tal, pode haver diferenças nas métricas que são coletadas ou relatadas. Para obter mais informações sobre as diferenças entre ONTAPI e REST, consulte "[ONTAP 9.14,1 mapeamento ONTAPI-to-REST](#)" a documentação.

Requisitos

A seguir estão os requisitos para configurar e usar este coletor de dados:

- Tem de ter acesso a uma conta de utilizador com o nível de acesso necessário. Observe que as permissões de administrador são necessárias ao criar um novo usuário/função REST.
 - Funcionalmente, o Insights de infraestrutura de dados faz principalmente solicitações de leitura, mas algumas permissões de gravação são necessárias para que o Insights de infraestrutura de dados registre-se no array ONTAP. Veja a *Nota sobre permissões* imediatamente abaixo.
- ONTAP versão 9.14.1 ou superior.
- Requisitos do porto: 443

Uma Nota sobre permissões

Como vários painéis do ONTAP do Insights de infraestrutura de dados dependem de contadores avançados do ONTAP, você deve manter **Ativar coleta avançada de dados de contador** habilitado na seção Configuração avançada do coletor de dados.

Para criar uma conta local para Insights de infraestrutura de dados no nível do cluster, faça login no ONTAP com o nome de usuário/senha do administrador de gerenciamento de cluster e execute os seguintes comandos no servidor ONTAP:

1. Antes de começar, você deve estar conectado ao ONTAP com uma conta *Administrador* e comandos de *nível de diagnóstico* devem estar ativados.
2. Recupere o nome do vserver do tipo *admin*. Você usará esse nome em comandos subsequentes.

```
vserver show -type admin  
. Crie uma função usando os seguintes comandos:
```

```

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. Crie o usuário somente leitura usando o seguinte comando. Depois de executar o comando Create, você será solicitado a digitar uma senha para esse usuário.

```

security login create -username ci_user -application http
-authentication-method password -role ci_readonly

```

Se a conta AD/LDAP for usada, o comando deve ser

```

security login create -user-or-group-name DOMAIN\aduser/adgroup
-application http -authentication-method domain -role ci_readonly

```

A função resultante e o login do usuário serão parecidos com o seguinte. Sua saída real pode variar:

```

security login rest-role show -vserver <vserver name> -role restRole

```

Vserver	Role Name	API	Access 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>

User/Group	Authentication	Acct	Second
Name	Application Method	Role Name	Locked Method
restUser	http password	restRole	no none

Migração

Para migrar de um coletor de dados ONTAP (ontapi) anterior para o coletor REST ONTAP mais recente, faça o seguinte:

1. Adicione o RESTO DO coletor. Recomenda-se inserir informações para um usuário diferente do configurado para o coletor anterior. Por exemplo, use o usuário anotado na seção permissões acima.
2. Pausar o coletor anterior, para que ele não continue a coletar dados.
3. Deixe o novo coletor DE REPOUSO adquirir dados durante, pelo menos, 30 minutos. Ignore quaisquer dados durante este período que não pareçam "normais".
4. Após o período de repouso, você deve ver seus dados estabilizados à medida que o coletor DE REPOUSO continua a adquirir.

Você pode usar esse mesmo processo para retornar ao coletor anterior, se desejar.

Configuração

Campo	Descrição
Endereço IP de gerenciamento do ONTAP	Endereço IP ou nome de domínio totalmente qualificado do cluster NetApp. Deve ser IP/FQDN de gerenciamento de cluster.
Nome de utilizador REST do ONTAP	Nome de usuário para cluster NetApp
Palavra-passe REST do ONTAP	Palavra-passe para cluster NetApp

Configuração avançada

Campo	Descrição
Intervalo de enquete de inventário (min)	O padrão é de 60 minutos.
Intervalo de enquete de desempenho (seg)	O padrão é de 60 segundos.
Coleta avançada de dados de contador	Selecione esta opção para incluir os dados do Contador Avançado do ONTAP em enquetes. Ativado por predefinição.
Ativar a coleção de eventos EMS	Selecione esta opção para incluir dados de eventos de registo EMS do ONTAP. Ativado por predefinição.
Intervalo da sondagem EMS (seg)	O padrão é de 60 segundos.

Terminologia

O Data Infrastructure Insights adquire inventário, logs e dados de desempenho do coletor de dados do ONTAP. Para cada tipo de ativo adquirido, a terminologia mais comum usada para o ativo é mostrada. Ao visualizar ou solucionar problemas desse coletor de dados, tenha em mente a seguinte terminologia:

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
Disco	Disco
Grupo RAID	Grupo de discos
Cluster	Armazenamento

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
Nó	Nó de storage
Agregado	Pool de storage
LUN	Volume
Volume	Volume interno
Storage Virtual Machine/SVM	Storage Virtual Machine

Terminologia de gerenciamento de dados do ONTAP

Os termos a seguir se aplicam a objetos ou referências que você pode encontrar nas páginas iniciais de ativos de storage do ONTAP Data Management. Muitos desses termos também se aplicam a outros coletores de dados.

Armazenamento

- Modelo – Uma lista delimitada por vírgulas dos nomes de modelo de nó único e discreto dentro deste cluster. Se todos os nós nos clusters forem do mesmo tipo de modelo, apenas um nome de modelo aparecerá.
- Fornecedor – mesmo nome do fornecedor que você veria se você estivesse configurando uma nova fonte de dados.
- Número de série – o UUID da matriz
- IP – geralmente serão os IP (s) ou nome de host (s) conforme configurado na fonte de dados.
- Versão de microcódigo – firmware.
- Capacidade bruta – soma de base 2 de todos os discos físicos no sistema, independentemente da sua função.
- Latência – uma representação do que o host enfrenta cargas de trabalho, tanto na leitura quanto na gravação. Idealmente, o Data Infrastructure Insights está fornecendo esse valor diretamente, mas isso geralmente não é o caso. Em vez do array que oferece isso, o Data Infrastructure Insights geralmente está executando um cálculo ponderado por IOPs derivado das estatísticas individuais de volumes internos.
- Taxa de transferência – agregada a partir de volumes internos. Gerenciamento – isso pode conter um hiperlink para a interface de gerenciamento do dispositivo. Criado programaticamente pela fonte de dados Data Infrastructure Insights como parte dos relatórios de inventário.

Pool de storage

- Armazenamento – em que storage esse pool vive. Obrigatório.
- Tipo – um valor descritivo de uma lista de uma lista enumerada de possibilidades. Mais comumente será "agregado" ou "RAID Group".
- Nó – se a arquitetura desse storage array for tal que os pools pertençam a um nó de armazenamento específico, seu nome será visto aqui como um hiperlink para sua própria página inicial.
- Usa Flash Pool – valor Sim/não – este pool baseado em SATA/SAS tem SSDs usados para aceleração de cache?
- Redundância – nível RAID ou esquema de proteção. RAID_DP é paridade dupla, RAID_TP é paridade tripla.
- Capacidade – os valores aqui são a capacidade lógica usada, utilizável e a capacidade total lógica, e a

porcentagem usada entre eles.

- Capacidade sobrecomprometida – se, usando tecnologias de eficiência, você tiver alocado uma soma total de capacidades de volume ou volume interno maior que a capacidade lógica do pool de storage, o valor percentual aqui será maior que 0%.
- Snapshot – capacidades de snapshot usadas e totais, se a arquitetura do seu pool de armazenamento dedicar parte da sua capacidade a segmentos de áreas exclusivamente para snapshots. As configurações do ONTAP em MetroCluster provavelmente exibirão isso, enquanto outras configurações do ONTAP são menores.
- Utilização – um valor percentual que mostra a maior porcentagem de ocupado em disco de qualquer disco que contribui com a capacidade para esse pool de armazenamento. A utilização de disco não tem necessariamente uma forte correlação com o desempenho do array – a utilização pode ser alta devido a recompilações de disco, atividades de deduplicação, etc., na ausência de cargas de trabalho orientadas pelo host. Além disso, as implementações de replicação de muitos arrays podem aumentar a utilização de disco, sem serem exibidas como volume interno ou workload de volume.
- IOPS – a soma de IOPs de todos os discos que contribuem com capacidade para esse pool de storage. Taxa de transferência – a taxa de transferência soma de todos os discos que contribuem para a capacidade deste pool de armazenamento.

Nó de storage

- Armazenamento – em que storage array esse nó faz parte. Obrigatório.
- Parceiro HA – em plataformas onde um nó fará failover para um e apenas um outro nó, ele geralmente será visto aqui.
- Estado – saúde do nó. Disponível apenas quando o array estiver saudável o suficiente para ser inventariado por uma fonte de dados.
- Modelo – nome do modelo do nó.
- Versão – nome da versão do dispositivo.
- Número de série – o número de série do nó.
- Memória – memória base 2, se disponível.
- Utilização – no ONTAP, este é um índice de tensão do controlador de um algoritmo proprietário. Em cada pesquisa de desempenho, um número entre 0 e 100% será relatado que é o maior da contenção de disco WAFL ou da utilização média da CPU. Se você observar valores sustentados > 50%, isso é indicativo de subdimensionamento – potencialmente, um controlador/nó não é grande o suficiente ou não discos giratórios suficientes para absorver a carga de trabalho de gravação.
- IOPS – derivado diretamente das chamadas REST do ONTAP no objeto do nó.
- Latência – derivada diretamente das CHAMADAS REST do ONTAP no objeto nó.
- Taxa de transferência – derivada diretamente das CHAMADAS REST do ONTAP no objeto nó.
- Processadores – contagem de CPU.

Métricas de potência do ONTAP

Vários modelos do ONTAP fornecem métricas de potência para Insights de infraestrutura de dados que podem ser usados para monitoramento ou alerta. As listas de modelos suportados e não suportados abaixo não são abrangentes, mas devem fornecer alguma orientação; em geral, se um modelo estiver na mesma família que um na lista, o suporte deve ser o mesmo.

Modelos suportados:

A200 A220 A250 A300 A320 A400 A700 A700S A800 A900 C190 FAS2240-4 FAS2552 FAS2650 FAS2720 FAS2750 FAS8200 FAS8300 FAS8700 FAS9000

Modelos não suportados:

FAS2620 FAS3250 FAS3270 FAS500f FAS6280 FAS/AFF 8020 FAS/AFF 8040 FAS/AFF 8060 FAS/AFF 8080

Solução de problemas

Algumas coisas para tentar se você encontrar problemas com este coletor de dados:

Problema:	Tente isto:
Ao tentar criar um coletor de DADOS REST do ONTAP, um erro como o seguinte é visto: Configuração: 10.193.70.14: API REST do ONTAP em 10.193.70.14 não está disponível: 10.193.70.14 falha ao OBTER /api/cluster: 400 solicitação incorreta	Isso é provavelmente devido a um array ONTAP (oldeer), por exemplo, ONTAP 9.6) que não tem recursos de API REST. O ONTAP 9.14,1 é a versão mínima do ONTAP suportada pelo coletor REST do ONTAP. As respostas "400 Bad Request" devem ser esperadas em versões pré-REST do ONTAP. Para versões do ONTAP que suportam REST, mas não são 9.14.1 ou posterior, você pode ver a seguinte mensagem semelhante: Configuração: 10.193.98.84: API REST do ONTAP em 10.193.98.84 não está disponível: 10.193.98.84: API REST do ONTAP em 10.193.98.84 está disponível: cheryl5-cluster-2 9.10.1 a3cb3247-3d3c-11ee-8ff3-005056b364a7 mas não tem a versão mínima 9.14.1.
Vejo métricas vazias ou "0" onde o coletor ONTAP ontapi mostra dados.	O ONTAP REST não relata métricas que são usadas internamente apenas no sistema ONTAP. Por exemplo, agregados de sistema não serão coletados pelo ONTAP REST, somente os SVM do tipo "dados" serão coletados. Outros exemplos de métricas REST do ONTAP que podem relatar dados zero ou vazios: InternalVolumes: REST já não relata vol0. Agregados: O RESTO não relata mais aggr0. Armazenamento: A maioria das métricas é um conjunto de métricas de volume interno e será afetada pelo acima. Máquinas virtuais de armazenamento: O REST não relata mais SVM's do tipo diferente de 'data' (por exemplo, 'cluster', 'gmt', 'nó'). Você também pode notar uma alteração na aparência dos gráficos que têm dados, devido à alteração no período de sondagem de desempenho padrão de 15 minutos para 5 minutos. Polling mais frequente significa mais pontos de dados para plotar.

Informações adicionais podem ser encontradas na ["Suporte"](#) página ou no ["Matriz de suporte do Data Collector"](#).

NetApp Data ONTAP operando no coletor de dados de 7 modos

Para sistemas de storage que usam o software Data ONTAP operando no modo 7, você usa o coletor de dados de 7 modos, que usa a CLI para obter dados de capacidade e

performance.

Terminologia

O Data Infrastructure Insights adquire as seguintes informações de inventário do coletor de dados do modo 7 do NetApp. Para cada tipo de ativo adquirido, a terminologia mais comum usada para esse ativo é mostrada. Ao visualizar ou solucionar problemas desse coletor de dados, tenha em mente a seguinte terminologia:



Este coletor de dados é "obsoleto".

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
Disco	Disco
Grupo RAID	Grupo de discos
Arquivador	Armazenamento
Arquivador	Nó de storage
Agregado	Pool de storage
LUN	Volume
Volume	Volume interno

Nota: Estes são apenas mapeamentos de terminologia comuns e podem não representar todos os casos para este coletor de dados.

Requisitos

Você precisa do seguinte para configurar e usar este coletor de dados:

- Endereços IP do controlador de storage e do parceiro FAS.
- Porta 443
- Um nome de usuário e senha personalizados no nível de administrador para controlador e controlador de parceiro com os seguintes recursos de função para o modo 7:
 - "api-*": Use isso para permitir que o OnCommand Insight execute todos os comandos da API de armazenamento NetApp.
 - "Login-http-admin": Use isso para permitir que o OnCommand Insight se conecte ao armazenamento NetApp via HTTP.
 - "Security-API-vFiler": Use isso para permitir que o OnCommand Insight execute comandos da API de armazenamento NetApp para recuperar informações da unidade do vFiler.
 - "cli-options": Use isso para ler as opções do sistema de armazenamento.
 - "cli-lun": Acesse esses comandos para gerenciar LUNs. Exibe o status (caminho de LUN, tamanho, estado online/offline e estado compartilhado) do LUN ou classe de LUNs fornecidos.
 - "cli-df": Use isso para exibir espaço livre em disco.
 - "cli-ifconfig": Use isso para exibir interfaces e endereços IP.

Configuração

Campo	Descrição
Endereço do sistema de armazenamento	Endereço IP ou nome de domínio totalmente qualificado para o sistema de armazenamento NetApp
Nome de utilizador	Nome de usuário do sistema de storage NetApp
Palavra-passe	Palavra-passe para o sistema de armazenamento NetApp
Endereço do parceiro de HA no cluster	Endereço IP ou nome de domínio totalmente qualificado para o parceiro HA
Nome de usuário do parceiro de HA no cluster	Nome de usuário do parceiro HA
Senha do HA Partner Filer no cluster	Senha para o parceiro HA

Configuração avançada

Campo	Descrição
Intervalo de enquete de inventário (min)	Intervalo entre sondagens de inventário. O padrão é 20 minutos.
Tipo de ligação	HTTPS ou HTTP, também exibe a porta padrão
Substituir porta de ligação	Se estiver em branco, use a porta padrão no campo tipo de conexão; caso contrário, insira a porta de conexão a ser usada
Intervalo de enquete de desempenho (seg)	Intervalo entre sondagens de desempenho. O padrão é 300 segundos.

Conexão de sistemas de armazenamento

Como alternativa ao uso do usuário administrativo padrão para esse coletor de dados, você pode configurar um usuário com direitos administrativos diretamente nos sistemas de storage NetApp para que esse coletor de dados possa adquirir dados de sistemas de storage NetApp.

A conexão com sistemas de armazenamento NetApp exige que o usuário, que é especificado ao adquirir o arquivador principal (no qual o sistema de armazenamento existe), atenda às seguintes condições:

- O usuário deve estar em vfiler0 (arquivador de raiz/pfiler).

Os sistemas de armazenamento são adquiridos ao adquirir o arquivador principal.

- Os comandos a seguir definem as capacidades de função do usuário:
 - "api-*": Use isso para permitir que Insights de infraestrutura de dados executem todos os comandos da API de armazenamento NetApp.

Este comando é necessário para usar o ZAPI.

- "Login-http-admin": Use isso para permitir que o Insights de infraestrutura de dados se conecte ao armazenamento NetApp via HTTP. Este comando é necessário para usar o ZAPI.
- "Security-API-vfiler": Use isso para permitir que os Insights de infraestrutura de dados executem comandos de API de storage do NetApp para recuperar informações da unidade do vFiler.

- "cli-options": Para o comando "options" e usado para o IP do parceiro e licenças habilitadas.
- "cli-lun": Acesse esses comandos para gerenciar LUNs. Exibe o status (caminho de LUN, tamanho, estado online/offline e estado compartilhado) do LUN ou classe de LUNs fornecidos.
- "cli-df": Para comandos "DF -s", "DF -r", "DF -A -r" e usados para exibir espaço livre.
- "CLI-ifconfig": Para o comando "ifconfig -a" e usado para obter o endereço IP do arquivador.
- "cli-rdfile": Para o comando "rdfile /etc/netgroup" e usado para obter netgroups.
- "cli-date": Para o comando "date" e usado para obter a data completa para obter cópias Snapshot.
- "cli-snap": Para o comando "snap list" e usado para obter cópias Snapshot.

Se as permissões cli-date ou cli-snap não forem fornecidas, a aquisição poderá ser concluída, mas as cópias Snapshot não serão relatadas.

Para adquirir uma fonte de dados do modo 7 com êxito e não gerar avisos no sistema de armazenamento, você deve usar uma das seguintes cadeias de comando para definir suas funções de usuário. A segunda string listada aqui é uma versão simplificada da primeira:

- login-http-admin,api-*,security-api-vfile,cli-rdfile,cli-options,cli-df,cli-lun,cli-ifconfig,cli-date,cli-snap,_,
- login-http-admin,api-* ,security-api-vfile,cli-

Solução de problemas

Algumas coisas para tentar se você encontrar problemas com este coletor de dados:

Inventário

Problema:	Tente isto:
Receber 401 resposta HTTP ou 13003 código de erro ZAPI e ZAPI retorna "insuficiente Privileges" ou "não autorizado para este comando"	Verifique o nome de usuário e a senha e o Privileges/permissões do usuário.
Erro "Falha ao executar comando"	Verifique se o usuário tem a seguinte permissão no dispositivo: • api-* • cli-date • cli-DF • cli-ifconfig • CLI-lun • CLI-operations • cli-rdfile • cli-snap • login-http-admin • security-api-vfiler também verifique se a versão do ONTAP é suportada pelo Data Infrastructure Insights e verifique se as credenciais usadas correspondem às credenciais do dispositivo
A versão do cluster é inferior a 8,1	A versão mínima suportada do cluster é 8,1. Atualize para a versão mínima suportada.
ZAPI retorna "a função de cluster não é cluster_mgmt LIF"	A UA precisa falar com o IP de gerenciamento de cluster. Verifique o IP e mude para um IP diferente, se necessário
Erro: "Os filers do modo 7 não são suportados"	Isso pode acontecer se você usar esse coletor de dados para descobrir o arquivador de modo 7D. Em vez disso, altere o IP para apontar para o arquivador cdot.

Problema:	Tente isto:
O comando ZAPI falha após a tentativa	AAU tem problema de comunicação com o cluster. Verifique a rede, o número da porta e o endereço IP. O usuário também deve tentar executar um comando da linha de comando da máquina AU.
Falha ao ligar a AU ao ZAPI	Verifique a conectividade IP/porta e confirme a configuração ZAPI.
Falha ao conectar-se ao ZAPI via HTTP	Verifique se a porta ZAPI aceita texto simples. Se AU tentar enviar texto simples para um soquete SSL, a comunicação falha.
A comunicação falha com SSLException	Au está tentando enviar SSL para uma porta de texto simples em um arquivador. Verifique se a porta ZAPI aceita SSL ou se usa uma porta diferente.
Erro de conexão adicional: A resposta ZAPI tem o código de erro 13001, "banco de dados não está aberto" o código de erro ZAPI é 60 e a resposta contém "API não terminou no tempo" resposta ZAPI contém "inicializar_sessão() ambiente NULL retornado o código de erro ZAPI é 14007 e a resposta contém "nó não está saudável"	Verifique a rede, o número da porta e o endereço IP. O usuário também deve tentar executar um comando da linha de comando da máquina AU.
Erro de tempo limite do soquete com ZAPI	Verifique a conectividade do arquivador e/ou aumente o tempo limite.
"Os clusters do modo C não são suportados pela fonte de dados do modo 7" erro	Verifique o IP e altere o IP para um cluster do modo 7D.
Erro "Falha ao se conectar ao vFiler"	Verifique se os recursos de usuário adquirentes incluem o seguinte no mínimo: API-* security-api-vfiler login-http-admin Confirme que o arquivador está executando o mínimo ONTAPI versão 1,7.

Informações adicionais podem ser encontradas na ["Suporte"](#) página ou no ["Matriz de suporte do Data Collector"](#).

Coletor de dados da API NetApp e-Series Legacy SANtricity

O coletor de dados da API Legacy SANtricity da NetApp e-Series reúne dados de inventário e desempenho. O coletor suporta firmware 7.x usando as mesmas configurações e relatando os mesmos dados.

Terminologia

O Cloud Insight adquire as seguintes informações de inventário do coletor de dados NetApp e-Series. Para cada tipo de ativo adquirido, a terminologia mais comum usada para esse ativo é mostrada. Ao visualizar ou solucionar problemas desse coletor de dados, tenha em mente a seguinte terminologia:

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
Disco	Disco
Grupo de volume	Grupo de discos

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
Storage array	Armazenamento
Controlador	Nó de storage
Grupo de volume	Pool de storage
Volume	Volume

Nota: Estes são apenas mapeamentos de terminologia comuns e podem não representar todos os casos para este coletor de dados.

Terminologia e-Series (Landing Page)

Os termos a seguir se aplicam a objetos ou referências que você pode encontrar nas páginas iniciais de ativos do NetApp e-Series. Muitos desses termos também se aplicam a outros coletores de dados.

Armazenamento

- Modelo – nome do modelo do dispositivo.
- Vendedor – mesmo nome do fornecedor que você veria se você estivesse configurando uma nova fonte de dados
- Número de série – o número de série da matriz. Em sistemas de storage de arquitetura de cluster, como o NetApp Clustered Data ONTAP, esse número de série pode ser menos útil do que os números de série individuais "nós de storage"
- IP – geralmente serão os IP (s) ou nome de host (s) conforme configurado na fonte de dados
- Versão de microcódigo – firmware
- Capacidade bruta – soma de base 2 de todos os discos físicos no sistema, independentemente da sua função
- Latência – uma representação do que o host enfrenta cargas de trabalho, tanto na leitura quanto na gravação. Idealmente, o Data Infrastructure Insights está fornecendo esse valor diretamente, mas isso geralmente não é o caso. Em vez do array que oferece isso, o Data Infrastructure Insights geralmente executa um cálculo ponderado por IOPs derivado das estatísticas de volumes individuais.
- Taxa de transferência – o host total do array voltado para a taxa de transferência. Idealmente obtido diretamente do array, se não estiver disponível, o Data Infrastructure Insights está somando a taxa de transferência dos volumes para obter esse valor
- Gerenciamento – isso pode conter um hiperlink para a interface de gerenciamento do dispositivo. Criado programaticamente pela fonte de dados Data Infrastructure Insights como parte dos relatórios de inventário

Pool de storage

- Armazenamento – em que storage esse pool vive. Obrigatório
- Tipo – um valor descritivo de uma lista de uma lista enumerada de possibilidades. Mais comumente será "thin Provisioning" ou "RAID Group"
- Nó – se a arquitetura desse storage array for tal que os pools pertençam a um nó de armazenamento específico, seu nome será visto aqui como um hiperlink para sua própria página inicial
- Usa Flash Pool – valor Sim/não
- Redundância – nível RAID ou esquema de proteção. Os relatórios do e-Series "RAID 7" para pools DDP

- Capacidade – os valores aqui são a capacidade lógica usada, utilizável e a capacidade total lógica, e a porcentagem usada entre eles. Esses valores incluem a capacidade de "preservação" do e-Series, o que resulta em números e na porcentagem mais alta do que a própria interface de usuário do e-Series pode mostrar
- Capacidade sobrecomprometida – se, por meio de tecnologias de eficiência, você tiver alocado uma soma total de capacidades de volume ou volume interno maior do que a capacidade lógica do pool de armazenamento, o valor percentual aqui será superior a 0%.
- Snapshot – capacidades de snapshot usadas e totais, se a arquitetura do seu pool de armazenamento dedicar parte da sua capacidade a segmentos de áreas exclusivamente para snapshots
- Utilização – um valor percentual que mostra a maior porcentagem de ocupado em disco de qualquer disco que contribui com a capacidade para esse pool de armazenamento. A utilização de disco não tem necessariamente uma forte correlação com o desempenho do array – a utilização pode ser alta devido a recompilações de disco, atividades de deduplicação, etc., na ausência de cargas de trabalho orientadas pelo host. Além disso, as implementações de replicação de muitos arrays podem impulsionar a utilização de disco, sem ser mostradas como workload de volume.
- IOPS – a soma de IOPs de todos os discos que contribuem com capacidade para esse pool de storage. Se as IOPs de disco não estiverem disponíveis em uma determinada plataforma, esse valor será obtido da soma de IOPs de volume para todos os volumes que estiverem nesse pool de armazenamento
- Taxa de transferência – a taxa de transferência soma de todos os discos que contribuem para a capacidade deste pool de armazenamento. Se a taxa de transferência do disco não estiver disponível em uma determinada plataforma, esse valor será obtido a partir da soma de volume para todos os volumes instalados neste pool de armazenamento

Nó de storage

- Armazenamento – em que storage array esse nó faz parte. Obrigatório
- Parceiro HA – em plataformas onde um nó fará failover para um e apenas um outro nó, ele geralmente será visto aqui
- Estado – saúde do nó. Disponível apenas quando o array estiver saudável o suficiente para ser inventariado por uma fonte de dados
- Modelo – nome do modelo do nó
- Versão – nome da versão do dispositivo.
- Número de série – o número de série do nó
- Memória – memória base 2, se disponível
- Utilização – geralmente um número de utilização da CPU ou, no caso do NetApp ONTAP, um índice de tensão do controlador. No momento, a utilização não está disponível para o NetApp e-Series
- IOPS – um número que representa os IOPs orientados pelo host neste controlador. Idealmente obtido diretamente do array, se não estiver disponível, ele será calculado somando todas as IOPs para volumes que pertencem exclusivamente a esse nó.
- Latência – um número que representa a latência típica do host ou o tempo de resposta neste controlador. Idealmente obtido diretamente do array, se não estiver disponível, ele será calculado executando um cálculo ponderado de IOPs a partir de volumes que pertencem exclusivamente a esse nó.
- Taxa de transferência – um número que representa a taxa de transferência orientada pelo host neste controlador. Idealmente obtido diretamente do array, se não estiver disponível, ele será calculado somando toda a taxa de transferência para volumes que pertencem exclusivamente a esse nó.
- Processadores – contagem de CPU

Requisitos

- O endereço IP de cada controlador na matriz
- Requisito de porta 2463

Configuração

Campo	Descrição
Lista separada por vírgulas de IPs do controlador SANtricity da matriz	Endereços IP e/ou nomes de domínio totalmente qualificados para os controladores de matriz

Configuração avançada

Campo	Descrição
Intervalo de enquete de inventário (min)	O padrão é de 30 minutos
Intervalo de enquete de desempenho até 3600 segundos	O padrão é de 300 segundos

Solução de problemas

Informações adicionais sobre este coletor de dados podem ser encontradas na ["Suporte"](#) página ou no ["Matriz de suporte do Data Collector"](#).

Coletor de DADOS REST do NetApp e-Series

O coletor de DADOS REST do NetApp e-Series coleta dados de inventário e desempenho. O coletor suporta firmware 7.x usando as mesmas configurações e relatando os mesmos dados. O coletor REST monitora o status de criptografia de pools de storage, bem como o status de criptografia de discos e volumes relacionados, além de fornecer a utilização de CPU de nó de storage como contadores de desempenho - funcionalidade não fornecida no coletor legado do SANtricity e-Series.

Terminologia

O Cloud Insight adquire as seguintes informações de inventário do NetApp e-Series, usando REST. Para cada tipo de ativo adquirido, a terminologia mais comum usada para esse ativo é mostrada. Ao visualizar ou solucionar problemas desse coletor de dados, tenha em mente a seguinte terminologia:

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
Disco	Disco
Grupo de volume	Grupo de discos
Storage array	Armazenamento
Controlador	Nó de storage
Grupo de volume	Pool de storage
Volume	Volume

Nota: Estes são apenas mapeamentos de terminologia comuns e podem não representar todos os casos para este coletor de dados.

Requisitos

- O endereço IP de cada controlador na matriz
- Este coletor suporta apenas matrizes de modelos e-Series com **capacidades de API REST nativas**. A organização e-Series envia uma distribuição de API REST instalável fora do array para arrays e-Series mais antigos: Este coletor não suporta esse cenário. Os usuários com arrays mais antigos devem continuar usando o coletor do Data Infrastructure Insights "API SANtricity do e-Series".
- O campo "endereço IP do controlador e-Series" suporta uma cadeia delimitada por vírgulas de 2 nomes IP/host; o coletor tentará inteligentemente o segundo IP/nome do host se o primeiro estiver inacessível.
- Porta HTTPS: A predefinição é 8443.

Configuração

Campo	Descrição
Endereços IP do controlador e-Series	Endereços IP separados por vírgulas e/ou nomes de domínio totalmente qualificados para os controladores de matriz

Configuração avançada

Campo	Descrição
Intervalo de enquete de inventário (min)	O padrão é de 30 minutos
Intervalo de enquete de desempenho até 3600 segundos	O padrão é de 300 segundos

Terminologia e-Series (Landing Page)

Os termos a seguir se aplicam a objetos ou referências que você pode encontrar nas páginas iniciais de ativos do NetApp e-Series. Muitos desses termos também se aplicam a outros coletores de dados.

Armazenamento

- Modelo – nome do modelo do dispositivo.
- Vendedor – mesmo nome do fornecedor que você veria se você estivesse configurando uma nova fonte de dados
- Número de série – o número de série da matriz. Em sistemas de storage de arquitetura de cluster, como o NetApp Clustered Data ONTAP, esse número de série pode ser menos útil do que os números de série individuais "nós de storage"
- IP – geralmente serão os IP (s) ou nome de host (s) conforme configurado na fonte de dados
- Versão de microcódigo – firmware
- Capacidade bruta – soma de base 2 de todos os discos físicos no sistema, independentemente da sua função
- Latência – uma representação do que o host enfrenta cargas de trabalho, tanto na leitura quanto na gravação. Idealmente, o Data Infrastructure Insights está fornecendo esse valor diretamente, mas isso geralmente não é o caso. Em vez do array que oferece isso, o Data Infrastructure Insights geralmente

executa um cálculo ponderado por IOPs derivado das estatísticas de volumes individuais.

- Taxa de transferência – o host total do array voltado para a taxa de transferência. Idealmente obtido diretamente do array, se não estiver disponível, o Data Infrastructure Insights está somando a taxa de transferência dos volumes para obter esse valor
- Gerenciamento – isso pode conter um hiperlink para a interface de gerenciamento do dispositivo. Criado programaticamente pela fonte de dados Data Infrastructure Insights como parte dos relatórios de inventário

Pool de storage

- Armazenamento – em que storage esse pool vive. Obrigatório
- Tipo – um valor descritivo de uma lista de uma lista enumerada de possibilidades. Mais comumente será "thin Provisioning" ou "RAID Group"
- Nó – se a arquitetura desse storage array for tal que os pools pertençam a um nó de armazenamento específico, seu nome será visto aqui como um hiperlink para sua própria página inicial
- Usa Flash Pool – valor Sim/não
- Redundância – nível RAID ou esquema de proteção. Os relatórios do e-Series "RAID 7" para pools DDP
- Capacidade – os valores aqui são a capacidade lógica usada, utilizável e a capacidade total lógica, e a porcentagem usada entre eles. Esses valores incluem a capacidade de "preservação" do e-Series, o que resulta em números e na porcentagem mais alta do que a própria interface de usuário do e-Series pode mostrar
- Capacidade sobrecomprometida – se, por meio de tecnologias de eficiência, você tiver alocado uma soma total de capacidades de volume ou volume interno maior do que a capacidade lógica do pool de armazenamento, o valor percentual aqui será superior a 0%.
- Snapshot – capacidades de snapshot usadas e totais, se a arquitetura do seu pool de armazenamento dedicar parte da sua capacidade a segmentos de áreas exclusivamente para snapshots
- Utilização – um valor percentual que mostra a maior porcentagem de ocupado em disco de qualquer disco que contribui com a capacidade para esse pool de armazenamento. A utilização de disco não tem necessariamente uma forte correlação com o desempenho do array – a utilização pode ser alta devido a recompilações de disco, atividades de deduplicação, etc., na ausência de cargas de trabalho orientadas pelo host. Além disso, as implementações de replicação de muitos arrays podem impulsionar a utilização de disco, sem ser mostradas como workload de volume.
- IOPS – a soma de IOPs de todos os discos que contribuem com capacidade para esse pool de storage. Se as IOPs de disco não estiverem disponíveis em uma determinada plataforma, esse valor será obtido da soma de IOPs de volume para todos os volumes que estiverem nesse pool de armazenamento
- Taxa de transferência – a taxa de transferência soma de todos os discos que contribuem para a capacidade deste pool de armazenamento. Se a taxa de transferência do disco não estiver disponível em uma determinada plataforma, esse valor será obtido a partir da soma de volume para todos os volumes instalados neste pool de armazenamento

Nó de storage

- Armazenamento – em que storage array esse nó faz parte. Obrigatório
- Parceiro HA – em plataformas onde um nó fará failover para um e apenas um outro nó, ele geralmente será visto aqui
- Estado – saúde do nó. Disponível apenas quando o array estiver saudável o suficiente para ser inventariado por uma fonte de dados

- Modelo – nome do modelo do nó
- Versão – nome da versão do dispositivo.
- Número de série – o número de série do nó
- Memória – memória base 2, se disponível
- Utilização – geralmente um número de utilização da CPU ou, no caso do NetApp ONTAP, um índice de tensão do controlador. No momento, a utilização não está disponível para o NetApp e-Series
- IOPS – um número que representa os IOPs orientados pelo host neste controlador. Idealmente obtido diretamente do array, se não estiver disponível, ele será calculado somando todas as IOPs para volumes que pertencem exclusivamente a esse nó.
- Latência – um número que representa a latência típica do host ou o tempo de resposta neste controlador. Idealmente obtido diretamente do array, se não estiver disponível, ele será calculado executando um cálculo ponderado de IOPs a partir de volumes que pertencem exclusivamente a esse nó.
- Taxa de transferência – um número que representa a taxa de transferência orientada pelo host neste controlador. Idealmente obtido diretamente do array, se não estiver disponível, ele será calculado somando toda a taxa de transferência para volumes que pertencem exclusivamente a esse nó.
- Processadores – contagem de CPU

Solução de problemas

Informações adicionais sobre este coletor de dados podem ser encontradas na ["Suporte"](#) página ou no ["Matriz de suporte do Data Collector"](#).

Configurando o coletor de dados do servidor de gerenciamento NetApp HCI

O coletor de dados do servidor de gerenciamento do NetApp HCI coleta informações do host do NetApp HCI e requer Privileges somente leitura em todos os objetos dentro do servidor de gerenciamento.

Este coletor de dados adquire apenas a partir do **servidor de Gestão NetApp HCI**. Para coletar dados do sistema de armazenamento, você também deve configurar o ["NetApp SolidFire"](#) coletor de dados.

Terminologia

O Data Infrastructure Insights adquire as seguintes informações de inventário desse coletor de dados. Para cada tipo de ativo adquirido, a terminologia mais comum usada para o ativo é mostrada. Ao visualizar ou solucionar problemas desse coletor de dados, tenha em mente a seguinte terminologia:

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
Disco virtual	Disco
Host	Host
Máquina virtual	Máquina virtual
Armazenamento de dados	Armazenamento de dados
LUN	Volume
Porta Fibre Channel	Porta

Estes são apenas mapeamentos de terminologia comuns e podem não representar todos os casos para este

coletor de dados.

Requisitos

As seguintes informações são necessárias para configurar este coletor de dados:

- Endereço IP do servidor de gerenciamento NetApp HCI
- Nome de usuário e senha somente leitura para o servidor de Gerenciamento NetApp HCI
- Leia somente Privileges em todos os objetos no servidor de gerenciamento do NetApp HCI.
- Acesso ao SDK no servidor de gerenciamento do NetApp HCI – normalmente já configurado.
- Requisitos de porta: HTTP-80 https-443
- Validar acesso:
 - Faça login no servidor de gerenciamento do NetApp HCI usando o nome de usuário e a senha acima
 - Verificar SDK habilitado: telnet <vc_ip> 443

Configuração e conexão

Campo	Descrição
Nome	Nome exclusivo para o coletor de dados
Unidade de aquisição	Nome da unidade de aquisição

Configuração

Campo	Descrição
MVIP do cluster de storage do NetApp HCI	Endereço IP virtual de gerenciamento
Nó de gerenciamento de SolidFire (mNode)	Endereço IP do nó de gerenciamento
Nome de utilizador	Nome de utilizador utilizado para aceder ao servidor de gestão NetApp HCI
Palavra-passe	Palavra-passe utilizada para aceder ao servidor de gestão NetApp HCI
Nome de usuário do vCenter	Nome de usuário do vCenter
Senha do vCenter	Senha do vCenter

Configuração avançada

Na tela de configuração avançada, marque a caixa **desempenho da VM** para coletar dados de desempenho. A coleção de inventário está ativada por predefinição. Os seguintes campos podem ser configurados:

Campo	Descrição
Intervalo de pesquisa de inventário (min)	Default é 20
Filtrar VMs por	Selecione CLUSTER, DATA CENTER ou HOST ESX
Escolha 'Excluir' ou 'incluir' para especificar uma lista	Especifique se deseja incluir ou excluir VMs

Filtrar Lista de dispositivos	Lista de VMs a filtrar (separadas por vírgulas ou ponto e vírgula separadas se a vírgula for usada no valor) para filtragem somente por ESX_HOST, CLUSTER e DATA CENTER
Intervalo de pesquisa de desempenho (seg)	A predefinição é 300

Solução de problemas

Algumas coisas para tentar se você encontrar problemas com este coletor de dados:

Inventário

Problema:	Tente isto:
Erro: Incluir lista para filtrar VMs não pode estar vazia	Se a opção incluir lista estiver selecionada, liste nomes válidos de data center, cluster ou host para filtrar VMs
Erro: Falha ao instanciar uma conexão com o VirtualCenter no IP	Soluções possíveis: * Verifique as credenciais e o endereço IP inseridos. * Tente se comunicar com o Virtual Center usando o Infrastructure Client. * Tente se comunicar com o Virtual Center usando o Navegador de objetos gerenciados (por exemplo, MOB).
Erro: O VirtualCenter at IP tem certificado não conforme exigido pela JVM	Soluções possíveis: * Recomendado: Re-gerar certificado para o Virtual Center usando uma chave RSA mais forte (por exemplo, 1024 bits). * Não recomendado: Modifique a configuração JVM java.security para aproveitar a restrição jdk.certpath.disabledAlgorithms para permitir a chave RSA de 512 bits. Consulte as notas de versão da atualização 40 do JDK 7 em " http://www.oracle.com/technetwork/java/javase/7u40-relnotes-2004172.html "

Informações adicionais podem ser encontradas na "[Suporte](#)" página ou no "[Matriz de suporte do Data Collector](#)".

Coletor de dados em array all-flash NetApp SolidFire

O coletor de dados de array all-flash NetApp SolidFire dá suporte à coleta de inventário e desempenho de configurações de SolidFire iSCSI e Fibre Channel.

O coletor de dados do SolidFire utiliza a API REST do SolidFire. A unidade de aquisição em que reside o coletor de dados precisa ser capaz de iniciar conexões HTTPS com a porta TCP 443 no endereço IP de gerenciamento de cluster SolidFire. O coletor de dados precisa de credenciais capazes de fazer consultas de API REST no cluster SolidFire.

Terminologia

O Data Infrastructure Insights adquire as seguintes informações de inventário do coletor de dados de array all-flash NetApp SolidFire. Para cada tipo de ativo adquirido pelo Data Infrastructure Insights, a terminologia mais comum usada para esse ativo é mostrada. Ao visualizar ou solucionar problemas desse coletor de dados, tenha em mente a seguinte terminologia:

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
Condução	Disco
Cluster	Armazenamento
Nó	Nó de storage
Volume	Volume
Porta Fibre Channel	Porta
Grupo Acesso volume, atribuição LUN	Mapa de volume
Sessão iSCSI	Máscara de volume

Nota: Estes são apenas mapeamentos de terminologia comuns e podem não representar todos os casos para este coletor de dados.

Requisitos

A seguir estão os requisitos para configurar este coletor de dados:

- Endereço IP virtual de gerenciamento
- Nome de usuário e credenciais somente leitura
- Porta 443

Configuração

Campo	Descrição
Endereço IP virtual de gerenciamento (MVIP)	Endereço IP virtual de gerenciamento do cluster do SolidFire
Nome de utilizador	Nome utilizado para iniciar sessão no cluster SolidFire
Palavra-passe	Palavra-passe utilizada para iniciar sessão no cluster SolidFire

Configuração avançada

Campo	Descrição
Tipo de ligação	Escolha o tipo de conexão
Porta de comunicação	Porta usada para API NetApp
Intervalo de enquete de inventário (min)	O padrão é de 20 minutos
Intervalo de enquete de desempenho (seg)	O padrão é de 300 segundos

Solução de problemas

Quando o SolidFire relata um erro, ele é exibido no Insights de infraestrutura de dados da seguinte forma:

Uma mensagem de erro foi recebida de um dispositivo SolidFire ao tentar recuperar dados. A chamada foi <method> (<parameterString>). A mensagem de erro do dispositivo foi (verifique o manual do dispositivo): <message>

Local:

- O <method> é um método HTTP, como GET ou PUT.
- O <parameterString> é uma lista separada por vírgulas de parâmetros que foram incluídos na CHAMADA REST.
- O <message> é o que o dispositivo retornou como a mensagem de erro.

Informações adicionais sobre este Coletor de dados podem ser encontradas "[Suporte](#)" na página ou no "[Matriz de suporte do Data Collector](#)".

Coletor de dados NetApp StorageGRID

O coletor de dados NetApp StorageGRID suporta a coleta de inventário e desempenho de configurações do StorageGRID.



O StorageGRID é medido a uma taxa bruta diferente de TB para Unidade gerenciada. Cada 40 TB de capacidade StorageGRID não formatada é cobrado como 1 "[Unidade gerenciada \(MU\)](#)".

Terminologia

Insights de infraestrutura de dados adquire as seguintes informações de inventário do coletor NetApp StorageGRID. Para cada tipo de ativo adquirido, a terminologia mais comum usada para esse ativo é mostrada. Ao visualizar ou solucionar problemas desse coletor de dados, tenha em mente a seguinte terminologia:

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
StorageGRID	Armazenamento
Nó	Nó
Locatário	Pool de storage
Balde	Volume interno

Requisitos

A seguir estão os requisitos para configurar esta fonte de dados:

- Endereço IP do host StorageGRID
- Um nome de usuário e senha para um usuário que teve as funções de consulta métrica e Acesso ao locatário atribuídas
- Porta 443

Configuração

Campo	Descrição
Endereço IP do host StorageGRID	Endereço IP virtual de gerenciamento do dispositivo StorageGRID
Nome de utilizador	Nome utilizado para iniciar sessão no dispositivo StorageGRID
Palavra-passe	Palavra-passe utilizada para iniciar sessão no dispositivo StorageGRID

Configuração avançada

Campo	Descrição
Intervalo de enquete de inventário (min)	O padrão é de 60 minutos
Intervalo de enquete de desempenho (seg)	O padrão é de 900 segundos

Logon único (SSO)

As "StorageGRID" versões de firmware têm versões de API correspondentes; a API 3,0 e as versões mais recentes suportam login de logon único (SSO).

Versão do firmware	Versão da API	Suporte single sign on (SSO)
11,1	2	Não
11,2	3,0	Sim
11,5	3,3	Sim

Solução de problemas

Informações adicionais sobre este Coletor de dados podem ser encontradas ["Suporte"](#) na página ou no ["Matriz de suporte do Data Collector"](#).

Coletor de dados Nutanix NX

O Data Infrastructure Insights usa o coletor de dados Nutanix para descobrir dados de inventário e desempenho para sistemas de armazenamento Nutanix NX.

Terminologia

A Data Infrastructure Insights adquire as seguintes informações de inventário do coletor de dados Nutanix. Para cada tipo de ativo adquirido pelo Data Infrastructure Insights, a terminologia mais comum usada para esse ativo é mostrada. Ao visualizar ou solucionar problemas desse coletor de dados, tenha em mente a seguinte terminologia:

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
Pool de storage	Pool de storage
Recipiente Nutanix	Volume interno

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
Recipiente Nutanix	Partilha de ficheiros
Compartilhamento NFS	Partilhar

Nota: Estes são apenas mapeamentos de terminologia comuns e podem não representar todos os casos para este coletor de dados.

Requisitos

- O endereço IP dos serviços de dados externos para o cluster
- Nome de usuário e senha somente leitura, a menos que grupos_de volume estejam em uso, nesse caso, nome de usuário e senha de administrador são necessários
- Requisito de porta: HTTPS 443

Configuração

Campo	Descrição
Endereço IP externo do prisma	O endereço IP dos serviços de dados externos para o cluster
Nome de utilizador	Nome de usuário para a conta de administrador
Palavra-passe	Palavra-passe para a conta de administrador

Configuração avançada

Campo	Descrição
Porta de TCP	Porta TCP usada para se conectar ao array Nutanix. A predefinição é 9440.
Intervalo de pesquisa de inventário (min)	Intervalo entre sondagens de inventário. O padrão é 60 minutos.
Intervalo de pesquisa de desempenho (seg)	Intervalo entre sondagens de desempenho. O padrão é 300 segundos.

Solução de problemas

Informações adicionais sobre este Coletor de dados podem ser encontradas ["Suporte"](#) na página ou no ["Matriz de suporte do Data Collector"](#).

Coletor de dados OpenStack

O coletor de dados OpenStack (REST API / KVM) adquire dados de inventário para todas as instâncias OpenStack e, opcionalmente, dados de desempenho de VM.

Requisitos

- Endereço IP do controlador OpenStack
- Credencial de função de administrador do OpenStack e acesso sudo ao hipervisor Linux KVM. Se você

não estiver usando a conta de administrador ou o administrador equivalente Privileges, você precisará usar o teste e o erro para identificar as políticas padrão para relaxar para o seu ID de usuário do coletor de dados.

- O módulo OpenStack Gnocchi deve ser instalado e configurado para coleta de desempenho. A configuração do Gnocchi é feita editando o arquivo nova.conf para cada hypervisor e, em seguida, reiniciando o serviço Nova Compute em cada hypervisor. O nome da opção muda para diferentes versões do OpenStack:
 - Icehouse
 - Juno
 - Quilo
 - Liberdade
 - Mitaka
 - Newton
 - Ocata
- Para estatísticas de CPU, "ComputeDriverCPUMonitor" precisa ser ativado em /etc/nova/nova.conf em nós de computação.
- Requisitos do porto:
 - 5000 para http e 13000 para https, para o serviço Keystone
 - 22 para KVM SSH
 - 8774 para Nova Compute Service
 - 8776 para o serviço do bloco do Cinder
 - 8777 para Gnocchi Performance Service
 - 9292 for Glance Image Service **Observação** a porta se liga ao serviço específico e o serviço pode ser executado no controlador ou em outro host em ambientes maiores.

Configuração

Campo	Descrição
Endereço IP do controlador OpenStack	Endereço IP ou nome de domínio totalmente qualificado do controlador OpenStack
Administrador do OpenStack	Nome de usuário para um administrador OpenStack
Senha do OpenStack	Senha usada para o administrador do OpenStack
Locatário do administrador do OpenStack	Nome do locatário do Administrador do OpenStack
KVM sudo usuário	Nome de usuário do sudo KVM
Escolha 'Senha' ou 'Arquivo de chave OpenSSH' para especificar o tipo de credencial	Tipo de credencial usado para se conectar ao dispositivo via SSH
Caminho completo para chave privada de inventário	Caminho completo para chave privada de inventário
KVM sudo Password	KVM sudo Password

Configuração avançada

Campo	Descrição
Habilite a descoberta de inventário do hipervisor por meio de SSH	Verifique isto para ativar a descoberta de inventário do hipervisor através de SSH
Porta de URL do OpenStack Admin	Porta de URL do OpenStack Admin
Use HTTPS	Verifique para usar HTTP seguro
Porta SSH	Porta usada para SSH
Geometrias de processo SSH	Número de tentativas de tentativa de inventário
Intervalo de enquete de inventário (min)	Intervalo entre sondagens de inventário. O padrão é 20 minutos.

Solução de problemas

Algumas coisas para tentar se você encontrar problemas com este coletor de dados:

Inventário

Problema:	Tente isto:
"Erro de configuração" com mensagens de erro começam com "a política não permite" ou "você não está autorizado"	* Verificar endereço ip * verificar nome de usuário e senha

Informações adicionais podem ser encontradas na ["Suporte"](#) página ou no ["Matriz de suporte do Data Collector"](#).

Coletor de dados Oracle ZFS Storage Appliance

O Data Infrastructure Insights usa o coletor de dados do Oracle ZFS Storage Appliance para coletar dados de inventário e desempenho.

Terminologia

O Data Infrastructure Insights adquire informações de inventário com o coletor de dados Oracle ZFS. Para cada tipo de ativo adquirido pelo Data Infrastructure Insights, a terminologia mais comum usada para esse ativo é mostrada. Ao visualizar ou solucionar problemas desse coletor de dados, tenha em mente a seguinte terminologia:

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
Disco (SSD)	Disco
Cluster	Armazenamento
Controlador	Nó de storage
LUN	Volume
Mapa LUN	Mapa de volume
Iniciador, alvo	Máscara de volume

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
Partilhar	Volume interno

Nota: Estes são apenas mapeamentos de terminologia comuns e podem não representar todos os casos para esta fonte de dados.

Requisitos

- Nomes de host para o controlador ZFS-1 e o controlador ZFS-2
- Nome de usuário e senha do administrador
- Requisito de porta: 215 HTTP/HTTPS

Métricas de performance necessárias

Os dispositivos Oracle ZFS oferecem aos administradores de armazenamento grandes quantidades de flexibilidade para capturar estatísticas de desempenho. O Data Infrastructure Insights espera que você tenha *cada* controlador em um par de alta disponibilidade configurado para capturar as seguintes métricas:

- smb2.ops[compartilhar]
- nfs3.ops[compartilhar]
- nfs4.ops[compartilhar]
- nfs4-1.ops[compartilhar]

A falha em fazer com que o controlador capture um ou todos eles provavelmente resultará em o Data Infrastructure Insights não ter, ou subreportar, a carga de trabalho nos "volumes internos".

Configuração

Campo	Descrição
Nome do host ZFS Controller-1	Nome de host para controlador de storage 1
Nome do host ZFS Controller-2	Nome de host para controlador de storage 2
Nome de utilizador	Nome de utilizador da conta de utilizador do administrador do sistema de armazenamento
Palavra-passe	Palavra-passe para a conta de utilizador administrador

Configuração avançada

Campo	Descrição
Tipo de ligação	HTTPS ou HTTP, também exibe a porta padrão
Substituir porta de ligação	Se estiver em branco, use a porta padrão no campo tipo de conexão; caso contrário, insira a porta de conexão a ser usada
Intervalo de pesquisa de inventário	O padrão é 60 segundos
Intervalo de enquete de desempenho (seg)	A predefinição é 300.

Solução de problemas

Algumas coisas para tentar se você encontrar problemas com este coletor de dados:

Inventário

Problema:	Tente isto:
"Credenciais de início de sessão inválidas"	Valide a conta de usuário e a senha do ZFS
"Erro de configuração" com mensagem de erro "o serviço DE REPOUSO está desativado"	Verifique se o serviço REST está ativado neste dispositivo.
"Erro de configuração " com mensagem de erro "Usuário não autorizado para comando"	<p>Esse erro provavelmente deve-se a certas funções (por exemplo, 'Advanced_analytics') não serem incluídas para o usuário configurado.</p> <p>A aplicação do escopo do Analytics para o usuário com função somente leitura pode remover o erro. Siga estes passos:</p> <ol style="list-style-type: none">1. No sistema ZFS, a partir do ecrã Configuration → Users (Configuração → utilizadores), mova o rato sobre a função e faça duplo clique para permitir a edição2. Selecione "Analytics" (análise) no menu pendente Scope (Escopo). É apresentada uma lista das propriedades possíveis.3. Clique na caixa de seleção mais alta e ela selecionará todas as três propriedades.4. Clique no botão Adicionar no lado direito.5. Clique no botão aplicar no canto superior direito da janela pop-up. A janela pop-up será fechada.

Informações adicionais podem ser encontradas na ["Suporte"](#) página ou no ["Matriz de suporte do Data Collector"](#).

Coletor de dados Pure Storage FlashArray

O Data Infrastructure Insights usa o coletor de dados Pure Storage FlashArray para coletar dados de inventário e performance.

Terminologia

Para cada tipo de ativo adquirido pelo Data Infrastructure Insights, a terminologia mais comum usada para o ativo é mostrada. Ao visualizar ou solucionar problemas desse coletor de dados, tenha em mente a seguinte terminologia:

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
Unidade (SSD)	Disco
Array	Armazenamento
Controlador	Nó de storage
Volume	Volume
Mapa LUN	Mapa de volume
Iniciador, alvo	Máscara de volume

Nota: Estes são apenas mapeamentos de terminologia comuns e podem não representar todos os casos para este coletor de dados.

Requisitos

- Endereço IP do sistema de armazenamento
- Nome de utilizador e palavra-passe da conta de administrador do sistema de armazenamento Pure.
- Requisito de porta: HTTP/HTTPS 80/443

Configuração

Campo	Descrição
Endereço IP do host FlashArray	Endereço IP do sistema de armazenamento
Nome de utilizador	Nome de usuário com admin Privileges
Senha para a conta privilegiada do administrador	Palavra-passe

Configuração avançada

Campo	Descrição
Tipo de ligação	Escolha HTTP ou HTTPS. Também exibe a porta padrão.
Substituir a porta TCP	Se estiver em branco, use a porta padrão no campo tipo de conexão; caso contrário, insira a porta de conexão a ser usada
Intervalo de pesquisa de inventário (min)	O padrão é 60 minutos
Intervalo de enquete de desempenho (seg)	A predefinição é 300

Solução de problemas

Algumas coisas para tentar se você encontrar problemas com este coletor de dados:

Inventário

Problema:	Tente isto:
"Credenciais de login inválidas" com mensagens de erro "a política não permite" ou "você não está autorizado"	Valide a conta de usuário e a senha da Pure através da interface http da Pure

Informações adicionais podem ser encontradas na ["Suporte"](#) página ou no ["Matriz de suporte do Data Collector"](#).

Coletor de dados Red Hat Virtualization

O Data Infrastructure Insights usa o coletor de dados Red Hat Virtualization para coletar dados de inventário de cargas de trabalho virtualizadas do Linux e do Microsoft Windows.

Terminologia

Para cada tipo de ativo adquirido pelo Data Infrastructure Insights, a terminologia mais comum usada para o ativo é mostrada. Ao visualizar ou solucionar problemas desse coletor de dados, tenha em mente a seguinte terminologia:

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
Disco	Disco virtual
Host	Host
Máquina virtual	Máquina virtual
Domínio de armazenamento	Armazenamento de dados
Unidade lógica	LUN

Nota: Estes são apenas mapeamentos de terminologia comuns e podem não representar todos os casos para este coletor de dados.

Requisitos

- Endereço IP do servidor RHEV na porta 443 via API REST
- Nome de utilizador e palavra-passe só de leitura
- RHEV versão mais recente 3,0

Configuração

Campo	Descrição
Endereço IP do servidor RHEV	Endereço IP do sistema de armazenamento
Nome de utilizador	Nome de usuário com admin Privileges
Senha para a conta privilegiada do administrador	Palavra-passe

Configuração avançada

Campo	Descrição
Porta de comunicação HTTPS	Porta usada para comunicação HTTPS com o RHEV
Intervalo de pesquisa de inventário (min)	O padrão é 20 minutos.

Solução de problemas

Informações adicionais sobre este Coletor de dados podem ser encontradas ["Suporte"](#) na página ou no ["Matriz de suporte do Data Collector"](#).

Coletor de dados CDM da Rubrik

O Data Infrastructure Insights usa o coletor de dados da Rubrik para adquirir dados de inventário e desempenho de dispositivos de storage da Rubrik.

Terminologia

O Data Infrastructure Insights adquire as seguintes informações de inventário do coletor de dados da Rubrik. Para cada tipo de ativo adquirido pelo Data Infrastructure Insights, a terminologia mais comum usada para esse ativo é mostrada. Ao visualizar ou solucionar problemas desse coletor de dados, tenha em mente a seguinte terminologia:

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
Cluster	Armazenamento, pool de armazenamento
Nó	Nó de storage
Disco	Disco

Nota: Estes são apenas mapeamentos de terminologia comuns e podem não representar todos os casos para esta fonte de dados.

Requisitos

Para configurar este coletor de dados, são necessários os seguintes itens:

- A Unidade de aquisição do Data Infrastructure Insights iniciará conexões com a porta TCP 443 para o cluster Rubrik. Um coletor por cluster.
- Endereço IP do cluster da Rubrik.
- Nome de utilizador e palavra-passe para o cluster.
- Endereço IP ou nome do host do cluster Rubrik.
- Para Autenticação básica, um nome de usuário e uma senha para o cluster. Se você preferir usar a autenticação baseada em conta de Serviço, precisará de uma conta de Serviço, segredo e um ID de Organização
- Requisito de porta: HTTPS 443

Configuração

Campo	Descrição
IP	Endereço IP do cluster Rubrik
Nome de utilizador	Nome de utilizador para o cluster
Palavra-passe	Palavra-passe para o cluster

Configuração avançada

Intervalo de pesquisa de inventário (min)	A predefinição é 60
Intervalo de enquete de desempenho (seg)	A predefinição é 300

Solução de problemas

Algumas coisas para tentar se você encontrar problemas com este coletor de dados:

Inventário

Problema:	Tente isto:
Recebi uma mensagem informando que mais de um armazenamento foi criado.	Verifique se o cluster está configurado corretamente e se o coletor está apontando para um único cluster.
Recebi um aviso de que a API de disco retornou mais dados	Consulte o suporte para obter dados adicionais.

Informações adicionais podem ser encontradas na ["Suporte"](#) página ou no ["Matriz de suporte do Data Collector"](#).

Configurando o coletor de dados do VMware vSphere

O coletor de dados do VMware vSphere coleta informações de configuração e desempenho do convidado da VM e do host ESXi e requer Privileges somente leitura em todos os objetos do vSphere. A partir de agosto de 2024, o coletor do vSphere também traz mensagens de log de ambientes vSphere e algumas métricas específicas da VMware. Observe que o Data Infrastructure Insights só pode recuperar informações de logs do VMware de ambientes vSphere 8.0.1 ou superior. Da mesma forma, as métricas específicas do fornecedor são suportadas apenas para ambientes vSphere mais de 7. Como tal, você pode querer desativar a caixa de seleção logs e/ou métricas específicas do fornecedor em um determinado coletor se ele for apontado para uma instância mais antiga do vSphere.

Terminologia

O Data Infrastructure Insights adquire as seguintes informações de inventário do coletor de dados do VMware vSphere. Para cada tipo de ativo adquirido, a terminologia mais comum usada para o ativo é mostrada. Ao visualizar ou solucionar problemas desse coletor de dados, tenha em mente a seguinte terminologia:

Termo do fornecedor/modelo	Termo do Insights de infraestrutura de dados
Disco virtual	Disco
Host	Host
Máquina virtual	Máquina virtual
Armazenamento de dados	Armazenamento de dados
LUN	Volume
Porta Fibre Channel	Porta

Estes são apenas mapeamentos de terminologia comuns e podem não representar todos os casos para este coletor de dados.

Requisitos

As seguintes informações são necessárias para configurar este coletor de dados:

- Endereço IP do servidor do Virtual Center
- Nome de usuário e senha somente leitura no Virtual Center
- Exigimos Privileges somente leitura em todos os objetos dentro do Centro Virtual.
- Acesso ao SDK no servidor do Virtual Center – normalmente já configurado.
- Requisitos de porta: HTTP-80 https-443
- Validar acesso:
 - Faça login no Virtual Center Client usando o nome de usuário e a senha acima
 - Verificar SDK habilitado: telnet <vc_ip> 443

Configuração e conexão

Campo	Descrição
Nome	Nome exclusivo para o coletor de dados
Unidade de aquisição	Nome da unidade de aquisição

Configuração

Campo	Descrição
Endereço IP do centro virtual	Endereço IP do Centro Virtual
Nome de utilizador	Nome de utilizador utilizado para aceder ao Centro Virtual
Palavra-passe	Palavra-passe utilizada para aceder ao Centro Virtual

Configuração avançada

Na tela de configuração avançada, marque a caixa **desempenho da VM** para coletar dados de desempenho. A coleção de inventário está ativada por predefinição. Os seguintes campos podem ser configurados:

Campo	Descrição
Intervalo de pesquisa de inventário (min)	A predefinição é 20
Filtrar VMs	Selecione CLUSTER, DATA CENTER ou HOST ESX
Escolha 'Excluir' ou 'incluir' para especificar uma lista	Criar uma lista de filtros (CLUSTER, DATA CENTER e/ou ESX_HOST)
Número de tentativas	A predefinição é 3
Porta de comunicação	A predefinição é 443
Filtrar Lista de dispositivos...	Esta lista deve consistir em correspondências exatas de cadeia de caracteres - se você pretende filtrar por ESX_HOST, você deve criar uma lista delimitada por vírgulas dos "nomes" exatos dos seus hosts ESX conforme relatado no Data Infrastructure Insights e no vSphere. Esses "nomes" podem ser endereços IP, nomes de host simples ou nomes de domínio totalmente qualificados (FQDNs) - isso é determinado por como esses hosts foram nomeados quando foram originalmente adicionados ao vSphere. Ao filtrar por CLUSTER, use os nomes de cluster do estilo Data Infrastructure Insights conforme relatado pelo IC em hipervisores - Data Infrastructure Insights prepende o nome do cluster vSphere com o nome do data center vSphere e uma barra direta - "DC1/clusterA" é o nome do cluster Data Infrastructure Insights relatada em um hypervisor no clusterA dentro do data center DC1.
Intervalo de pesquisa de desempenho (seg)	A predefinição é 300

Mapeamento de tags VMware para anotações do Data Infrastructure Insights

O coletor de dados VMware permite preencher anotações do Data Infrastructure Insights com tags configuradas no VMware. As anotações devem ser nomeadas exatamente como as tags VMware. O Data Infrastructure Insights sempre preencherá anotações de tipo texto com o mesmo nome e fará uma "melhor tentativa" para preencher anotações de outros tipos (número, boolean, etc.). Se a anotação for de um tipo diferente e o coletor de dados não a preencher, pode ser necessário remover a anotação e recriá-la como um tipo de texto.

Observe que as tags VMware podem diferenciar maiúsculas de minúsculas, enquanto as tags Data Infrastructure Insights diferenciam maiúsculas de minúsculas. Então, se você criar uma anotação chamada "PROPRIETÁRIO" no Data Infrastructure Insights e tags chamadas "PROPRIETÁRIO", "proprietário" e "proprietário" no VMware, todas essas variações de "proprietário" serão mapeadas para a anotação "PROPRIETÁRIO" do Cloud Insight.

Tenha em mente o seguinte:

- Atualmente, apenas publica automaticamente informações de suporte para dispositivos NetApp.
- Como essas informações de suporte são mantidas em formulário de anotação, você pode consultá-las ou usá-las em painéis.
- Se um usuário sobrescrever ou esvaziar o valor da anotação, o valor será preenchido automaticamente novamente quando o Data Infrastructure Insights atualizar anotações, o que ele faz uma vez por dia.

Solução de problemas

Algumas coisas para tentar se você encontrar problemas com este coletor de dados:

Inventário

Problema:	Tente isto:
Erro: Incluir lista para filtrar VMs não pode estar vazia	Se a opção incluir lista estiver selecionada, liste nomes válidos de data center, cluster ou host para filtrar VMs
Erro: Falha ao instanciar uma conexão com o VirtualCenter no IP	Soluções possíveis: * Verifique as credenciais e o endereço IP inseridos. * Tente se comunicar com o Virtual Center usando o VMware Infrastructure Client. * Tente se comunicar com o Virtual Center usando o Navegador de objetos gerenciados (por exemplo, MOB).
Erro: O VirtualCenter at IP tem certificado não conforme exigido pela JVM	Soluções possíveis: * Recomendado: Re-gerar certificado para o Virtual Center usando uma chave RSA mais forte (por exemplo, 1024 bits). * Não recomendado: Modifique a configuração JVM <code>java.security</code> para aproveitar a restrição <code>jdk.certpath.disabledAlgorithms</code> para permitir a chave RSA de 512 bits. " Notas de versão da atualização 40 do JDK 7 "Consulte .
Estou vendo a mensagem: "O pacote VMware Logs não é suportado no VMware abaixo da versão 8,0.1"	A coleção de logs não é suportada em versões VMware anteriores a 8,0.1. Atualize sua infraestrutura do VI Center para a versão 8.0.1 ou posterior, se desejar usar o recurso conjuntos de logs dentro do Data Infrastructure Insights. Para obter mais informações, consulte este " Artigo da KB ".

Informações adicionais podem ser encontradas na "[Suporte](#)" página ou no "[Matriz de suporte do Data Collector](#)".

Referência do coletor de dados - Serviços

Coleta de dados de nó

O Data Infrastructure Insights reúne métricas do nó no qual você instala um agente.

Instalação

1. A partir de **Observability > Collectors**, escolha um sistema operacional/plataforma. Observe que a instalação de qualquer coletor de dados de integração (Kubernetes, Docker, Apache, etc.) também configurará a coleta de dados de nós.
2. Siga as instruções para configurar o agente. As instruções variam dependendo do tipo de sistema operacional ou Plataforma que você está usando para coletar dados.

Objetos e contadores

Os seguintes objetos e seus contadores são coletados como métricas do Node:

Objeto:	Identificadores:	Atributos:	Pontos de dados:
Sistema de ficheiros do nó	Tipo caminho dispositivo UUUID nó	Nome do nó IP do nó modo de SO do nó	Livres inodes livres inodes totais usados Total usado Total usado usado
Disco do nó	Disco UUUID nó	Nome do nó IP do nó os do nó	Tempo de e/S Total IOPS em andamento ler bytes (por seg) tempo de leitura Total leituras (por seg) tempo de e/S ponderado Total de bytes de gravação (por seg) tempo de gravação Total de gravações (por seg) tempo de gravação tempo de leitura tempo de e/S
CPU de nó	CPU UUUID nó	Nome do nó IP do nó os do nó	Uso da CPU do usuário uso da CPU ocioso uso da CPU processador CPU interrupção uso da CPU uso da CPU DPC CPU uso
Nó	UUID de nó	Nome do nó IP do nó os do nó	Kernel tempo de inicialização Kernel Context switches (por seg) Kernel Entropy available Kernel interrupts (por seg) Kernel processes forked (por seg) memória ativa disponível memória Total memória disponível memória Buffered
Rede de nós	UUID do nó de interface de rede	Nó Nome nó IP nó os	Bytes recebidos bytes recebidos Pacotes enviados Outboud Pacotes descartados erros Outboud Pacotes recebidos Pacotes descartados Pacotes recebidos erros recebidos Pacotes recebidos pacotes recebidos pacotes enviados

Configuração

As informações de configuração e resolução de problemas podem ser encontradas ["Configurando um](#)

[Agente](#)"na página.

ActiveMQ Data Collector

O Data Infrastructure Insights usa esse coletor de dados para coletar métricas do ActiveMQ.

Instalação

1. A partir de **Observability > Collectors**, clique em * Data Collector*. Escolha ActiveMQ.

Selecione o sistema operacional ou a plataforma na qual o agente Telegraf está instalado.

2. Se você ainda não instalou um Agente para coleção ou deseja instalar um Agente para um sistema operacional ou plataforma diferente, clique em *Mostrar instruções* para expandir as "[Instalação do agente](#)" instruções.
3. Selecione a chave de acesso do agente para uso com este coletor de dados. Você pode adicionar uma nova chave de acesso ao agente clicando no botão * chave de acesso ao agente*. Prática recomendada: Use uma chave de acesso de agente diferente somente quando você quiser agrupar coletores de dados, por exemplo, por SO/Plataforma.
4. Siga as etapas de configuração para configurar o coletor de dados. As instruções variam dependendo do tipo de sistema operacional ou Plataforma que você está usando para coletar dados.



ActiveMQ Configuration

Gathers ActiveMQ metrics.

What Operating System or Platform Are You Using?

[Need Help?](#)

Windows

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3) [+ Agent Access Key](#)

*Please ensure that you have a Telegraf Agent in you environment before configuring [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1 Copy the contents below into a new .conf file under the C:\Program Files\telegraf\telegraf.d\ folder. For example, copy the contents to the C:\Program Files\telegraf\telegraf.d\cloudinsights-activemq.conf file.

```
[[inputs.activemq]]
  ## Required ActiveMQ Endpoint, port
  ## USER-ACTION: Provide address of ActiveMQ, HTTP port for ActiveMQ
  server = "<INSERT_ACTIVEMQ_ADDRESS>"
  port = <INSERT_ACTIVEMQ_PORT>
```

- 2 Replace <INSERT_ACTIVEMQ_ADDRESS> with the applicable ActiveMQ server address. Please specify a real machine address, and refrain from using a loopback address.
- 3 Replace <INSERT_ACTIVEMQ_PORT> with the applicable ActiveMQ server HTTP port.
- 4 Replace <INSERT_ACTIVEMQ_USERNAME> and <INSERT_ACTIVEMQ_PASSWORD> with the applicable ActiveMQ credentials.
- 5 Modify 'webadmin' if needed (if ActiveMQ server changes web admin root path).
- 6 Modify 'Namespace' if needed for server disambiguation (to avoid name clashes).
- 7 Restart the Telegraf service.

```
Stop-Service -Name telegraf -ErrorAction SilentlyContinue; Start-Service -Name telegraf
```

Configuração

As informações podem ser encontradas no ["Documentação do ActiveMQ"](#)

Objetos e contadores

Os seguintes objetos e seus contadores são coletados:

Objeto:	Identificadores:	Atributos:	Pontos de dados:
Fila ActiveMQ	Servidor de porta de fila de namespace	UUUID do nó IP do nó de nome do nó	Tamanho da fila de contagem de filas de contagem de filas de contagem de filas de contagem de filas
Assinante ActiveMQ	ID de conexão ID de cliente Port Server namespace	É subscrição do Seletor de SO do nó de nome do nó de destino ativo nó UUID do nó de destino ativo	Contagem de desfila despachada contagem despachado tamanho da fila contagem de espera pendente contagem Enqueue tamanho da fila
Tópico ActiveMQ	Tópico servidor de porta namespace	Nó Nome nó nó IP nó UUID nó os	Tamanho da contagem Enqueue contagem contagem contagem Dequeue consumidores

Solução de problemas

Informações adicionais podem ser encontradas na "[Suporte](#)" página.

Apache Data Collector

Este coletor de dados permite a coleta de dados de servidores Apache em seu localatário.

Pré-requisitos

- Você deve ter seu servidor HTTP Apache configurado e funcionando corretamente
- Você deve ter permissões de sudo ou administrador no host/VM do agente
- Normalmente, o módulo Apache *mod_status* está configurado para expor uma página na localização `/Server-status?auto` do servidor Apache. A opção *ExtendedStatus* deve estar ativada para coletar todos os campos disponíveis. Para obter informações sobre como configurar seu servidor, consulte a documentação do módulo Apache: https://httpd.apache.org/docs/2.4/mod/mod_status.html#enable

Instalação


1. A partir de **Observability > Collectors**, clique em * Data Collector*. Escolha Apache.

Selecione o sistema operacional ou a plataforma na qual o agente Telegraf está instalado.

2. Se você ainda não instalou um Agente para coleção ou deseja instalar um Agente para um sistema operacional ou plataforma diferente, clique em *Mostrar instruções* para expandir as "[Instalação do agente](#)" instruções.
3. Selecione a chave de acesso do agente para uso com este coletor de dados. Você pode adicionar uma nova chave de acesso ao agente clicando no botão * chave de acesso ao agente*. Prática recomendada:

Use uma chave de acesso de agente diferente somente quando você quiser agrupar coletores de dados, por exemplo, por SO/Plataforma.

4. Siga as etapas de configuração para configurar o coletor de dados. As instruções variam dependendo do tipo de sistema operacional ou Plataforma que você está usando para coletar dados.



Apache Configuration

Gathers Apache metrics.

What Operating System or Platform Are You Using?

[Need Help?](#)

Ubuntu & Debian

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3) [+ Agent Access Key](#)

*Please ensure that you have a Telegraf Agent in you environment before configuring. [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1 Ensure that the Apache HTTP Server system you're going to gather metrics on has the 'mod_status' module enabled and exposed. For details refer to the following document.
- 2 Copy the contents below into a new .conf file under the /etc/telegraf/telegraf.d/ directory. For example, copy the contents to the /etc/telegraf/telegraf.d/cloudinsights-apache.conf file.

```
[[inputs.apache]]
  ## An array of URLs to gather from, must be directed at the machine
  ## readable version of the mod_status page including the auto query string.
  ## USER-ACTION: Provide address of apache server, port for apache server, confirm path for
  server-status.
  ## Please specify actual machine IP address, and refrain from using a loopback address. (f.e.
```
- 3 Replace <INSERT_APACHE_ADDRESS> with the applicable Apache server address. Please specify a real machine address, and refrain from using a loopback address.
- 4 Replace <INSERT_APACHE_PORT> with the applicable Apache server port.
- 5 Modify the '/server-status' path in accordance to the Apache server configuration.
- 6 Restart the Telegraf service.

```
systemctl restart telegraf
```

Configuração

O plugin do Telegraf para o servidor HTTP do Apache depende do módulo 'od_status' para ser ativado. Quando isso estiver ativado, o servidor HTTP do Apache irá expor um endpoint HTML que pode ser

visualizado no seu navegador ou raspado para extração do status de todas as configurações do servidor HTTP do Apache.

Compatibilidade:

A configuração foi desenvolvida em relação ao servidor HTTP do Apache versão 2,4.38.

Ativar mod_status:

Ativar e expor os módulos 'mod_status' envolve duas etapas:

- Módulo de ativação
- Expondo estatísticas do módulo

Módulo de ativação:

O carregamento de módulos é controlado pelo arquivo de configuração em '/usr/local/apache/conf/httpd.conf'. Edite o arquivo de configuração e descomente as seguintes linhas:

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

Expondo estatísticas do módulo:

A exposição do 'mod_status' é controlada pelo arquivo de configuração sob '/usr/local/apache2/conf/extra/httpd-info.conf'. Certifique-se de que você tem o seguinte arquivo de configuração (pelo menos, outras diretivas estarão lá):

```
# 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
```

Para obter instruções detalhadas sobre o módulo 'mod_status', consulte ["Documentação do Apache"](#)

Objetos e contadores

Os seguintes objetos e seus contadores são coletados:

Objeto:	Identificadores:	Atributos:	Pontos de dados:
Apache	Servidor de namespace	O tempo de atividade do servidor principal da geração do servidor principal do servidor de geração MPM do nó IP está a parar	Workers ocupados bytes por solicitação bytes por segundo CPU Crianças sistema CPU Crianças Usuário CPU carga CPU sistema CPU usuários conexões assíncronas fechando conexões assíncronas manter Alive conexões assíncronas escrevendo conexões duração total por solicitação trabalhadores ociosos carga média (últimos 1m) carga média (últimos 15m) carga média (últimos 5m) processos solicitações por segundo Total

Solução de problemas

Informações adicionais podem ser encontradas na ["Suporte"](#) página.

Consul Data Collector

O Data Infrastructure Insights usa esse coletor de dados para coletar métricas da Cònsul.

Instalação

1. A partir de **Observability > Collectors**, clique em * Data Collector*. Escolha Cònsul.

Se você não tiver configurado um Agente para coleta, será solicitado ["instale um agente"](#) ao locatário.

Se você já tiver um agente configurado, selecione o sistema operacional ou a Plataforma apropriada e clique em **continuar**.

2. Siga as instruções na tela Consul Configuration (Configuração do cònsul) para configurar o coletor de dados. As instruções variam dependendo do tipo de sistema operacional ou Plataforma que você está usando para coletar dados.

Configuração

As informações podem ser encontradas no ["Documentação do cònsul"](#).

Objetos e contadores para cònsul

Os seguintes objetos e seus contadores são coletados:

Objeto:	Identificadores:	Atributos:	Pontos de dados:
Cônsul	Nó de serviço de ID de verificação de namespace	Nó IP nó os nó UUID Nome do nó Serviço Nome verificar Nome ID do serviço Status	Aviso de aprovação crítica

Solução de problemas

Informações adicionais podem ser encontradas na ["Suporte"](#) página.

Coletor de dados Couchbase

O Data Infrastructure Insights usa esse coletor de dados para coletar métricas do Couchbase.

Instalação

1. A partir de **Observability > Collectors**, clique em * Data Collector*. Escolha Couchbase.

Selecione o sistema operacional ou a plataforma na qual o agente Telegraf está instalado.
2. Se você ainda não instalou um Agente para coleção ou deseja instalar um Agente para um sistema operacional ou plataforma diferente, clique em *Mostrar instruções* para expandir as ["Instalação do agente"](#) instruções.
3. Selecione a chave de acesso do agente para uso com este coletor de dados. Você pode adicionar uma nova chave de acesso ao agente clicando no botão * chave de acesso ao agente*. Prática recomendada: Use uma chave de acesso de agente diferente somente quando você quiser agrupar coletores de dados, por exemplo, por SO/Plataforma.
4. Siga as etapas de configuração para configurar o coletor de dados. As instruções variam dependendo do tipo de sistema operacional ou Plataforma que você está usando para coletar dados.



Couchbase Configuration

Gathers Couchbase metrics.

What Operating System or Platform Are You Using?

[Need Help?](#)

Windows

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)

+ Agent Access Key

*Please ensure that you have a Telegraf Agent in you environment before configuring. [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1 Copy the contents below into a new .conf file under the C:\Program Files\telegraf\telegraf.d\ folder. For example, copy the contents to the C:\Program Files\telegraf\telegraf.d\cloudinsights-couchbase.conf file.

```
## Read metrics from one or many couchbase clusters
[[inputs.couchbase]]
  ## specify servers via a url matching:
  ## [protocol://][:password]@address[:port]
  ## e.g.
  ## http://username:password@127.0.0.1:8090
```

- 2 Replace <INSERT_USERNAME> and <INSERT_PASSWORD> with couchbase server account credentials.
- 3 Replace <INSERT_COUCHBASE_ADDRESS> with the applicable Couchbase address. Please specify a real machine address, and refrain from using a loopback address.
- 4 Replace <INSERT_COUCHBASE_PORT> with the applicable Couchbase port.
- 5 Restart the Telegraf service.

```
Stop-Service -Name telegraf -ErrorAction SilentlyContinue; Start-Service -Name telegraf
```

Configuração

As informações podem ser encontradas no "[Documentação do Couchbase](#)".

Objetos e contadores

Os seguintes objetos e seus contadores são coletados:

Objeto:	Identificadores:	Atributos:	Pontos de dados:
Nó Couchbase	Nome do host do nó Couchbase do namespace Cluster	IP do nó de nome do nó	Memória livre Total de memória
Balde Couchbase	Cluster de bucket do namespace	IP do nó de nome do nó	Dados usados dados Registros disco usado contagem de itens memória operações usadas por segundo cota usada

Solução de problemas

Informações adicionais podem ser encontradas na ["Suporte"](#) página.

CouchDB Data Collector

O Data Infrastructure Insights usa esse coletor de dados para coletar métricas do CouchDB.

Instalação

1. A partir de **Observability > Collectors**, clique em * Data Collector*. Escolha CouchDB.

Selecione o sistema operacional ou a plataforma na qual o agente Telegraf está instalado.
2. Se você ainda não instalou um Agente para coleção ou deseja instalar um Agente para um sistema operacional ou plataforma diferente, clique em *Mostrar instruções* para expandir as ["Instalação do agente"](#) instruções.
3. Selecione a chave de acesso do agente para uso com este coletor de dados. Você pode adicionar uma nova chave de acesso ao agente clicando no botão * chave de acesso ao agente*. Prática recomendada: Use uma chave de acesso de agente diferente somente quando você quiser agrupar coletores de dados, por exemplo, por SO/Plataforma.
4. Siga as etapas de configuração para configurar o coletor de dados. As instruções variam dependendo do tipo de sistema operacional ou Plataforma que você está usando para coletar dados.



CouchDB Configuration

Gathers CouchDB metrics.

What Operating System or Platform Are You Using?

[Need Help?](#)

RHEL & CentOS

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)

+ Agent Access Key

*Please ensure that you have a Telegraf Agent in you environment before configuring. [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1 Copy the contents below into a new `.conf` file under the `/etc/telegraf/telegraf.d/` directory. For example, copy the contents to the `/etc/telegraf/telegraf.d/cloudinsights-couchdb.conf` file.

```
## Read CouchDB Stats from one or more servers
[[inputs.couchdb]]
  ## Works with CouchDB stats endpoints out of the box
  ## Multiple Hosts from which to read CouchDB stats:
  ## USER-ACTION: Provide comma-separated list of couchdb IP(s) and port(s).
  ## USER-ACTION: Multiple Hosts from which to read CouchDB stats:
  ## USER-ACTION: Provide comma-separated list of couchdb IP(s) and port(s).
```

- 2 Replace `<INSERT_COUCHDB_ADDRESS>` with the applicable CouchDB address. Please specify a real machine address, and refrain from using a loopback address.
- 3 Replace `<INSERT_COUCHDB_PORT>` with the applicable CouchDB port.
- 4 Modify the URL if CouchDB monitoring is exposed at different path
- 5 Restart the Telegraf service.

```
systemctl restart telegraf
```

Configuração

As informações podem ser encontradas no "[Documentação do CouchDB](#)".

Objetos e contadores

Os seguintes objetos e seus contadores são coletados:

Objeto:	Identificadores:	Atributos:	Pontos de dados:
CouchDB	Servidor de namespace	IP do nó de nome do nó	Autenticação Cache Hits Autenticação Cache Miss Banco de dados lê Banco de dados escreve bancos de dados abrir arquivos do sistema operacional tempo máximo pedido min tempo de solicitação httpd métodos Copiar httpd Request métodos Excluir httpd Request métodos obter httpd Request métodos Head httpd Request métodos Post httpd Request métodos put Status Codes 200 405 500 Status Codes 304 403 409 Status Codes 400 404 412 Status Codes 401 Status 202 Status Codes 301 Status 201 Status Codes

Solução de problemas

Informações adicionais podem ser encontradas na ["Suporte"](#) página.

Docker Data Collector

O Data Infrastructure Insights usa esse coletor de dados para coletar métricas do Docker.

Instalação

1. A partir de **Observability > Collectors**, clique em * Data Collector*. Escolha Docker.

Se você não tiver configurado um Agente para coleta, será solicitado ["instale um agente"](#) ao locatário.

Se você já tiver um agente configurado, selecione o sistema operacional ou a Plataforma apropriada e clique em **continuar**.

2. Siga as instruções na tela Configuração do Docker para configurar o coletor de dados. As instruções variam dependendo do tipo de sistema operacional ou Plataforma que você está usando para coletar dados.



Docker Configuration

Gathers Docker metrics.

What Operating System or Platform Are You Using?

[Need Help?](#)

RHEL & CentOS

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)

[+ Agent Access Key](#)

*Please ensure that you have a Telegraf Agent in you environment before configuring. [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1 Copy the contents below into a new `.conf` file under the `/etc/telegraf/telegraf.d/` directory. For example, copy the contents to the `/etc/telegraf/telegraf.d/cloudinsights-docker.conf` file.

```
[[inputs.docker]]
  ## Docker Endpoint
  ## To use TCP, set endpoint = "tcp://[[ip]][:port]". By default, Docker uses port 2375 for
  unencrypted and 2376 for encrypted
  ## To use environment variables (ie, docker-machine), set endpoint = "ENV"
```

- 2 Replace `<INSERT_DOCKER_ENDPOINT>` with the applicable Docker endpoint.
- 3 Modify 'Namespace' if needed for server disambiguation (to avoid name clashes).
- 4 Restart the Telegraf service.

```
systemctl restart telegraf
```

Configuração

O plugin de entrada Telegraf para Docker coleta métricas por meio de um soquete UNIX especificado ou um endpoint TCP.

Compatibilidade

A configuração foi desenvolvida em relação ao Docker versão 1.12.6.

Configuração

Acessando o Docker através de um soquete UNIX

Se o agente Telegraf estiver sendo executado no baremetal, adicione o usuário Unix telegraf ao grupo Unix docker executando o seguinte:

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

Se o agente Telegraf estiver sendo executado em um pod Kubernetes, exponha o soquete Unix do Docker mapeando o soquete no pod como um volume e, em seguida, montando esse volume em /var/run/Docker.Sock. Por exemplo, adicione o seguinte ao PodSpec:

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

Em seguida, adicione o seguinte ao recipiente:

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

Observe que o instalador do Data Infrastructure Insights fornecido para a plataforma Kubernetes cuida desse mapeamento automaticamente.

Acesse o Docker por meio de um endpoint TCP

Por padrão, o Docker usa a porta 2375 para acesso não criptografado e a porta 2376 para acesso criptografado.

Objetos e contadores

Os seguintes objetos e seus contadores são coletados:

Objeto:	Identificadores:	Atributos:	Pontos de dados:
Docker Engine	Motor Docker de namespace	Nó Nome nó nó IP UUID Node os Kubernetes Cluster Docker Version Unit	Contentores de memória Containers usados Containers em execução Containers parados CPUs Go Routines imagens Listener Eventos usado descritores de Arquivo dados disponíveis dados totais dados usados metadados disponíveis metadados Total metadados metadados metadados Total metadados usado Pool blocksize
Contêiner do Docker	Nome do contêiner do namespace Docker Engine	Kubernetes Container Hash Kubernetes Container Ports Kubernetes Container Restart Count Kubernetes Container Termination Message Path Kubernetes Container Termination Message Policy Kubernetes Pod Termination Quote Container Image Container Status Container Status Container Version Node Name Kubernetes Container Log Path	Memória ativa memória anônima memória ativa memória Cache memória limite hierárquico memória inativa memória inativa Arquivo inativo memória memória memória memória mapeada memória máxima utilização memória Página Falha memória memória Principal memória pagada memória pagada na memória memória
Docker Container Block io	Nome do contentor Nome do dispositivo Docker Engine	Kubernetes Container Hash Kubernetes Container Ports Kubernetes Container Restart Count Kubernetes Container Termination Message Path Kubernetes Container Termination Message Policy Kubernetes Pod Termination Grace Period Container Image Container Status Container Status Container Version Node Name Kubernetes Container Log Path	Io Service bytes recursive Async io Service bytes recursive Read io Service bytes recursive Sync io Service bytes recursive Total io Service bytes recursive Write io recursive IO Serviced recursive Read IO Serviced Sync io recursive resposta recursiva IO de resposta recursiva Total io Write recursive

Objeto:	Identificadores:	Atributos:	Pontos de dados:
Docker Container Network	Nome do contentor do namespace Network Docker Engine	Container Image Container Status Container Version Node Name Node IP Node UUUID Node os K8s Cluster Docker Version Container ID	RX dropped RX bytes RX erros RX pacotes RX TX dropped TX bytes TX erros TX pacotes TX
CPU de contêiner do Docker	Nome do contêiner do namespace CPU Docker Engine	Kubernetes Container Hash Kubernetes Container Ports Kubernetes Container Restart Count Kubernetes Container Termination Message Path Kubernetes Container Termination Message Policy Kubernetes Pod Termination Quote Form Grace Period Kubernetes Config seen Kubernetes Config	Estrangulamento períodos estrangulados estrangulados períodos estrangulados utilização do tempo estrangulado no modo Kernel utilização no modo Utilizador percentagem utilização do sistema Total de utilização

Solução de problemas

Problema:	Tente isto:
Não vejo minhas métricas do Docker no Data Infrastructure Insights depois de seguir as instruções na página de configuração.	Verifique os logs do agente do Telegraf para ver se ele relata o seguinte erro: E! Erro no plugin [inputs.Docker]: Obteve permissão negada ao tentar se conectar ao socket do daemon do Docker, se isso acontecer, siga as etapas necessárias para fornecer ao agente Telegraf acesso ao socket Unix do Docker, conforme especificado acima.

Informações adicionais podem ser encontradas na ["Suporte"](#) página.

Elasticsearch Data Collector

O Data Infrastructure Insights usa esse coletor de dados para coletar métricas do Elasticsearch.

1. A partir de **Observability > Collectors**, clique em * Data Collector*. Escolha Elasticsearch.
Selecione o sistema operacional ou a plataforma na qual o agente Telegraf está instalado.
2. Se você ainda não instalou um Agente para coleção ou deseja instalar um Agente para um sistema operacional ou plataforma diferente, clique em *Mostrar instruções* para expandir as ["Instalação do agente"](#) instruções.
3. Selecione a chave de acesso do agente para uso com este coletor de dados. Você pode adicionar uma nova chave de acesso ao agente clicando no botão * chave de acesso ao agente*. Prática recomendada: Use uma chave de acesso de agente diferente somente quando você quiser agrupar coletores de dados,

por exemplo, por SO/Plataforma.

4. Siga as etapas de configuração para configurar o coletor de dados. As instruções variam dependendo do tipo de sistema operacional ou Plataforma que você está usando para coletar dados.

Elasticsearch Configuration
Gathers Elasticsearch metrics.

What Operating System or Platform Are You Using? [Need Help?](#)

Ubuntu & Debian

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3) [+ Agent Access Key](#)

*Please ensure that you have a Telegraf Agent in you environment before configuring. [Show Instructions](#)

Follow Configuration Steps [Need Help?](#)

- 1 Copy the contents below into a new .conf file under the /etc/telegraf/telegraf.d/ directory. For example, copy the contents to the /etc/telegraf/telegraf.d/cloudinsights-elasticsearch.conf file.

```
[[inputs.elasticsearch]]
  ## USER-ACTION: Provide comma-separated list of Elasticsearch servers.
  ## Note that for scenarios in which metrics from multiple Elasticsearch clusters are being
  ## sent to Cloud Insights, the Elasticsearch cluster names must be unique.
  ## Please specify actual machine IP address, and refrain from using a loopback address
  ..
```

- 2 Replace <INSERT_ELASTICSEARCH_ADDRESS> with the applicable Elasticsearch address. Please specify a real machine address, and refrain from using a loopback address.
- 3 Replace <INSERT_ELASTICSEARCH_PORT> with the applicable Elasticsearch port.
- 4 Restart the Telegraf service.

```
systemctl restart telegraf
```

Configuração

As informações podem ser encontradas no ["Documentação do Elasticsearch"](#).

Objetos e contadores

Os seguintes objetos e seus contadores são coletados:

Objeto:	Identificadores:	Atributos:
Cluster Elasticsearch	Cluster de namespace	Status do cluster de nome do nó IP
Nó Elasticsearch	Cluster de namespace ES Node ID ES Node IP ES Node Node Node	ID da zona

Solução de problemas

Informações adicionais podem ser encontradas na ["Suporte"](#) página.

Flink Data Collector

O Data Infrastructure Insights usa esse coletor de dados para coletar métricas do Flink.

Instalação

1. A partir de **Observability > Collectors**, clique em * Data Collector*. Escolha Flink.

Selecione o sistema operacional ou a plataforma na qual o agente Telegraf está instalado.

2. Se você ainda não instalou um Agente para coleção ou deseja instalar um Agente para um sistema operacional ou plataforma diferente, clique em *Mostrar instruções* para expandir as ["Instalação do agente"](#) instruções.
3. Selecione a chave de acesso do agente para uso com este coletor de dados. Você pode adicionar uma nova chave de acesso ao agente clicando no botão * chave de acesso ao agente*. Prática recomendada: Use uma chave de acesso de agente diferente somente quando você quiser agrupar coletores de dados, por exemplo, por SO/Plataforma.
4. Siga as etapas de configuração para configurar o coletor de dados. As instruções variam dependendo do tipo de sistema operacional ou Plataforma que você está usando para coletar dados.



Flink Configuration

Gathers Flink metrics.

What Operating System or Platform Are You Using?

[Need Help?](#)

Windows

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)

+ Agent Access Key

*Please ensure that you have a Telegraf Agent in you environment before configuring. [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1 Install Jolokia on your Flink JobManager(s) and Flink Task Manager(s). For details refer to the following [document](#).
- 2 Copy the contents below into a new .conf file under the C:\Program Files\telegraf\telegraf.d\ folder. For example, copy the contents to the C:\Program Files\telegraf\telegraf.d\cloudinsights-flink.conf file.

```
## *****  
## JobManager  
## *****  
[[inputs.jolokia2_agent]]  
  ## USER-ACTION: Provide address(es) of flink Job Manager(s), port for jolokia, add one URL  
  ## USER-ACTION: Provide address(es) of flink Task Manager(s), port for jolokia, add one URL
```

- 3 Replace <INSERT_FLINK_JOBMANAGER_ADDRESS> with the applicable Flink Job Manager address(es). Please specify a real machine address, and refrain from using a loopback address.
- 4 Replace <INSERT_FLINK_TASKMANAGER_ADDRESS> with the applicable Flink Task Manager address(es). Please specify a real machine address, and refrain from using a loopback address.
- 5 Replace <INSERT_JOLOKIA_PORT> with the applicable jolokia port.
- 6 Modify 'Namespace' if needed for server disambiguation (to avoid name clashes).
- 7 Modify 'Cluster' if needed for Flink cluster designation.
- 8 Restart the Telegraf service.

```
Stop-Service -Name telegraf -ErrorAction SilentlyContinue; Start-Service -Name telegraf
```

Configuração

Uma implantação completa do Flink envolve os seguintes componentes:

JobManager: O sistema primário Flink. Coordena uma série de TaskManagers. Em uma configuração de alta disponibilidade, o sistema terá mais de um JobManager. **TaskManager:** É aqui que os operadores Flink são executados. O plugin Flink é baseado no plugin Jolokia da telegraf. Como um requisito para reunir informações de todos os componentes do Flink, o JMX precisa ser configurado e exposto via Jolokia em todos os componentes.

Compatibilidade

A configuração foi desenvolvida em relação ao Flink versão 1,7.0.

Configuração

Jolokia Agent JAR

Para todos os componentes individuais, uma versão do arquivo jar do agente Jolokia deve ser baixada. A versão testada contra foi "[Agente Jolokia 1.6.0](#)".

As instruções abaixo supõem que o arquivo jar baixado (jolokia-jvm-1,6.0-Agent.jar) é colocado sob a localização '/opt/flink/lib/'.

JobManager

Para configurar o JobManager para expor a API Jolokia, você pode configurar a seguinte variável de ambiente em seus nós e reiniciar o JobManager:

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

Você pode escolher um porto diferente para Jolokia (8778). Se você tem um IP interno para bloquear Jolokia, você pode substituir o "Catch All" 0.0.0.0 pelo seu próprio IP. Observe que esse IP precisa ser acessível a partir do plugin telegraf.

TaskManager

Para configurar o(s) TaskManager(s) para expor a API Jolokia, você pode configurar a seguinte variável de ambiente nos nós e reiniciar o TaskManager:

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

Você pode escolher um porto diferente para Jolokia (8778). Se você tem um IP interno para bloquear Jolokia, você pode substituir o "Catch All" 0.0.0.0 pelo seu próprio IP. Observe que esse IP precisa ser acessível a partir do plugin telegraf.

Objetos e contadores

Os seguintes objetos e seus contadores são coletados:

Objeto:	Identificadores:	Atributos:	Pontos de dados:
Flink Task Manager	Servidor de namespace de cluster	Nome do nó IP do nó de ID do Gestor de tarefas	<p>Rede disponível</p> <p>segmentos de memória rede</p> <p>Total segmentos de memória coleção de lixo PS</p> <p>MarkSweep contagem de lixo PS</p> <p>MarkSweep tempo coleta de lixo contagem de scavenge contagem de lixo contagem de lixo PS scavenge tempo Heap memória comprometida memória de Heap memória de Heap máximo memória de heap usada contagem de threads Daemon contagem de threads contagem de threads contagem de threads contagem de threads Total de threads iniciado</p>
Trabalho Flink	ID do trabalho do servidor de namespace do cluster	<p>Nome do nó Nome do trabalho</p> <p>Nome do nó IP último Checkpoint caminho Externo tempo de reinício</p>	<p>Tempo de inatividade</p> <p>reinicializações completas último alinhamento do Checkpoint Buffered Last Checkpoint duração último tamanho do Checkpoint número de Checkpoints concluídos número de Checkpoints falhados número de Checkpoints em curso número de Checkpoints uptime</p>
Flink Job Manager	Servidor de namespace de cluster	IP do nó de nome do nó	<p>Coleção de lixo PS</p> <p>MarkSweep contagem de lixo PS</p> <p>MarkSweep tempo coleta de lixo contagem de scavenge contagem de lixo PS scavenge tempo Heap memória comprometida memória de heap memória de Heap máximo memória de heap usada número registrado</p> <p>Gerenciadores de tarefas em execução Slots de tarefa disponíveis contagem de</p>

Objeto:	Identificadores:	Atributos:	Pontos de dados:
Tarefa Flink	ID da tarefa do ID da tarefa do namespace do cluster	Nome do nó do servidor Nome do trabalho Sub-tarefa Índice tentativa da tarefa Número da tentativa da tarefa Nome da tarefa Gestor de tarefas ID nó IP Atual marca de água da entrada	Buffers em uso do pool Buffers em comprimento da fila Buffers out uso do pool Buffers out comprimento da fila Número Buffers em número local Buffers em número local por segundo Número Buffers em número local por segundo Número de taxa Buffers em número remoto por segundo Número de contagem de Registros por segundo Número local por segundo Número de Registros por segundo Número remoto por segundo Número de Registros por segundo Número
Operador tarefa Flink	ID da tarefa ID do operador do namespace do cluster	Nome do nó do servidor Nome do trabalho Nome do Operador Sub-tarefa ID tentativa da tarefa Número tentativa da tarefa Nome da tarefa Nome da tarefa Gestor de tarefas ID Node IP	Entrada atual marca de água Saída atual número de marca de água Registros em número Registros em por segundo Número de contagem Registros em por segundo Número de registo para fora Número de contagem Número de registros para fora por segundo Número de taxa de registo

Solução de problemas

Informações adicionais podem ser encontradas na ["Suporte"](#) página.

Coletor de dados Hadoop

O Data Infrastructure Insights usa esse coletor de dados para coletar métricas do Hadoop.

Instalação


1. A partir de **Observability > Collectors**, clique em * Data Collector*. Escolha Hadoop.

Selecione o sistema operacional ou a plataforma na qual o agente Telegraf está instalado.

2. Se você ainda não instalou um Agente para coleção ou deseja instalar um Agente para um sistema operacional ou plataforma diferente, clique em *Mostrar instruções* para expandir as ["Instalação do agente"](#)

instruções.

3. Selecione a chave de acesso do agente para uso com este coletor de dados. Você pode adicionar uma nova chave de acesso ao agente clicando no botão * chave de acesso ao agente*. Prática recomendada: Use uma chave de acesso de agente diferente somente quando você quiser agrupar coletores de dados, por exemplo, por SO/Plataforma.
4. Siga as etapas de configuração para configurar o coletor de dados. As instruções variam dependendo do tipo de sistema operacional ou Plataforma que você está usando para coletar dados.



Hadoop Configuration

Gathers Hadoop metrics.

What Operating System or Platform Are You Using?

[Need Help?](#)

Ubuntu & Debian

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3) [+ Agent Access Key](#)

*Please ensure that you have a Telegraf Agent in you environment before configuring [Show Instructions](#)

Follow Configuration Steps

Need Help?

- 1 Install Jolokia on your Hadoop NameNode, Secondary NameNode, DataNode(s), ResourceManager, NodeManager(s) and JobHistoryServer. For details refer to the following [document](#).
- 2 Copy the contents below into a new .conf file under the /etc/telegraf/telegraf.d/ directory. For example, copy the contents to the /etc/telegraf/telegraf.d/cloudinsights-hadoop.conf file.

```
#####  
# NAMENODE #  
#####  
[[inputs.jolokia2_agent]]  
  ## USER-ACTION: Provide address(es) of Hadoop NameNode, port for jolokia  
  ## Please specify real machine address and refrain from using a loopback address
```

- 3 Replace <INSERT_HADOOP_NAMENODE_ADDRESS> with the applicable Hadoop NameNode address. Please specify a real machine address, and refrain from using a loopback address. Replace corresponding <INSERT_JOLOKIA_PORT> with the NameNode's assigned Jolokia port.
- 4 Replace <INSERT_HADOOP_SECONDARYNAMENODE_ADDRESS> with the applicable Hadoop Secondary NameNode address. Please specify a real machine address, and refrain from using a loopback address. Replace corresponding <INSERT_JOLOKIA_PORT> with the Secondary NameNode's assigned Jolokia port.
- 5 Replace <INSERT_HADOOP_DATANODE_ADDRESS> with the applicable Hadoop DataNode address(es). Please specify a real machine address, and refrain from using a loopback address. Replace corresponding <INSERT_JOLOKIA_PORT> with the DataNode's assigned Jolokia port.
- 6 Replace <INSERT_HADOOP_RESOURCEMANAGER_ADDRESS> with the applicable Hadoop ResourceManager address. Please specify a real machine address, and refrain from using a loopback address. Replace corresponding <INSERT_JOLOKIA_PORT> with the ResourceManager's assigned Jolokia port.
- 7 Replace <INSERT_HADOOP_NODEMANAGER_ADDRESS> with the applicable Hadoop NodeManager address(es). Please specify a real machine address, and refrain from using a loopback address. Replace corresponding <INSERT_JOLOKIA_PORT> with the NodeManager's assigned Jolokia port.
- 8 Replace <INSERT_HADOOP_JOBHISTORYSERVER_ADDRESS> with the applicable Hadoop Job History Server address. Please specify a real machine address, and refrain from using a loopback address. Replace corresponding <INSERT_JOLOKIA_PORT> with the Job History Server's assigned Jolokia port.
- 9 Modify 'Namespace' if needed for server disambiguation (to avoid name clashes).
- 10 Modify 'Cluster' if needed for Hadoop cluster designation.
- 11 Restart the Telegraf service.

```
systemctl restart telegraf
```

Configuração

Uma implantação completa do Hadoop envolve os seguintes componentes:

- NameNode: O sistema principal do Hadoop Distributed File System (HDFS). Coordena uma série de DataNodes.

- NameNode secundário: Um failover morno para o NameNode principal. No Hadoop, a promoção para NameNode não ocorre automaticamente. NameNode secundário reúne informações do NameNode para estar pronto para ser promovido quando necessário.
- DataNode: Proprietário real dos dados.
- ResourceManager: O sistema primário de computação (yarn). Coordena uma série de NodeManagers.
- NodeManager: O recurso para computação. Local real para execução de aplicativos.
- JobHistoryServer: Responsável por atender todas as solicitações relacionadas ao histórico de tarefas.

O plugin Hadoop é baseado no plugin Jolokia da telegraf. Como um requisito para reunir informações de todos os componentes do Hadoop, o JMX precisa ser configurado e exposto via Jolokia em todos os componentes.

Compatibilidade

A configuração foi desenvolvida em relação ao Hadoop versão 2,9.2.

Configuração

Jolokia Agent JAR

Para todos os componentes individuais, uma versão do arquivo jar do agente Jolokia deve ser baixada. A versão testada contra foi "[Agente Jolokia 1.6.0](#)".

As instruções abaixo supõem que o arquivo jar baixado (jolokia-jvm-1,6.0-Agent.jar) é colocado sob o local '/opt/hadoop/lib/'.

NameNode

Para configurar o NameNode para expor a API Jolokia, você pode configurar o seguinte em <HADOOP_HOME>/etc/Hadoop/Hadoop-env.sh:

```
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.
```

NameNode secundário

Para configurar o NameNode secundário para expor a API Jolokia, você pode configurar o seguinte em <HADOOP_HOME>/etc/Hadoop/Hadoop-env.sh:

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

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

DataNode

Para configurar os DataNodes para expor a API Jolokia, você pode configurar o seguinte em <HADOOP_HOME>/etc/Hadoop/Hadoop-env.sh:

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

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

ResourceManager

Para configurar o ResourceManager para expor a API Jolokia, você pode configurar o seguinte em <HADOOP_HOME>/etc/hadoop/Hadoop-env.sh:

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

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

NodeManager

Para configurar o NodeManagers para expor a API Jolokia, você pode configurar o seguinte em <HADOOP_HOME>/etc/Hadoop/Hadoop-env.sh:

```
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

Para configurar o JobHistoryServer para expor a API Jolokia, você pode configurar o seguinte em <HADOOP_HOME>/etc/Hadoop/Hadoop-env.sh:

```
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.

Objetos e contadores

Os seguintes objetos e seus contadores são coletados:

Objeto:	Identificadores:	Atributos:
NameNode secundário Hadoop	Servidor de namespace de cluster	Node Name Node IP Compile Info versão
Hadoop NodeManager	Servidor de namespace de cluster	IP do nó de nome do nó
Hadoop ResourceManager	Servidor de namespace de cluster	IP do nó de nome do nó
DataNode do Hadoop	Servidor de namespace de cluster	Versão do ID do cluster IP do nó de nome do nó
NameNode Hadoop	Servidor de namespace de cluster	ID da transação IP do nó Nome do nó último tempo escrito desde a última versão carregada Edits HA State File System State Block Pool ID Cluster Info compilação versão contagem de versão distinta
Hadoop JobHistoryServer	Servidor de namespace de cluster	IP do nó de nome do nó

Solução de problemas

Informações adicionais podem ser encontradas na ["Suporte"](#) página.

Coletor de dados HAProxy

O Data Infrastructure Insights usa esse coletor de dados para coletar métricas do HAProxy.

Instalação

1. A partir de **Observability > Collectors**, clique em * Data Collector*. Escolha HAProxy.

Selecione o sistema operacional ou a plataforma na qual o agente Telegraf está instalado.

2. Se você ainda não instalou um Agente para coleção ou deseja instalar um Agente para um sistema operacional ou plataforma diferente, clique em *Mostrar instruções* para expandir as "[Instalação do agente](#)" instruções.
3. Selecione a chave de acesso do agente para uso com este coletor de dados. Você pode adicionar uma nova chave de acesso ao agente clicando no botão * chave de acesso ao agente*. Prática recomendada: Use uma chave de acesso de agente diferente somente quando você quiser agrupar coletores de dados, por exemplo, por SO/Plataforma.
4. Siga as etapas de configuração para configurar o coletor de dados. As instruções variam dependendo do tipo de sistema operacional ou Plataforma que você está usando para coletar dados.



HAProxy Configuration

Gathers HAProxy metrics.

What Operating System or Platform Are You Using?

[Need Help?](#)

Ubuntu & Debian

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3) [+ Agent Access Key](#)

*Please ensure that you have a Telegraf Agent in you environment before configuring. [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1 Ensure that the HAProxy system you're going to gather metrics on has 'stats enable' option. For details refer to the following [document](#).
- 2 Copy the contents below into a new .conf file under the /etc/telegraf/telegraf.d/ directory. For example, copy the contents to the /etc/telegraf/telegraf.d/cloudinsights-haproxy.conf file.

```
# Read metrics of HAProxy, via socket or HTTP stats page
[[inputs.haproxy]]
  ## An array of address to gather stats about. Specify an ip on hostname
  ## with optional port. ie localhost, 10.10.3.33:1936, etc.
  ## Make sure you specify the complete path to the stats endpoint
  ## <url> for the endpoint? ie http://10.10.3.33:1936/haproxy?stats
```

- 3 Replace <INSERT_HAPROXY_ADDRESS> with the applicable HAProxy server address. Please specify a real machine address, and refrain from using a loopback address.
- 4 Replace <INSERT_HAPROXY_PORT> with the applicable HAProxy server port.
- 5 Modify the 'haproxy?stats' path in accordance to the HAProxy server configuration.
- 6 Modify 'username' and 'password' in accordance to the HAProxy server configuration (if credentials are required).
- 7 Modify 'Namespace' if needed for server disambiguation (to avoid name clashes).
- 8 Restart the Telegraf service.

```
systemctl restart telegraf
```

Configuração

O plugin da Telegraf para HAProxy depende da habilitação do HAProxy Stats. Esta é uma configuração incorporada no HAProxy, mas não está ativada fora da caixa. Quando ativado, o HAProxy irá expor um

endpoint HTML que pode ser visualizado no seu navegador ou eliminado para extração do estado de todas as configurações do HAProxy.

Compatibilidade:

A configuração foi desenvolvida contra o HAProxy versão 1,9.4.

Configuração:

Para ativar as estatísticas, edite o arquivo de configuração do haproxy e adicione as seguintes linhas após a seção 'defeitos', usando seu próprio usuário/senha e/ou URL do haproxy:

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

A seguir está um exemplo simplificado de arquivo de configuração com estatísticas ativadas:

```
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
```

Para obter instruções completas e atualizadas, consulte o "[Documentação do HAProxy](#)".

Objetos e contadores

Os seguintes objetos e seus contadores são coletados:

Objeto:	Identificadores:	Atributos:	Pontos de dados:
HAProxy Frontend	Proxy de endereço de namespace	Nome do nó IP do nó Proxy ID Mode Process id Sessions Rate Limit Server id Sessions Limit Status	Bytes in bytes out Cache Hits Cache Lookups Compression bytes Bypass Compression bytes out Compression bytes out Compression respostas taxa de conexão Max conexões Total de solicitações negadas pela regra de conexão solicitações negadas por preocupações de segurança solicitações negadas por solicitações de regras de sessão erros respostas 1xx 4xx respostas 2xx 5xx respostas 3xx respostas outras solicitações sessões intercetadas sessões Rate Requests Rate Requests Rate Max Total de sessões sessões reescreve

Objeto:	Identificadores:	Atributos:	Pontos de dados:
Servidor HAProxy	Servidor Proxy de Endereço de namespace	Node IP Name Check Time to Finish Check Fall Configuration Check Health Value Check Rise Configuration Check Status ID Proxy ID Last Change Time Last Session Time Process id Server id Status Weight	Servidores ativos servidores de backup bytes em bytes out check Downs Check Fails Cliente aborta conexões tempo médio tempo de inatividade Total respostas negadas erros de conexão respostas 1xx respostas 2xx respostas 3xx respostas 4xx respostas 5xx respostas outro servidor selecionado Total fila atual fila máxima tempo média sessões por segundo sessões por segundo tempo máximo reutilização de conexão tempo média sessões sessões sessões sessões Max transferência de servidor aborta sessões Total de sessões Redespachos pedidos Redespachos pedidos RRecrutamento de solicitações
Backend HAProxy	Proxy de endereço de namespace	Nome do nó IP ID do proxy último tempo alteração tempo último modo sessão ID do processo ID do servidor sessões limite peso do estado	Servidores ativos servidores de backup bytes em bytes out Cache Hits Cache Lookups Check Downs Cliente aborta compactação bytes Bypass compactação bytes em compressão bytes out Compression respostas conexões tempo médio tempo de inatividade Total solicitações negadas por preocupações de Segurança respostas negadas por preocupações de Segurança erros de conexão erros de resposta respostas 1xx 4xx respostas 2xx 5xx respostas 3xx respostas

Solução de problemas

Informações adicionais podem ser encontradas na ["Suporte"](#) página.

Coletor de dados JVM

O Data Infrastructure Insights usa esse coletor de dados para coletar métricas da JVM.

Instalação

1. A partir de **Observability > Collectors**, clique em * Data Collector*. Escolha JVM.

Selecione o sistema operacional ou a plataforma na qual o agente Telegraf está instalado.

2. Se você ainda não instalou um Agente para coleção ou deseja instalar um Agente para um sistema operacional ou plataforma diferente, clique em *Mostrar instruções* para expandir as ["Instalação do agente"](#) instruções.
3. Selecione a chave de acesso do agente para uso com este coletor de dados. Você pode adicionar uma nova chave de acesso ao agente clicando no botão * chave de acesso ao agente*. Prática recomendada: Use uma chave de acesso de agente diferente somente quando você quiser agrupar coletores de dados, por exemplo, por SO/Plataforma.
4. Siga as etapas de configuração para configurar o coletor de dados. As instruções variam dependendo do tipo de sistema operacional ou Plataforma que você está usando para coletar dados.



Java Configuration

Gathers JVM metrics.

What Operating System or Platform Are You Using?

[Need Help?](#)

RHEL & CentOS

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)

[+ Agent Access Key](#)

*Please ensure that you have a Telegraf Agent in you environment before configuring. [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1 Install Jolokia on your JVMs. For details refer to the following [document](#).
- 2 Copy the contents below into a new .conf file under the /etc/telegraf/telegraf.d/ directory. For example, copy the contents to the /etc/telegraf/telegraf.d/cloudinsights-jvm.conf file.

```
# Read JMX metrics through Jolokia
[[inputs.jolokia2_agent]]
  # USER-ACTION: Provide address(es) of JVM, port for jolokia, add one URL for each JVM in
  # your cluster
  # Please specify actual machine IP address, and refrain from using a loopback address (i.e.
  # 10.1.1.1 or 127.0.0.1)
```

- 3 Replace <INSERT_JVM_ADDRESS> with the applicable JVM address. Please specify a real machine address, and refrain from using a loopback address.
- 4 Replace <INSERT_JOLOKIA_PORT> with the applicable JVM jolokia port.
- 5 Modify 'Namespace' if needed for server disambiguation (to avoid name clashes).
- 6 Restart the Telegraf service.

```
systemctl restart telegraf
```

Configuração

As informações podem ser encontradas em "[Documentação do JVM](#)".

Objetos e contadores

Os seguintes objetos e seus contadores são coletados:

Objeto:	Identificadores:	Atributos:	Pontos de dados:
JVM	JVM do namespace	Arquitetura OS Nome do SO versão Runtime especificação Runtime especificação Runtime do fornecedor Runtime especificação versão tempo de execução VM Nome tempo de execução VM Nome tempo de execução VM Vendor Runtime versão VM Nome nó IP	Classe carregada Classe carregada Total Class Unloaded Memory Heap Consolidated Memory Heap Init Memory Heap used Max Memory Heap used Memory Non Heap Consolidated Memory Non Heap Init Memory Non Heap Max Memory Non Heap used Memory Objects Pending G1 Sequence os Processors Available G1 G1 G1

Solução de problemas

Informações adicionais podem ser encontradas na ["Suporte"](#) página.

Kafka Data Collector

O Data Infrastructure Insights usa esse coletor de dados para coletar métricas do Kafka.

Instalação

1. A partir de **Observability > Collectors**, clique em * Data Collector*. Escolha Kafka.

Selecione o sistema operacional ou a plataforma na qual o agente Telegraf está instalado.

2. Se você ainda não instalou um Agente para coleção ou deseja instalar um Agente para um sistema operacional ou plataforma diferente, clique em *Mostrar instruções* para expandir as ["Instalação do agente"](#) instruções.
3. Selecione a chave de acesso do agente para uso com este coletor de dados. Você pode adicionar uma nova chave de acesso ao agente clicando no botão * chave de acesso ao agente*. Prática recomendada: Use uma chave de acesso de agente diferente somente quando você quiser agrupar coletores de dados, por exemplo, por SO/Plataforma.
4. Siga as etapas de configuração para configurar o coletor de dados. As instruções variam dependendo do tipo de sistema operacional ou Plataforma que você está usando para coletar dados.



Kafka Configuration

Gathers Kafka metrics.

What Operating System or Platform Are You Using?

[Need Help?](#)

Windows

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3) [+ Agent Access Key](#)

*Please ensure that you have a Telegraf Agent in you environment before configuring [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1 Install Jolokia on your Kafka brokers. For details refer to the following [document](#).
- 2 Copy the contents below into a new .conf file under the C:\Program Files\telegraf\telegraf.d\ folder. For example, copy the contents to the C:\Program Files\telegraf\telegraf.d\cloudinsights-kafka.conf file.

```
# Read JMX metrics through Jolokia
[[inputs.jolokia2_agent]]
  ## USER-ACTION: Provide address(es) of kafka broker(s), port for jolokia, add one URL for
  ## each broker in your cluster
  ## Please specify actual machine IP address, and refrain from using a loopback address (i.e.
  ## 127.0.0.1)
```

- 3 Replace <INSERT_KAFKA_BROKER_ADDRESS> with the applicable Kafka broker address. Please specify a real machine address, and refrain from using a loopback address.
- 4 Replace <INSERT_JOLOKIA_PORT> with the applicable Kafka broker jolokia port.
- 5 Modify 'Namespace' if needed for server disambiguation (to avoid name clashes).
- 6 Modify 'Cluster' if needed for Kafka cluster designation.
- 7 Restart the Telegraf service.

```
Stop-Service -Name telegraf -ErrorAction SilentlyContinue; Start-Service -Name telegraf
```

Configuração

O plugin Kafka é baseado no plugin Jolokia do telegraf. Como tal, um requisito para reunir informações de todos os corretores Kafka, o JMX precisa ser configurado e exposto via Jolokia em todos os componentes.

Compatibilidade

A configuração foi desenvolvida em relação ao Kafka versão 0.11.0.2.

Configuração

Todas as instruções abaixo assumem que o local de instalação do kafka é '/opt/kafka'. Você pode adaptar as instruções abaixo para refletir o local de instalação.

Jolokia Agent JAR

Uma versão o arquivo jar do agente Jolokia deve ser "transferido". A versão testada foi o agente Jolokia 1,6.0.

As instruções abaixo supõem que o arquivo jar baixado (jolokia-jvm-1,6.0-Agent.jar) é colocado sob o local '/opt/kafka/libs/'.

Kafka Brokers

Para configurar o Kafka Brokers para expor a API Jolokia, você pode adicionar o seguinte em <KAFKA_HOME>/bin/kafka-server-start.sh, imediatamente antes da chamada 'kafka-run-class.sh':

```
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"
```

Observe que o exemplo acima está usando 'hostname -i' para configurar a variável de ambiente 'RMI_HOSTNAME'. Em várias máquinas IP, isso precisará ser ajustado para reunir o IP que você se importa para conexões RMI.

Você pode escolher uma porta diferente para JMX (9999 acima) e Jolokia (8778). Se você tem um IP interno para bloquear Jolokia, você pode substituir o "Catch All" 0.0.0.0 pelo seu próprio IP. Observe que esse IP precisa ser acessível a partir do plugin telegraf. Você pode usar a opção '-Dcom.sun.management.jmxremote.authenticate=false' se não quiser autenticar. Use por sua própria conta e risco.

Objetos e contadores

Os seguintes objetos e seus contadores são coletados:

Objeto:	Identificadores:	Atributos:
Kafka Broker	Agente de namespace de cluster	IP do nó de nome do nó

Solução de problemas

Informações adicionais podem ser encontradas na "Suporte" página.

Kibana Data Collector

O Data Infrastructure Insights usa esse coletor de dados para coletar métricas da Kibana.

Instalação

1. A partir de **Observability > Collectors**, clique em * Data Collector*. Escolha Kibana.

Selecione o sistema operacional ou a plataforma na qual o agente Telegraf está instalado.

2. Se você ainda não instalou um Agente para coleção ou deseja instalar um Agente para um sistema operacional ou plataforma diferente, clique em *Mostrar instruções* para expandir as "[Instalação do agente](#)" instruções.
3. Selecione a chave de acesso do agente para uso com este coletor de dados. Você pode adicionar uma nova chave de acesso ao agente clicando no botão * chave de acesso ao agente*. Prática recomendada: Use uma chave de acesso de agente diferente somente quando você quiser agrupar coletores de dados, por exemplo, por SO/Plataforma.
4. Siga as etapas de configuração para configurar o coletor de dados. As instruções variam dependendo do tipo de sistema operacional ou Plataforma que você está usando para coletar dados.



Kibana Configuration

Gathers Kibana metrics.

What Operating System or Platform Are You Using?

[Need Help?](#)

Ubuntu & Debian

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)

+ Agent Access Key

*Please ensure that you have a Telegraf Agent in you environment before configuring. [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1 Copy the contents below into a new `.conf` file under the `/etc/telegraf/telegraf.d/` directory. For example, copy the contents to the `/etc/telegraf/telegraf.d/cloudinsights-kibana.conf` file.

```
[[inputs.kibana]]
  ## specify a list of one or more Kibana servers
  ## USER-ACTION: Provide address of kibana server(s), port(s) for kibana server
  ## Please specify actual machine IP address, and refrain from using a loopback address (i.e.
  localhost or 127.0.0.1).
```

- 2 Replace `<INSERT_KIBANA_ADDRESS>` with the applicable Kibana server address. Please specify a real machine address, and refrain from using a loopback address.
- 3 Replace `<INSERT_KIBANA_PORT>` with the applicable Kibana server port.
- 4 Replace `'username'` and `'pa$$word'` with the applicable Kibana server authentication credentials as needed, and uncomment the lines.
- 5 Modify `'Namespace'` if needed for server disambiguation (to avoid name clashes).
- 6 Restart the Telegraf service.

```
systemctl restart telegraf
```

Configuração

As informações podem ser encontradas no ["Documentação do Kibana"](#).

Objetos e contadores

Os seguintes objetos e seus contadores são coletados:

Objeto:	Identificadores:	Atributos:	Pontos de dados:
Kibana	Endereço do namespace	Estado da versão do nome do nó IP do nó	Conexões simultâneas Heap Max Heap usou solicitações por segundo tempo de resposta tempo de resposta tempo de resposta tempo de resposta máximo de tempo de atividade

Solução de problemas

Informações adicionais podem ser encontradas na ["Suporte"](#) página.

Instalação e configuração do operador de monitoramento Kubernetes

O Data Infrastructure Insights oferece a coleção **Operador de Monitoramento do Kubernetes** para Kubernetes. Navegue até **Kubernetes > Collectors > Kubernetes Collector** para implantar um novo operador.

Antes de instalar o operador de monitoramento do Kubernetes

Consulte ["Pré-requisitos"](#) a documentação antes de instalar ou atualizar o Operador de Monitoramento do Kubernetes.

Instalando o Operador de Monitoramento do 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

clustername

Namespace

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.

3 Optional: Upload the operator images to your private repository

By default, the operator pulls container images from the Cloud Insights repository. To use a private repository, download the required images using the Image Pull command. Then upload them to your private repository maintaining the same tags and directory structure. Finally, update the image paths in `operator-deployment.yaml` and the docker repository settings in `operator-config.yaml`. For more information review [the documentation](#).

Copy Image Pull Snippet

Reveal Image Pull Snippet

Copy Repository Password

Reveal Repository Password

This password is valid for 24 hours.

4 Optional: Review available configuration options

Configure custom options such as proxy and private repository settings. Review the [instructions and available options](#).

5 Deploy the operator (create new or upgrade existing)

Execute the `kubectl` snippet to apply the following operator YAML files.

- `operator-setup.yaml` - Create the operator's dependencies.
- `operator-secrets.yaml` - Create secrets holding your API key.
- `operator-deployment.yaml`, `operator-cr.yaml` - Deploy the NetApp Kubernetes Monitoring Operator.
- `operator-config.yaml` - Apply the configuration settings if not already present.

Copy kubectl Apply Snippet

Reveal kubectl Apply Snippet

After deploying the operator, **delete or securely store `operator-secrets.yaml`**.

6 Next

Etapas para instalar o agente do operador de monitoramento do Kubernetes no Kubernetes:

1. Insira um nome de cluster e um namespace exclusivos. Se você [a atualizar](#) é de um operador Kubernetes anterior, use o mesmo nome de cluster e namespace.
2. Uma vez que eles são inseridos, você pode copiar o snippet de comando de download para a área de transferência.
3. Cole o snippet em uma janela `bash` e execute-o. Os ficheiros de instalação do Operador serão transferidos. Observe que o snippet tem uma chave exclusiva e é válido por 24 horas.
4. Se você tiver um repositório personalizado ou privado, copie o trecho opcional Image Pull, cole-o em um shell `bash` e execute-o. Depois que as imagens tiverem sido puxadas, copie-as para o seu repositório privado. Certifique-se de manter as mesmas tags e estrutura de pastas. Atualize os caminhos em `operator-deployment.yaml`, bem como as configurações do repositório docker em `operator-config.yaml`.
5. Se desejar, revise as opções de configuração disponíveis, como proxy ou configurações de repositório privado. Você pode ler mais sobre "[opções de configuração](#)".
6. Quando estiver pronto, implante o Operador copiando o snippet de aplicação kubectl, baixando-o e executando-o.
7. A instalação prossegue automaticamente. Quando estiver concluído, clique no botão `Next`.
8. Quando a instalação estiver concluída, clique no botão `Next`. Certifique-se também de excluir ou armazenar com segurança o arquivo `operator-secrets.yaml`.

Se estiver usando um proxy, leia sobre [configurando proxy](#).

Se você tiver um repositório personalizado, leia sobre [usando um repositório docker personalizado/privado](#).

Componentes de monitoramento do Kubernetes

O monitoramento do Kubernetes do Data Infrastructure Insights é composto por quatro componentes de monitoramento:

- Métricas do cluster
- Desempenho de rede e mapa (opcional)
- Registos de eventos (opcional)
- Análise de mudança (opcional)

Os componentes opcionais acima são ativados por padrão para cada coletor do Kubernetes; se você decidir que não precisa de um componente para um coletor específico, você pode desativá-lo navegando para **Kubernetes > coletores** e selecionando *Modificar implantação* no menu "três pontos" do coletor à direita da tela.

NetApp / Observability / Collectors

Data Collectors 21 Acquisition Units 4 **Kubernetes Collectors**

Kubernetes Collectors (13)

[View Upgrade/Delete Documentation](#)


[+ Kubernetes Collector](#)

Filter...

Cluster Name ↑	Status	Operator Version	Network Performance and Map	Change Analysis	
au-pod	Outdated	1.1540.0	1.347.0	1.162.0	⋮
jks-troublemaker	Latest	1.1579.0	N/A	1.201.0	⋮
oom-test	Outdated	1.1555.0	N/A	1.161.0	⋮

Modify Deployment

O ecrã mostra o estado atual de cada componente e permite desativar ou ativar componentes para esse coletor, conforme necessário.

 **kubernetes**
Kubernetes

Modify Deployment

Cluster Information

Kubernetes Cluster
ci-demo-01

Network Performance and Map
Enabled - Online

Event Logs
Enabled - Online

Change Analysis
Enabled - Online

Deployment Options

[Need Help?](#)

- Network Performance and Map
- Event Logs
- Change Analysis

Cancel

Complete Modification

Atualização para o operador de monitoramento mais recente do Kubernetes

Determine se existe um AgentConfiguration com o Operador existente (se o seu namespace não for o *NetApp-monitoring* padrão, substitua o namespace apropriado):

```
kubectl -n netapp-monitoring get agentconfiguration netapp-monitoring-configuration
```

Se existir uma configuração AgentConfiguration:

- **Instale** O operador mais recente sobre o operador existente.
 - Certifique-se de que está [puxando as imagens mais recentes do recipiente](#) se estiver a utilizar um repositório personalizado.

Se o AgentConfiguration não existir:

- Anote o nome do cluster conforme reconhecido pelo Data Infrastructure Insights (se o namespace não for o monitoramento padrão do NetApp, substitua o namespace apropriado):

```
kubectl -n netapp-monitoring get agent -o jsonpath='{.items[0].spec.cluster-name}'
```

* Crie uma cópia de segurança do Operador existente (se o seu namespace não for o NetApp-monitoring predefinido, substitua o namespace apropriado):

```
kubectl -n netapp-monitoring get agent -o yaml > agent_backup.yaml
```

* <<to-remove-the-kubernetes-monitoring-operator,Desinstalar>> O operador existente.

* <<installing-the-kubernetes-monitoring-operator,Instale>> O operador mais recente.

- Use o mesmo nome de cluster.
- Depois de baixar os arquivos YAML do Operador mais recentes, coloque as personalizações encontradas no Agent_backup.yaml para o operador-config.yaml baixado antes de implantar.
- Certifique-se de que está [puxando as imagens mais recentes do recipiente](#) se estiver a utilizar um repositório personalizado.

Parando e iniciando o Operador de Monitoramento do Kubernetes

Para parar o operador de monitoramento do Kubernetes:

```
kubectl -n netapp-monitoring scale deploy monitoring-operator --replicas=0
```

Para iniciar o operador de monitoramento do Kubernetes:

```
kubectl -n netapp-monitoring scale deploy monitoring-operator --replicas=1
```

Desinstalação

Para remover o operador de monitoramento do Kubernetes

Observe que o namespace padrão para o Operador de Monitoramento do Kubernetes é "NetApp-monitoring". Se você tiver definido seu próprio namespace, substitua esse namespace nesses e todos os comandos e arquivos subsequentes.

As versões mais recentes do operador de monitoramento podem ser desinstaladas com os seguintes comandos:

```
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>
```

Se o operador de monitoramento foi implantado em seu próprio namespace dedicado, exclua o namespace:

```
kubectl delete ns <NAMESPACE>
Se o primeiro comando retornar "nenhum recurso encontrado", use as
instruções a seguir para desinstalar versões mais antigas do operador de
monitoramento.
```

Execute cada um dos seguintes comandos em ordem. Dependendo da sua instalação atual, alguns desses comandos podem retornar mensagens "objeto não encontrado". Essas mensagens podem ser ignoradas com segurança.

```
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>
```

Se uma restrição de contexto de segurança foi criada anteriormente:

```
kubectl delete scc telegraf-hostaccess
```

Sobre o Kube-State-metrics

O Operador de Monitoramento do Kubernetes do NetApp instala suas próprias métricas de estado do kube para evitar conflitos com outras instâncias.

Para obter informações sobre métricas Kube-State, ["esta página"](#) consulte .

Configurar/personalizar o Operador

Essas seções contêm informações sobre como personalizar a configuração do operador, trabalhar com proxy, usar um repositório docker personalizado ou privado ou trabalhar com o OpenShift.

Opções de configuração

As configurações mais comumente modificadas podem ser configuradas no recurso personalizado *AgentConfiguration*. Você pode editar esse recurso antes de implantar o operador editando o arquivo *operator-config.yaml*. Este arquivo inclui exemplos comentados de configurações. Consulte a lista de ["definições disponíveis"](#) para obter a versão mais recente do operador.

Você também pode editar esse recurso depois que o operador tiver sido implantado usando o seguinte comando:

```
kubectl -n netapp-monitoring edit AgentConfiguration
Para determinar se a versão implantada do operador suporta
AgentConfiguration, execute o seguinte comando:
```

```
kubectl get crd agentconfigurations.monitoring.netapp.com
Se você vir uma mensagem "erro do servidor (NotFound)", seu operador deve
ser atualizado antes de poder usar o AgentConfiguration.
```

Configurando o suporte Proxy

Há dois lugares onde você pode usar um proxy em seu locatário para instalar o Operador de Monitoramento do Kubernetes. Estes podem ser os mesmos ou sistemas proxy separados:

- Proxy necessário durante a execução do snippet de código de instalação (usando "curl") para conectar o sistema onde o snippet é executado ao seu ambiente Data Infrastructure Insights
- Proxy necessário pelo cluster do Kubernetes de destino para se comunicar com seu ambiente Data Infrastructure Insights

Se você usar um proxy para um ou ambos, para instalar o Monitor operacional Kubernetes, primeiro você deve garantir que o proxy esteja configurado para permitir uma boa comunicação com o ambiente Insights da infraestrutura de dados. Se você tiver um proxy e puder acessar o Data Infrastructure Insights do servidor/VM a partir do qual deseja instalar o Operador, o proxy provavelmente estará configurado corretamente.

Para o proxy usado para instalar o Monitor operacional Kubernetes, antes de instalar o Operador, defina as

variáveis de ambiente `http_proxy/https_proxy`. Para alguns ambientes proxy, você também pode precisar definir a variável `no_proxy environment`.

Para definir a(s) variável(s), execute as seguintes etapas em seu sistema **antes** de instalar o Operador de Monitoramento do Kubernetes:

1. Defina a(s) variável(s) de ambiente `https_proxy` e/ou `http_proxy` para o usuário atual:
 - a. Se o proxy que está sendo configurado não tiver Autenticação (nome de usuário/senha), execute o seguinte comando:

```
export https_proxy=<proxy_server>:<proxy_port>
.. Se o proxy que está sendo configurado tiver Autenticação (nome de
usuário/senha), execute este comando:
```

```
export
http_proxy=<proxy_username>:<proxy_password>@<proxy_server>:<proxy_po
rt>
```

Para que o proxy usado para que o cluster do Kubernetes se comunique com o ambiente Data Infrastructure Insights, instale o Operador de Monitoramento do Kubernetes depois de ler todas essas instruções.

Configure a seção proxy do AgentConfiguration no `operator-config.yaml` antes de implantar o Operador de Monitoramento do Kubernetes.

```
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
  ...
  ...
```

Usando um repositório docker personalizado ou privado

Por padrão, o operador de monitoramento do Kubernetes coletará imagens de contêiner do repositório Data Infrastructure Insights. Se você tiver um cluster do Kubernetes usado como destino para monitoramento e esse cluster estiver configurado para extrair apenas imagens de contêiner de um repositório ou Registro de contêiner personalizado ou privado do Docker, configure o acesso aos contêineres necessários pelo Operador de Monitoramento do Kubernetes.

Execute o "trecho de recebimento de imagem" do bloco de instalação do Operador de Monitoramento do NetApp. Esse comando fará login no repositório Data Infrastructure Insights, extrairá todas as dependências de imagem do operador e fará logout do repositório Data Infrastructure Insights. Quando solicitado, insira a senha temporária do repositório fornecida. Este comando transfere todas as imagens utilizadas pelo operador, incluindo as funcionalidades opcionais. Veja abaixo quais recursos essas imagens são usadas.

Funcionalidade do operador principal e monitoramento do Kubernetes

- monitoramento de NetApp
- ci-kube-rbac-proxy
- ci-ksm
- ci-telegraf
- distroless-root-user

Registro de eventos

- ci-fluente-bit
- ci-kurein-event-exporter

Desempenho de rede e mapa

- ci-net-observador

Envie a imagem do docker do operador para o seu repositório docker privado/local/empresarial de acordo com suas políticas corporativas. Certifique-se de que as tags de imagem e os caminhos de diretório para essas imagens em seu repositório sejam consistentes com os do repositório Data Infrastructure Insights.

Edite a implantação do operador de monitoramento no `operator-deployment.yaml` e modifique todas as referências de imagem para usar seu repositório Docker privado.

```
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>
```

Edite o `AgentConfiguration` no `operator-config.yaml` para refletir o novo local de repo do docker. Crie uma nova `imagePullSecret` para o seu repositório privado, para obter mais detalhes consulte <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
```

Instruções do OpenShift

Se você estiver executando no OpenShift 4,6 ou superior, você deve editar o AgentConfiguration em *operator-config.yaml* para ativar a configuração *runPrivileged*:

```
# Set runPrivileged to true SELinux is enabled on your kubernetes nodes
runPrivileged: true
```

O OpenShift pode implementar um nível adicional de segurança que pode bloquear o acesso a alguns componentes do Kubernetes.

Tolerações e taints

O *NetApp-ci-telegraf-ds*, o *NetApp-CI-Fluent-bit-ds* e o *NetApp-CI-NET-Observer-L4-DS* DaemonSets devem agendar um pod em cada nó do cluster para coletar corretamente os dados em todos os nós. O operador foi configurado para tolerar alguns **taints** conhecidos. Se você tiver configurado quaisquer taints personalizados em seus nós, impedindo assim que os pods sejam executados em cada nó, você poderá criar uma **tolerância** para essas taints. *"Em AgentConfiguration"* Se você tiver aplicado taints personalizados a todos os nós do cluster, também será necessário adicionar as tolerâncias necessárias à implantação do operador para permitir que o pod do operador seja agendado e executado.

Saiba mais sobre o Kubernetes ["Taints e Tolerations"](#).

Volte ao ["Página de Instalação do Operador de Monitoramento do Kubernetes do NetApp"](#)

Uma Nota sobre Segredos

Para remover a permissão do Operador de Monitoramento do Kubernetes para exibir segredos em todo o cluster, exclua os seguintes recursos do arquivo *operator-setup.yaml* antes de instalar:

```
ClusterRole/netapp-ci-<namespace>-agent-secret-clusterrole
ClusterRoleBinding/netapp-ci-<namespace>-agent-secret-clusterrolebinding
```

Se for uma atualização, exclua também os recursos do cluster:

```
kubectl delete ClusterRole/netapp-ci-<namespace>-agent-secret-clusterrole
kubectl delete ClusterRoleBinding/netapp-ci-<namespace>-agent-secret-
clusterrolebinding
```

Se a análise de mudança estiver ativada, modifique o *AgentConfiguration* ou *operator-config.yaml* para descomentar a seção de gerenciamento de alterações e inclua *kindsToIgnoreFromWatch: "segredos"* na seção Gerenciamento de alterações. Observe a presença e a posição de aspas simples e duplas nesta linha.

```
# 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"'
...
```

Verificando assinaturas de imagem do Operador de Monitoramento do Kubernetes

A imagem para o operador e todas as imagens relacionadas que ele implanta são assinadas pelo NetApp. Você pode verificar manualmente as imagens antes da instalação usando a ferramenta de cografia ou configurar um controlador de admissão do Kubernetes. Para obter mais detalhes, consulte ["Documentação do Kubernetes"](#).

A chave pública usada para verificar as assinaturas de imagem está disponível no bloco de instalação do Operador de Monitoramento em *Opcional: Carregue as imagens do operador para o seu repositório privado > chave Pública de assinatura de imagem*

Para verificar manualmente uma assinatura de imagem, execute as seguintes etapas:

1. Copie e execute o snippet de recebimento de imagem
2. Copie e insira a senha do repositório quando solicitado
3. Armazenar a chave Pública de assinatura de imagem (dii-image-signing.pub no exemplo)
4. Verifique as imagens usando o cosign. Consulte o exemplo a seguir de uso de 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}]

```

Solução de problemas

Algumas coisas para tentar se você encontrar problemas para configurar o operador de monitoramento do Kubernetes:

Problema:	Tente isto:
Não vejo um hiperlink/conexão entre o meu volume persistente do Kubernetes e o dispositivo de armazenamento de back-end correspondente. Meu volume persistente do Kubernetes é configurado usando o nome de host do servidor de armazenamento.	Siga as etapas para desinstalar o agente Telegraf existente e reinstalar o agente Telegraf mais recente. Você precisa estar usando o Telegraf versão 2,0 ou posterior, e o storage de cluster do Kubernetes precisa ser monitorado ativamente pelo Data Infrastructure Insights.
Estou vendo mensagens nos logs que se assemelham ao seguinte: E0901 15 352:21 v1:39,962145 1 k8s reflector.go:178] k8s.io/kube-State-metrics/internal/store/builder.go:352: Falha ao listar *v1.MutatingWebhookConfiguration: O servidor não conseguiu encontrar o recurso solicitado E0901 15:k8s:43,168161 1 reflector.go:178] 21.io/kube-State-State-lease	Essas mensagens podem ocorrer se você estiver executando o kube-State-metrics versão 2.0.0 ou superior com versões do Kubernetes abaixo de 1,20. Para obter a versão do Kubernetes: <i>Kubect! version</i> para obter a versão do kube-State-metrics: <i>Kubect! get deploy/kube-State-metrics -o jsonpath leases'</i> para evitar que essas mensagens aconteçam, os usuários podem modificar sua implantação do kube-State-metrics para desativar os seguintes: <i>Mutatinghookhooks</i>

Problema:	Tente isto:
<p>Vejo mensagens de erro do Telegraf semelhantes às seguintes, mas o Telegraf inicia e executa: Oct 11 14:23:41 ip-172-31-39-47 systemd[1]: Iniciou o agente de servidor orientado a plug-in para relatar métricas no InfluxDB. Oct 11 14:23:41 ip-172-31-39-47 telegraf[1827]: Tempo 2021-10-11T14:23:41Z" não foi possível criar o diretório de cache. /Etc/telegraf/.cache/floco de neve, err: Mkdir /etc/telegraf/.CA che: Permissão negada. Ignorado. Func"gostonflake.(*defaultLogger).Errorf" file "log.go:120" Oct:10 ip-23-41Z-39-47 telegraf[1827]: 2021" 31"erro de 11 14:23:41:172". Abra /etc/telegraf/.cache/floco de neve/ocsp_response_cache.json: nenhum arquivo ou diretório desse tipo de arquivo ou diretório.(*defaultLogger).Errorf" arquivo "log.go:120 23" Oct 2021 41Z:10 ip-172-31-39-47 telegraf[1827]: 11 14-23:41 A iniciar o Telegraf 1.19.3</p>	<p>Este é um problema conhecido. "Este artigo do GitHub"Consulte para obter mais detalhes. Enquanto o Telegraf estiver ativo e em execução, os usuários podem ignorar essas mensagens de erro.</p>
<p>No Kubernetes, meu(s) pod(s) Telegraf está relatando o seguinte erro: "Erro no processamento de informações de mountstats: Failed to open mountstats file: /Hostfs/proc/1/mountstats, error: Open /hostfs/proc/1/mountstats: Permission denied"</p>	<p>Se o SELinux estiver habilitado e aplicando, provavelmente impedirá que o(s) pod(s) Telegraf acesse o arquivo /proc/1/mountstats no nó Kubernetes. Para superar essa restrição, edite a configuração do agentConfiguration e ative a configuração RUNGED Privileged. Para obter mais detalhes, consulte "Instruções do OpenShift" a .</p>
<p>No Kubernetes, meu pod Telegraf ReplicaSet está relatando o seguinte erro: [inputs.prometheus] erro no plugin: Não foi possível carregar o par de chaves /etc/kupere/pki/etcd/Server.crt:/etc/kuGES/pki/etcd/Server.key: Open /etc/kuurge/pki/etcd/Server.crt: nenhum arquivo ou diretório</p>	<p>O pod Telegraf ReplicaSet destina-se a ser executado em um nó designado como mestre ou para o etcd. Se o pod ReplicaSet não estiver sendo executado em um desses nós, você receberá esses erros. Verifique se seus nós master/etcd têm manchetes neles. Se o fizerem, adicione as tolerâncias necessárias ao Telegraf ReplicaSet, telegraf-rs. Por exemplo, edite o ReplicaSet... kubectl edite rs telegraf-RS ...e adicione as tolerâncias apropriadas à especificação. Em seguida, reinicie o pod ReplicaSet.</p>
<p>Tenho um ambiente PSP/PSA. Isso afeta meu operador de monitoramento?</p>	<p>Se o seu cluster Kubernetes estiver em execução com a Política de Segurança do Pod (PSP) ou a admissão de Segurança do Pod (PSA), você deverá fazer o upgrade para o Operador de Monitoramento do Kubernetes mais recente. Siga estes passos para atualizar para o Operador atual com suporte para PSP/PSA: 1. Desinstalar o operador de monitoramento anterior: kubectl delete 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-rolebinding cluster-rolebinding.-rolebinding 2. Instale a versão mais recente do operador de monitorização.</p>

Problema:	Tente isto:
<p>Deparei-me com problemas ao tentar implementar o Operador e tenho PSP/PSA em utilização.</p>	<p>1. Edite o agente usando o seguinte comando: <code>Kubectl -n <name-space> edit Agent</code> 2. Marque "Segurança-política-ativada" como "falsa". Isso desativará as políticas de Segurança do Pod e a admissão de Segurança do Pod e permitirá que o Operador implante. Confirme usando os seguintes comandos: <code>Kubectl Get PSP</code> (deve mostrar a Política de Segurança Pod removida) <code>kubectl get all -n <namespace></code></p>
<p><code>grep -i psp</code> (deve mostrar que nada é encontrado)</p>	<p>Erros "ImagePullBackoff" vistos</p>
<p>Esses erros podem ser vistos se você tiver um repositório docker personalizado ou privado e ainda não tiver configurado o Operador de Monitoramento do Kubernetes para reconhecê-lo adequadamente. Leia mais sobre a configuração para repositório personalizado/privado.</p>	<p>Estou tendo um problema com a implantação do meu operador de monitoramento e a documentação atual não me ajuda a resolvê-lo.</p>
<p>Capture ou anote a saída dos comandos a seguir e entre em Contato com a equipe de suporte técnico.</p> <pre data-bbox="136 863 802 1325"> 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 </pre>	<p>Os pods NET-Observer (Workload Map) no namespace Operator estão em CrashLoopBackOff</p>
<p>Esses pods correspondem ao coletor de dados do mapa de workload para observabilidade de rede. Tente estes:</p> <ul style="list-style-type: none"> • Verifique os logs de um dos pods para confirmar a versão mínima do kernel. Por exemplo: <code>---- [ci-tenant-id]:"your-tenant-id", "Collector-cluster": "your-k8s-cluster-name", "ambiente": "prod", "nível": "erro", "msg": "falhou na validação. Razão: A versão 3.10.0 do kernel é menor que a versão mínima do kernel de 4.18.0", "Time": "2022-11-09T08:23:08Z" ----</code> • os pods do Net-Observer requerem que a versão do kernel do Linux seja pelo menos 4.18.0. Verifique a versão do kernel usando o comando <code>"uname -r"</code> e certifique-se de que eles são <code>> 4.18.0</code> 	<p>Os pods estão em execução no namespace do operador (padrão: Monitoramento NetApp), mas nenhum dado é exibido na IU para mapa de workload ou métricas do Kubernetes em consultas</p>

Problema:	Tente isto:
<p>Verifique a configuração de hora nos nós do cluster K8S. Para uma auditoria precisa e relatórios de dados, é altamente recomendável sincronizar a hora na máquina do agente usando o Network Time Protocol (NTP) ou o Simple Network Time Protocol (SNTP).</p>	<p>Alguns dos pods net-observer no namespace Operador estão no estado pendente</p>
<p>NET-Observer é um DaemonSet e executa um pod em cada nó do cluster k8s. • Observe o pod que está no estado pendente e verifique se ele está enfrentando um problema de recurso para CPU ou memória. Certifique-se de que a memória e a CPU necessárias estão disponíveis no nó.</p>	<p>Estou vendo o seguinte em meus logs imediatamente após instalar o Operador de Monitoramento do Kubernetes: [inputs.prometheus] erro no plugin: Erro ao fazer solicitação HTTP para <a href="http://kube-state-metrics.<namespace>.svc.cluster.local:8080/metrics">http://kube-state-metrics.<namespace>.svc.cluster.local:8080/metrics: Get <a href="http://kube-state-metrics.<namespace>.svc.cluster.local:8080/metrics">http://kube-state-metrics.<namespace>.svc.cluster.local:8080/metrics: Dial tcp: Lookup kube-State-metrics.<namespace>.svc.cluster.local: nenhum host</p>
<p>Normalmente, essa mensagem só é vista quando um novo operador é instalado e o pod <i>telegraf-rs</i> está ativo antes do pod <i>ksm</i> estar ativo. Essas mensagens devem parar quando todos os pods estiverem em execução.</p>	<p>Não vejo nenhuma métrica sendo coletada para os CronJobs do Kubernetes que existem no meu cluster.</p>
<p>Verifique a versão do Kubernetes (isto é <code>kubectl version, </code>). Se for v1,20.x ou inferior, esta é uma limitação esperada. A versão kube-State-metrics implantada com o Operador de Monitoramento do Kubernetes suporta apenas v1.CronJob. Com o Kubernetes 1,20.x e abaixo, o recurso CronJob está em v1beta.CronJob. Como resultado, as métricas de estado do kube não conseguem encontrar o recurso CronJob.</p>	<p>Depois de instalar o operador, os pods telegraf-ds entram em CrashLoopBackOff e os logs do pod indicam "su: Authentication failure".</p>
<p>Edite a seção telegraf em <i>AgentConfiguration</i> e defina <i>dockerMetricCollectionEnabled</i> como false. Para obter mais detalhes, consulte o "opções de configuração". ... spec: ... telegraf: ... - Name: docker run-mode : - DaemonSet substituições: - Chave: DOCKER_UNIX_SOCKET_PLACEHOLDER valor: unix:///run/docker.sock</p>	<p>Vejo mensagens de erro repetitivas semelhantes às seguintes nos meus logs do Telegraf: E! [Agent] erro ao gravar em outputs.http: Post "/https://<tenant_url>/rest/v1/Lake/ingest/influxdb": Prazo de contexto excedido (Client.Timeout excedido enquanto aguarda cabeçalhos)</p>
<p>Edite a seção telegraf em <i>AgentConfiguration</i> e aumente <i>outputTimeout</i> para 10s. Para obter mais detalhes, consulte o "opções de configuração".</p>	<p>Estou faltando dados <i>involvedobject</i> para alguns Registros de eventos.</p>
<p>Certifique-se de que seguiu os passos indicados na "Permissões" seção acima.</p>	<p>Por que estou vendo dois pods de operador de monitoramento em execução, um chamado NetApp-CI-monitoring-operator-<pod> e o outro chamado Monitoring-operator-<pod>?</p>

Problema:	Tente isto:
<p>A partir de 12 de outubro de 2023, o Data Infrastructure Insights refatorou a operadora para melhor atender nossos usuários; para que essas alterações sejam totalmente adotadas, você retire o operador antigo deve e instale o novo.</p>	<p>Os eventos do meu kubernetes pararam inesperadamente de reportar ao Data Infrastructure Insights.</p>
<p>Recuperar o nome do pod de exportador de eventos:</p> <pre> `kubectl -n netapp-monitoring get pods </pre>	<p>grep event-exporter</p>
<pre> awk '{print \$1}' </pre>	<pre> sed 's/event-exporter./event-exporter/' </pre> <p>Deve ser "NetApp-CI-event-exporter" ou "event-exporter". Em seguida, edite o agente de monitoramento <code>kubectl -n netapp-monitoring edit agent</code> e defina o valor para <code>LOG_FILE</code> para refletir o nome do pod de exportador de eventos apropriado encontrado na etapa anterior. Mais especificamente, <code>LOG_FILE</code> deve ser definido como <code>"/var/log/containers/NetApp-CI-event-exporters.log"</code> ou <code>"/var/log/containers/event-exporters*.log"</code></p> <pre> fluent-bit: ... - name: event-exporter-ci substitutions: - key: LOG_FILE values: - /var/log/containers/netapp-ci-event-exporter*.log </pre> <p>Alternativamente, pode-se desinstalar também e reinstalar o agente.</p>
<p>Estou vendo POD(s) implantado(s) pelo Operador de Monitoramento do Kubernetes travarem devido a recursos insuficientes.</p>	<p>Consulte o Operador de Monitoramento do Kubernetes "opções de configuração" para aumentar os limites de CPU e/ou memória conforme necessário.</p>
<p>Uma imagem ausente ou uma configuração inválida fez com que os pods de métricas de estado do NetApp-ci-kube falhassem na inicialização ou se preparassem. Agora o StatefulSet está preso e as alterações de configuração não estão sendo aplicadas aos pods NetApp-CI-kube-State-metrics.</p>	<p>O StatefulSet está em um "quebrado" estado. Depois de corrigir quaisquer problemas de configuração, salte os pods NetApp-CI-kube-State-metrics.</p>
<p>Os pods de métricas de estado do NetApp-ci-kube falham ao iniciar depois de executar uma atualização do Operador do Kubernetes, lançando o ErrImagePull (falha ao puxar a imagem).</p>	<p>Tente redefinir os pods manualmente.</p>

Problema:	Tente isto:
<p>"Evento descartado como sendo mais antigo do que maxEventAgeSeconds" mensagens estão sendo observadas para o meu cluster Kubernetes em Log Analysis.</p>	<p>Modifique o Operador <i>agentConfiguration</i> e aumente o <i>event-exporter-maxEventAgeds</i> (ou seja, para 60s), <i>event-exporter-kubeQPS</i> (ou seja, para 100) e <i>event-exporter-kubeBurst</i> (ou seja, para 500). Para obter mais detalhes sobre essas opções de configuração, consulte a "opções de configuração" página.</p>
<p>Telegraf avisa ou trava por causa de memória bloqueável insuficiente.</p>	<p>Tente aumentar o limite de memória bloqueável para o Telegraf no sistema operacional/nó subjacente. Se aumentar o limite não for uma opção, modifique a configuração do agente NKMO e defina <i>desprotegido</i> como <i>true</i>. Isto instruirá o Telegraf a não tentar reservar páginas de memória bloqueadas. Embora isso possa representar um risco de segurança, pois segredos descryptografados podem ser trocados para o disco, ele permite a execução em ambientes onde não é possível reservar memória bloqueada. Para obter mais detalhes sobre as opções de configuração <i>desprotegidas</i>, consulte a "opções de configuração" página.</p>
<p>Vejo mensagens de aviso do Telegraf que se assemelham às seguintes: <i>W! [Inputs.diskio] não é possível reunir o nome do disco para "vdc": Erro ao ler /dev/vdc: nenhum arquivo ou diretório</i></p>	<p>Para o Operador de Monitoramento do Kubernetes, essa mensagem de aviso é benigna e pode ser ignorada com segurança. Alternativamente, edite a seção telegraf em <i>AgentConfiguration</i> e defina <i>runDsPrivileged</i> como <i>true</i>. Para obter mais detalhes, consulte "opções de configuração do operador" a .</p>

Problema:	Tente isto:
<p>Meu pod fluent-bit está falhando com os seguintes erros: [2024 10/16 14:10:16 14 16:16 2024 23:23] [error] [/src/fluent-bit/plugins/in_tail/tail_fs_inotify.c:360 errno.24] muitos arquivos abertos [2024/10/16 14:16:23] [error] falha na inicialização tail,0 [Engine] [input]</p>	<p>Tente alterar suas configurações <i>fsnotify</i> no cluster:</p> <pre data-bbox="824 226 1481 919">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></pre> <p>Reinicie o Fluent-bit.</p> <p>Observação: Para tornar essas configurações persistentes entre as reinicializações do nó, você precisa colocar as seguintes linhas em <i>/etc/sysctl.conf</i></p> <pre data-bbox="824 1192 1481 1444">fs.inotify.max_user_instances=<something larger than current setting> fs.inotify.max_user_watches=<something larger than current setting></pre>

Informações adicionais podem ser encontradas na ["Suporte"](#) página ou no ["Matriz de suporte do Data Collector"](#).

Memcached Data Collector

O Data Infrastructure Insights usa esse coletor de dados para coletar métricas do memcached.

Instalação

1. A partir de **Observability > Collectors**, clique em * Data Collector*. Escolha memcached.

Configuração

As informações podem ser encontradas no ["Memcached wiki"](#).

Objetos e contadores

Os seguintes objetos e seus contadores são coletados:

Objeto:	Identificadores:	Atributos:	Pontos de dados:
Memcached	Servidor de namespace	Nome do nó IP	Aceitar conexões manipuladas solicitações de autenticação autenticações falhadas bytes usados bytes leitura (por seg) bytes escritos (por seg) CAS Badaval acessos CAS falhas de descarga Reqs (por seg) obter Reqs (por seg) Definir Reqs (por seg) toque Reqs (por seg) falhas de Acesso Total de acessos por seg. Falhas de acessos por seg. Solicitações de Segurança falhas de Segurança Total de acessos por seg. Falhas de acessos por seg. Falhas de acessos por seg

Solução de problemas

Informações adicionais podem ser encontradas na ["Suporte"](#)página.

MongoDB Data Collector

O Data Infrastructure Insights usa esse coletor de dados para coletar métricas do MongoDB.

Instalação

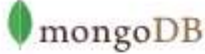
1. A partir de **Observability > Collectors**, clique em * Data Collector*. Escolha MongoDB.

Selecione o sistema operacional ou a plataforma na qual o agente Telegraf está instalado.

2. Se você ainda não instalou um Agente para coleção ou deseja instalar um Agente para um sistema operacional ou plataforma diferente, clique em *Mostrar instruções* para expandir as ["Instalação do agente"](#) instruções.
3. Selecione a chave de acesso do agente para uso com este coletor de dados. Você pode adicionar uma nova chave de acesso ao agente clicando no botão * chave de acesso ao agente*. Prática recomendada:

Use uma chave de acesso de agente diferente somente quando você quiser agrupar coletores de dados, por exemplo, por SO/Plataforma.

4. Siga as etapas de configuração para configurar o coletor de dados. As instruções variam dependendo do tipo de sistema operacional ou Plataforma que você está usando para coletar dados.



MongoDB Configuration

Gathers MongoDB metrics.

What Operating System or Platform Are You Using?

[Need Help?](#)

RHEL & CentOS

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3) [+ Agent Access Key](#)

*Please ensure that you have a Telegraf Agent in you environment before configuring. [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1 Open mongod.conf. Locate the line beginning with "bindIp", and append the address of the node on which the Telegraf agent resides. After saving the change, restart the MongoDB server.
- 2 Copy the contents below into a new .conf file under the /etc/telegraf/telegraf.d/ directory. For example, copy the contents to the /etc/telegraf/telegraf.d/cloudinsights-mongodb.conf file.

```
[[inputs.mongodb]]
  ## An array of URLs of the form:
  ## "mongodb://" [user ":" pass "@"] host [ ":" port]
  ## For example:
  ## mongodb://user:auth_key@10.10.3.30:27017,
  ## mongodb://10.10.3.30:27017
```
- 3 Replace <INSERT_MONGODB_ADDRESS> with the applicable MongoDB server address. Please specify a real machine address, and refrain from using a loopback address.
- 4 Replace <INSERT_MONGODB_PORT> with the applicable MongoDB port.
- 5 Restart the Telegraf service.

```
systemctl restart telegraf
```

Configuração

As informações podem ser encontradas no ["Documentação do MongoDB"](#).

Objetos e contadores

Os seguintes objetos e seus contadores são coletados:

Objeto:	Identificadores:	Atributos:	Pontos de dados:
MongoDB	Nome do namespace de host		
Banco de dados MongoDB	Nome do banco de dados		

Solução de problemas

Informações podem ser encontradas na ["Suporte"](#) página.

MySQL Data Collector

O Data Infrastructure Insights usa esse coletor de dados para coletar métricas do MySQL.

Instalação

1. A partir de **Observability > Collectors**, clique em * Data Collector*. Escolha MySQL.

Selecione o sistema operacional ou a plataforma na qual o agente Telegraf está instalado.
2. Se você ainda não instalou um Agente para coleção ou deseja instalar um Agente para um sistema operacional ou plataforma diferente, clique em *Mostrar instruções* para expandir as ["Instalação do agente"](#) instruções.
3. Selecione a chave de acesso do agente para uso com este coletor de dados. Você pode adicionar uma nova chave de acesso ao agente clicando no botão * chave de acesso ao agente*. Prática recomendada: Use uma chave de acesso de agente diferente somente quando você quiser agrupar coletores de dados, por exemplo, por SO/Plataforma.
4. Siga as etapas de configuração para configurar o coletor de dados. As instruções variam dependendo do tipo de sistema operacional ou Plataforma que você está usando para coletar dados.



MySQL Configuration

Gathers MySQL metrics.

What Operating System or Platform Are You Using?

[Need Help?](#)

Windows

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3) [+ Agent Access Key](#)

*Please ensure that you have a Telegraf Agent in you environment before configuring. [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1 Copy the contents below into a new .conf file under the C:\Program Files\telegraf\telegraf.d\ folder. For example, copy the contents to the C:\Program Files\telegraf\telegraf.d\cloudinsights-mysql.conf file.

```
[[inputs.mysql]]
  ## USER-ACTION: Provide comma-separated list of MySQL credentials, IP(s), and port(s)
  ## e.g. servers = ["user:passwd@tcp(127.0.0.1:3306)?tls=false"]
  ## Please specify actual machine IP address, and refrain from using a loopback address
  (i.e. localhost or 127.0.0.1).
```

- 2 Review and verify the contents of the configuration file.
- 3 Replace <INSERT_USERNAME> and <INSERT_PASSWORD> with the applicable MySQL credentials.
- 4 Replace <INSERT_PROTOCOL> with the applicable MySQL connection protocol. The typical protocol is tcp.
- 5 Replace <INSERT_MYSQL_ADDRESS> with the applicable MySQL server address. Please specify a real machine address, and refrain from using a loopback address.
- 6 Replace <INSERT_MYSQL_PORT> with the applicable MySQL server port. The typical port is 3306.
- 7 Modify the 'tls' parameter in accordance to the MySQL server configuration.
- 8 Restart the Telegraf service.

```
Stop-Service -Name telegraf -ErrorAction SilentlyContinue; Start-Service -Name telegraf
```

Configuração

As informações podem ser encontradas no ["Documentação do MySQL"](#).

Objetos e contadores

Os seguintes objetos e seus contadores são coletados:

Objeto:	Identificadores:	Atributos:	Pontos de dados:
MySQL	Servidor de namespace MySQL	Nome do nó IP	Clientes abortados (por seg) conexões abortadas (por seg) bytes RX (por seg) bytes TX (por seg) comandos Admin (por seg) comandos Alter comandos de evento Alter comandos de função Alter comandos de instância Alter comandos de procedimento Alter

Solução de problemas

Informações adicionais podem ser encontradas na ["Suporte"](#) página.

Netstat Data Collector

O Data Infrastructure Insights usa esse coletor de dados para coletar métricas do Netstat.

Instalação

1. A partir de **Observability > Collectors**, clique em * Data Collector*. Escolha Netstat.

Selecione o sistema operacional ou a plataforma na qual o agente Telegraf está instalado.
2. Se você ainda não instalou um Agente para coleção ou deseja instalar um Agente para um sistema operacional ou plataforma diferente, clique em *Mostrar instruções* para expandir as ["Instalação do agente"](#) instruções.
3. Selecione a chave de acesso do agente para uso com este coletor de dados. Você pode adicionar uma nova chave de acesso ao agente clicando no botão * chave de acesso ao agente*. Prática recomendada: Use uma chave de acesso de agente diferente somente quando você quiser agrupar coletores de dados, por exemplo, por SO/Plataforma.
4. Siga as etapas de configuração para configurar o coletor de dados. As instruções variam dependendo do tipo de sistema operacional ou Plataforma que você está usando para coletar dados.

netstat

Netstat Configuration

Gathers netstat metrics of the host where telegraf agent is installed.

What Operating System or Platform Are You Using?

[Need Help?](#)

Windows
▼

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)
▼

+ Agent Access Key

*Please ensure that you have a Telegraf Agent in you environment before configuring
Show Instructions

Follow Configuration Steps

[Need Help?](#)

- 1

Copy the contents below into a new .conf file under the C:\Program Files\telegraf\telegraf.d\ folder. For example, copy the contents to the C:\Program Files\telegraf\telegraf.d\cloudinsights-netstat.conf file.

```
# Read TCP metrics such as established, time wait and sockets counts.
[[inputs.netstat]]
# no configuration
[inputs.netstat.tags]
  CloudInsights = "true"
```
- 2

Restart the Telegraf service.

```
Stop-Service -Name telegraf -ErrorAction SilentlyContinue; Start-Service -Name telegraf
```

Configuração

Objetos e contadores

Os seguintes objetos e seus contadores são coletados:

Objeto:	Identificadores:	Atributos:	Pontos de dados:
Netstat	UUID de nó	Nome do nó IP	

Solução de problemas

Informações adicionais podem ser encontradas na ["Suporte"](#) página.

Nginx Data Collector


O Data Infrastructure Insights usa esse coletor de dados para coletar métricas do nginx.

Instalação

1. A partir de **Observability > Collectors**, clique em * Data Collector*. Escolha nginx.

Selecione o sistema operacional ou a plataforma na qual o agente Telegraf está instalado.

2. Se você ainda não instalou um Agente para coleção ou deseja instalar um Agente para um sistema operacional ou plataforma diferente, clique em *Mostrar instruções* para expandir as "[Instalação do agente](#)" instruções.
3. Selecione a chave de acesso do agente para uso com este coletor de dados. Você pode adicionar uma nova chave de acesso ao agente clicando no botão * chave de acesso ao agente*. Prática recomendada: Use uma chave de acesso de agente diferente somente quando você quiser agrupar coletores de dados, por exemplo, por SO/Plataforma.
4. Siga as etapas de configuração para configurar o coletor de dados. As instruções variam dependendo do tipo de sistema operacional ou Plataforma que você está usando para coletar dados.



Nginx Configuration

Gathers Nginx metrics.

What Operating System or Platform Are You Using?

[Need Help?](#)

Ubuntu & Debian

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3) [+ Agent Access Key](#)

*Please ensure that you have a Telegraf Agent in you environment before configuring. [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

1 If you already have a URL enabled to provide Nginx metrics, go directly to the plugin configuration.

2 Nginx metrics are available through a status page when the HTTP stub status module is enabled. Refer to the below link for verifying/enabling `http_stub_status_module`.

```
http://nginx.org/en/docs/http/nginx_http_stub_status_module.html
```

3 After verifying the module is enabled, modify the Nginx configuration to set up a locally-accessible URL for the status page:

```
server {
    listen    <PORT NUMBER>;
    Please specify actual machine IP address, and refrain from using a loopback address (i.e.
    localhost or 127.0.0.1)
    server_name <IP ADDRESS>;
    location /nginx_status {
        stub_status on;
    }
}
```

4 Reload the configuration:

```
nginx -s reload
```

5 Copy the contents below into a new `.conf` file under the `/etc/telegraf/telegraf.d/` directory. For example, copy the contents to the `/etc/telegraf/telegraf.d/cloudinsights-nginx.conf` file.

```
[[inputs.nginx]]
  ## USER-ACTION: Provide Nginx status url
  ## Please specify actual machine IP address where nginx_status is enabled, and refrain from
  ## using a loopback address (i.e. localhost or 127.0.0.1).
  ## When configuring with multiple Nginx servers, enter them in the format ["url1", "url2",
  ## ...]
```

6 Replace `<INSERT_NGINX_ADDRESS>` with the applicable Nginx address. Please specify a real machine address, and refrain from using a loopback address.

7 Replace `<INSERT_NGINX_PORT>` with the applicable Nginx port.

8 Restart the Telegraf service.

```
systemctl restart telegraf
```

Configuração

A coleção de métricas nginx requer que o nginx `"http_stub_status_module"` seja ativado.

Informações adicionais podem ser encontradas no ["Documentação do nginx"](#).

Objetos e contadores

Os seguintes objetos e seus contadores são coletados:

Objeto:	Identificadores:	Atributos:	Pontos de dados:
Nginx	Servidor de namespace	Porta de nome do nó IP do nó	Aceita solicitações de leitura tratadas ativas aguardando escrita

Solução de problemas

Informações adicionais podem ser encontradas na ["Suporte"](#) página.

PostgreSQL Data Collector

O Data Infrastructure Insights usa esse coletor de dados para coletar métricas do PostgreSQL.

Instalação

1. A partir de **Observability > Collectors**, clique em * Data Collector*. Escolha PostgreSQL.
Selecione o sistema operacional ou a plataforma na qual o agente Telegraf está instalado.
2. Se você ainda não instalou um Agente para coleção ou deseja instalar um Agente para um sistema operacional ou plataforma diferente, clique em *Mostrar instruções* para expandir as ["Instalação do agente"](#) instruções.
3. Selecione a chave de acesso do agente para uso com este coletor de dados. Você pode adicionar uma nova chave de acesso ao agente clicando no botão * chave de acesso ao agente*. Prática recomendada: Use uma chave de acesso de agente diferente somente quando você quiser agrupar coletores de dados, por exemplo, por SO/Plataforma.
4. Siga as etapas de configuração para configurar o coletor de dados. As instruções variam dependendo do tipo de sistema operacional ou Plataforma que você está usando para coletar dados.



PostgreSQL Configuration

Gathers PostgreSQL metrics.

What Operating System or Platform Are You Using?

[Need Help?](#)

RHEL & CentOS

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)

+ Agent Access Key

*Please ensure that you have a Telegraf Agent in you environment before configuring [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1 Copy the contents below into a new .conf file under the /etc/telegraf/telegraf.d/ directory. For example, copy the contents to the /etc/telegraf/telegraf.d/cloudinsights-postgresql.conf file.

```
[[inputs.postgresql]]
# USER-ACTION: Provide credentials for access, address of PostgreSQL server, port for
PostgreSQL server, one DB for access
address = "postgres://<INSERT_USERNAME>:<INSERT_PASSWORD>@<INSERT_POSTGRESQL_ADDRESS>:
<INSERT_POSTGRESQL_PORT>/<INSERT_DB>"
```

- 2 Replace <INSERT_USERNAME> and <INSERT_PASSWORD> with the applicable PostgreSQL credentials.
- 3 Replace <INSERT_POSTGRESQL_ADDRESS> with the applicable PostgreSQL address. Please specify a real machine address, and refrain from using a loopback address.
- 4 Replace <INSERT_POSTGRESQL_PORT> with the applicable PostgreSQL port.
- 5 Replace <INSERT_DB> with the applicable PostgreSQL database.
- 6 Modify 'Namespace' if needed for server disambiguation (to avoid name clashes).
- 7 Restart the Telegraf service.

```
systemctl restart telegraf
```

Configuração

As informações podem ser encontradas no "[Documentação do PostgreSQL](#)".

Objetos e contadores

Os seguintes objetos e seus contadores são coletados:

Objeto:	Identificadores:	Atributos:	Pontos de dados:
Servidor PostgreSQL	Servidor de Banco de dados de namespace	IP do nó de nome do nó	Buffers alocados Buffers backend Buffers backend File Sync Buffers Checkpoints Limpar Checkpoints Sync Time Checkpoints Write Time Checkpoints Checkpoints Requests Checkpoints Checkpoints Timed Max written clean
Banco de dados PostgreSQL	Servidor de Banco de dados de namespace	IP nó Nome nó OID base dados	Blocos de tempo de leitura blocos de tempo de gravação blocos de tempo hits blocos lê conflitos deadlocks número do cliente arquivos temporários bytes arquivos de temperatura número linhas excluídas linhas recuperadas linhas inseridas linhas retornadas transações atualizadas transações confirmadas Rollbacked

Solução de problemas

Informações adicionais podem ser encontradas na ["Suporte"](#) página.

Puppet Agent Data Collector

O Data Infrastructure Insights usa esse coletor de dados para coletar métricas do Puppet Agent.

Instalação

1. A partir de **Observability > Collectors**, clique em * Data Collector*. Escolha Puppet.
Selecione o sistema operacional ou a plataforma na qual o agente Telegraf está instalado.
2. Se você ainda não instalou um Agente para coleção ou deseja instalar um Agente para um sistema operacional ou plataforma diferente, clique em *Mostrar instruções* para expandir as ["Instalação do agente"](#) instruções.
3. Selecione a chave de acesso do agente para uso com este coletor de dados. Você pode adicionar uma nova chave de acesso ao agente clicando no botão * chave de acesso ao agente*. Prática recomendada: Use uma chave de acesso de agente diferente somente quando você quiser agrupar coletores de dados, por exemplo, por SO/Plataforma.
4. Siga as etapas de configuração para configurar o coletor de dados. As instruções variam dependendo do tipo de sistema operacional ou Plataforma que você está usando para coletar dados.



Puppet Agent Configuration

Gathers Puppet agent metrics.

What Operating System or Platform Are You Using?

[Need Help?](#)

Windows

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3) [+ Agent Access Key](#)

*Please ensure that you have a Telegraf Agent in you environment before configuring [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1 Copy the contents below into a new .conf file under the C:\Program Files\telegraf\telegraf.d\ folder. For example, copy the contents to the C:\Program Files\telegraf\telegraf.d\cloudinsights-puppetagent.conf file.

```
## Reads last_run_summary.yaml file and converts to measurements
[[inputs.puppetagent]]
  ## Location of puppet last run summary file
  ## USER-ACTION: Modify the location if last_run_summary.yaml is on different path
  location = "/var/lib/puppet/state/last_run_summary.yaml"
```

- 2 Modify 'location' if last_run_summary.yaml is on different path
- 3 Modify 'Namespace' if needed for puppet agent disambiguation (to avoid name clashes).
- 4 Restart the Telegraf service.

```
Stop-Service -Name telegraf -ErrorAction SilentlyContinue; Start-Service -Name telegraf
```

Configuração

As informações podem ser encontradas no ["Documentação da marionete"](#)

Objetos e contadores

Os seguintes objetos e seus contadores são coletados:

Objeto:	Identificadores:	Atributos:	Pontos de dados:
---------	------------------	------------	------------------

Agente de fantoche	UUUID nó namespace	Nome do nó localização nó versão IP Configstring versão Puppet	Alterações Total Eventos falhas Eventos sucesso Eventos recursos totais recursos alterados recursos Falha recursos Falha ao reiniciar recursos recursos Outofsync recursos reiniciados recursos programados recursos ignorados tempo total tempo de ancoragem tempo de recuperação da configuração tempo tempo tempo do cron tempo Exec tempo do arquivo tempo do arquivo tempo do pacote tempo horário do pacote horário do serviço tempo do Sshaughhorizedkey tempo Total do Usuário

Solução de problemas

Informações adicionais podem ser encontradas na ["Suporte"](#) página.

Redis Data Collector

O Data Infrastructure Insights usa esse coletor de dados para coletar métricas do Redis. Redis é um armazenamento de estrutura de dados em memória de código aberto usado como um banco de dados, cache e corretor de mensagens, suportando as seguintes estruturas de dados: Strings, hashes, listas, conjuntos e muito mais.

Instalação

1. A partir de **Observability > Collectors**, clique em * Data Collector*. Escolha Redis.

Selecione o sistema operacional ou a plataforma na qual o agente Telegraf está instalado.

2. Se você ainda não instalou um Agente para coleção ou deseja instalar um Agente para um sistema operacional ou plataforma diferente, clique em *Mostrar instruções* para expandir as ["Instalação do agente"](#) instruções.
3. Selecione a chave de acesso do agente para uso com este coletor de dados. Você pode adicionar uma nova chave de acesso ao agente clicando no botão * chave de acesso ao agente*. Prática recomendada: Use uma chave de acesso de agente diferente somente quando você quiser agrupar coletores de dados, por exemplo, por SO/Plataforma.
4. Siga as etapas de configuração para configurar o coletor de dados. As instruções variam dependendo do tipo de sistema operacional ou Plataforma que você está usando para coletar dados.



Redis Configuration

Gathers Redis metrics.

What Operating System or Platform Are You Using?

[Need Help?](#)

Windows

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)

+ Agent Access Key

*Please ensure that you have a Telegraf Agent in you environment before configuring. [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1 Configure Redis to accept connections from the address of the node on which the Telegraf agent resides. Open the Redis configuration file.

```
vi /etc/redis.conf
```

- 2 Locate the line that begins with 'bind 127.0.0.1', and append the address of the node on which the Telegraf agent resides

```
bind 127.0.0.1 <NODE_IP_ADDRESS>
```

- 3 Copy the contents below into a new .conf file under the C:\Program Files\telegraf\telegraf.d\ folder. For example, copy the contents to the C:\Program Files\telegraf\telegraf.d\cloudinsights-redis.conf file.

```
# Read metrics from one or many redis servers
[[inputs.redis]]
  ## specify servers via a url matching:
  ## [protocol://][:password]@address[:port]
  ## e.g.
  ## http://127.0.0.1:6379?auth=passw0rd
```

- 4 Replace <INSERT_REDIS_ADDRESS> with the applicable Redis address. Please specify a real machine address, and refrain from using a loopback address.

- 5 Replace <INSERT_REDIS_PORT> with the applicable Redis port.

- 6 Restart the Telegraf service.

```
Stop-Service -Name telegraf -ErrorAction SilentlyContinue; Start-Service -Name telegraf
```

Configuração

As informações podem ser encontradas no "[Documentação Redis](#)".

Objetos e contadores

Os seguintes objetos e seus contadores são coletados:

Objeto:	Identificadores:	Atributos:	Pontos de dados:
Redis	Servidor de namespace		

Solução de problemas















Informações adicionais podem ser encontradas na "[Suporte](#)" página.

Referência do ícone do objeto



Ícones de objeto usados em Insights de infraestrutura de dados.

Ícones de infra-estrutura:

Storage

-  Backend Storage Array
-  Backend Volume
-  Disk
-  Internal Volume
-  Masking
-  Path
-  Q-Tree
-  Quota
-  Share
-  Storage
-  Storage Node
-  Storage Pool
-  Tape
-  Volume
-  Virtual Storage Array
-  Virtual Volume

Networking

-  Fabric
-  iSCSI Network Portal
-  iSCSI Session
-  NAS
-  NPV Switch
-  NPV Chassis
-  Port
-  Switch
-  Zone
-  Zone Members





Compute

-  Datastore
-  Host
-  Virtual Machine
-  VMDK






Application

-  Application

Misc.

-  Unknown
-  Generic
-  Violation
-  Failure

Ícones do Kubernetes:

-  Cluster
-  Namespace
-  Workload
-  Node
-  Pod

Ícones de mapa e monitoramento de desempenho de rede do Kubernetes:



Avisos legais

Avisos legais fornecem acesso a declarações de direitos autorais, marcas registradas, patentes e muito mais.

Direitos de autor

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

Marcas comerciais

NetApp, o logotipo DA NetApp e as marcas listadas na página de marcas comerciais da NetApp são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.

["https://www.netapp.com/company/legal/trademarks/"](https://www.netapp.com/company/legal/trademarks/)

Patentes

Uma lista atual de patentes de propriedade da NetApp pode ser encontrada em:

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

Política de privacidade

["https://www.netapp.com/company/legal/privacy-policy/"](https://www.netapp.com/company/legal/privacy-policy/)

Código aberto

Os arquivos de aviso fornecem informações sobre direitos autorais de terceiros e licenças usadas no software NetApp.

["Aviso para Insights de infraestrutura de dados \(anteriormente Cloud Insights\)"](#)

["Aviso de segurança de carga de trabalho \(anteriormente Cloud Secure\)"](#)

Informações sobre direitos autorais

Copyright © 2024 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPTÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.