



# **Configurando o Insight**

## OnCommand Insight

NetApp  
October 24, 2024

# Índice

Configurando o Insight .....	1
Acessando a IU da Web .....	1
Instalando suas licenças do Insight .....	2
Configurar e gerenciar contas de usuário .....	7
Configurando uma mensagem de aviso de login .....	15
Ferramenta SecurityAdmin .....	15
Suporte para Smart Card e certificado de login .....	41
Importando certificados SSL .....	50
Configuração de backups semanais para seu banco de dados Insight .....	53
Arquivamento de dados de desempenho .....	55
Configurando seu e-mail .....	56
Configurar notificações SNMP .....	57
Habilitando o recurso syslog .....	58
Configurando o desempenho e garanta notificações de violação .....	59
Configurando notificações de eventos no nível do sistema .....	60
Configurando o processamento ASUP .....	60
Definindo aplicativos .....	62
Sua hierarquia de entidades empresariais .....	65
Definir anotações .....	68
Consulta de ativos .....	83
Gerenciamento de políticas de performance .....	90
Importar e exportar dados do utilizador .....	94

# Configurando o Insight

Para configurar o Insight, você deve ativar as licenças do Insight, configurar suas fontes de dados, definir usuários e notificações, habilitar backups e executar todas as etapas de configuração avançadas necessárias.

Depois que o sistema OnCommand Insight for instalado, você deverá executar estas tarefas de configuração:

- Instale as licenças do Insight.
- Configure suas fontes de dados no Insight.
- Configurar contas de usuário.
- Configure o seu e-mail.
- Defina as notificações SNMP, email ou syslog, se necessário.
- Ative backups semanais automáticos do seu banco de dados Insight.
- Execute todas as etapas avançadas de configuração necessárias, incluindo a definição de anotações e limites.

## Acessando a IU da Web

Depois de instalar o OnCommand Insight, você deve instalar suas licenças e, em seguida, configurar o Insight para monitorar seu ambiente. Para fazer isso, use um navegador da Web para acessar a IU da Web do Insight.

### Passos

1. Execute um dos seguintes procedimentos:

- Abra o Insight no servidor Insight:

```
https://fqdn
```

- Abra o Insight de qualquer outro local:

```
https://fqdn:port
```


O número da porta é 443 ou outra porta configurada quando o servidor Insight foi instalado. O número da porta é padrão para 443 se você não o especificar no URL.

A caixa de diálogo OnCommand Insight é

OnCommand Insight

Username:

Password:

 Launch Java UI

exibida:

2. Digite seu nome de usuário e senha e clique em **Login**.

Se as licenças tiverem sido instaladas, é apresentada a página de configuração da fonte de dados.



Uma sessão do navegador do Insight que está inativa por 30 minutos é esgotada e você é desconectado automaticamente do sistema. Para maior segurança, é recomendável fechar o navegador após sair do Insight.

## Instalando suas licenças do Insight

Depois de receber o ficheiro de licença que contém as chaves de licença Insight do NetApp, pode utilizar as funcionalidades de configuração para instalar todas as suas licenças ao mesmo tempo.

### Sobre esta tarefa

As chaves de licença Insight são armazenadas em um `.txt` arquivo ou `.lic`.

### Passos

1. Abra o arquivo de licença em um editor de texto e copie o texto.
2. Abra o Insight em seu navegador.
3. Na barra de ferramentas Insight, clique em **Admin**.
4. Clique em **Configuração**.
5. Clique na guia **licenças**.
6. Clique em **Atualizar licença**.
7. Copie o texto da chave de licença na caixa de texto **Licença**.
8. Selecione a operação **Update (mais comum)**.
9. Clique em **Salvar**.
10. Se você estiver usando o modelo de licenciamento do Insight Consumption, marque a caixa **Ativar o envio de informações de uso para o NetApp** na seção **Enviar informações de uso**. O proxy deve estar configurado e habilitado corretamente para o seu ambiente.

## Depois de terminar

Depois de instalar as licenças, você pode executar estas tarefas de configuração:

- Configurar fontes de dados.
- Criar contas de usuário do OnCommand Insight.

## Licenças OnCommand Insight

O OnCommand Insight opera com licenças que habilitam recursos específicos no Insight Server.

### • Descubra

Discover é a licença básica do Insight que suporta inventário. Você deve ter uma licença Discover para usar o OnCommand Insight, e a licença Discover deve ser emparelhada com pelo menos uma das licenças assure, Perform ou Plan.

### • \* Assegurar\*

Uma licença assure fornece suporte para a funcionalidade de garantia, incluindo política de caminho global e SAN e gerenciamento de violações. Uma licença assure também permite que você visualize e gerencie vulnerabilidades.

### • Executar

Uma licença Perform suporta o monitoramento de desempenho em páginas de ativos, widgets do painel, consultas e assim por diante, bem como o gerenciamento de políticas e violações de desempenho.

### • Plano

Uma licença Plan suporta funções de Planejamento, incluindo uso e alocação de recursos.

### • Pacote de utilização do host

Uma licença de utilização do host suporta a utilização do sistema de arquivos em hosts e máquinas virtuais.

### • Criação de relatórios

Uma licença de criação de relatórios suporta autores adicionais para relatórios. Esta licença requer a licença Plan.

Os módulos OnCommand Insight são licenciados para prazo anual ou perpétuo:

- Por terabyte de capacidade monitorada para descobrir, assegurar, Planejar, executar módulos
- Por número de hosts para o pacote de utilização do host
- Número de unidades adicionais de Pro-autores Cognos necessárias para a criação de relatórios

As chaves de licença são um conjunto de strings exclusivas que são geradas para cada cliente. Você pode obter chaves de licença do seu representante da OnCommand Insight.

As licenças instaladas controlam as seguintes opções disponíveis no software:

- **Descubra**

Adquirir e gerenciar inventário (Fundação)

Monitore alterações e gerencie políticas de inventário

- \* **Assegurar\***

Exibir e gerenciar políticas e violações de caminho de SAN

Visualize e gerencie vulnerabilidades

Exibir e gerenciar tarefas e migrações

- **Plano**

Exibir e gerenciar solicitações

Exibir e gerenciar tarefas pendentes

Visualizar e gerenciar violações de reserva

Visualize e gerencie violações de balanceamento de portas

- **Executar**

Monitore dados de desempenho, incluindo dados em widgets do painel, páginas de ativos e consultas

Visualizar e gerenciar políticas e violações de desempenho

As tabelas a seguir fornecem detalhes sobre os recursos disponíveis com e sem a licença Perform para usuários admin e não administradores.

Recurso (admin)	Com a licença de execução	Sem executar licença
Aplicação	Sim	Sem dados de desempenho ou gráficos
Máquina virtual	Sim	Sem dados de desempenho ou gráficos
Hipervisor	Sim	Sem dados de desempenho ou gráficos
Host	Sim	Sem dados de desempenho ou gráficos
Armazenamento de dados	Sim	Sem dados de desempenho ou gráficos
VMDK	Sim	Sem dados de desempenho ou gráficos

Volume interno	Sim	Sem dados de desempenho ou gráficos
Volume	Sim	Sem dados de desempenho ou gráficos
Pool de storage	Sim	Sem dados de desempenho ou gráficos
Disco	Sim	Sem dados de desempenho ou gráficos
Armazenamento	Sim	Sem dados de desempenho ou gráficos
Nó de storage	Sim	Sem dados de desempenho ou gráficos
Malha	Sim	Sem dados de desempenho ou gráficos
Porta do switch	Sim	Sem dados de desempenho ou gráficos; "erros de porta" mostra "N/A"
Porta de armazenamento	Sim	Sim
Porta de NPV	Sim	Sem dados de desempenho ou gráficos
Interrutor	Sim	Sem dados de desempenho ou gráficos
Switch NPV	Sim	Sem dados de desempenho ou gráficos
Qtrees	Sim	Sem dados de desempenho ou gráficos
Cota	Sim	Sem dados de desempenho ou gráficos
Caminho	Sim	Sem dados de desempenho ou gráficos
Zona	Sim	Sem dados de desempenho ou gráficos

Membro da zona	Sim	Sem dados de desempenho ou gráficos
Dispositivo genérico	Sim	Sem dados de desempenho ou gráficos
Fita	Sim	Sem dados de desempenho ou gráficos
Mascaramento	Sim	Sem dados de desempenho ou gráficos
Sessões ISCSI	Sim	Sem dados de desempenho ou gráficos
Portais de rede ICSI	Sim	Sem dados de desempenho ou gráficos
Pesquisa	Sim	Sim
Administrador	Sim	Sim
Painel de instrumentos	Sim	Sim
Widgets	Sim	Parcialmente disponível (apenas widgets de ativo, consulta e administrador estão disponíveis)
Painel de violações	Sim	Oculto
Painel ativos	Sim	Parcialmente disponível (os widgets de IOPS de armazenamento e IOPS de VM estão ocultos)
Gerenciar políticas de performance	Sim	Oculto
Gerir anotações	Sim	Sim
Gerir regras de anotação	Sim	Sim
Gerenciar aplicativos	Sim	Sim
Consultas	Sim	Sim
Gerenciar entidades de negócios	Sim	Sim



Recurso	Usuário - com licença de execução	Convidado - com licença de execução	Usuário - sem executar licença	Convidado - sem licença de execução
Painel ativos	Sim	Sim	Parcialmente disponível (os widgets de IOPS de armazenamento e IOPS de VM estão ocultos)	Parcialmente disponível (os widgets de IOPS de armazenamento e IOPS de VM estão ocultos)
Painel de instrumentos personalizado	Exibir somente (sem opções de criar, editar ou salvar)	Exibir somente (sem opções de criar, editar ou salvar)	Exibir somente (sem opções de criar, editar ou salvar)	Exibir somente (sem opções de criar, editar ou salvar)
Gerenciar políticas de performance	Sim	Oculto	Oculto	Oculto
Gerir anotações	Sim	Oculto	Sim	Oculto
Gerenciar aplicativos	Sim	Oculto	Sim	Oculto
Gerenciar entidades de negócios	Sim	Oculto	Sim	Oculto
Consultas	Sim	Visualizar e editar apenas (sem opção de guardar)	Sim	Visualizar e editar apenas (sem opção de guardar)

## Configurar e gerenciar contas de usuário

As contas de usuário, a autenticação de usuário e a autorização de usuário podem ser definidas e gerenciadas de duas maneiras: No servidor LDAP (Lightweight Directory Access Protocol) do Microsoft Active Directory (versão 2 ou 3) ou em um banco de dados interno de usuários do OnCommand Insight. Ter uma conta de usuário diferente para cada pessoa fornece uma maneira de controlar os direitos de acesso, preferências individuais e responsabilidade. Use uma conta que tenha Privileges de administrador para esta operação.

### Antes de começar

Você deve ter concluído as seguintes tarefas:

- Instale as licenças do OnCommand Insight.
- Atribua um nome de utilizador exclusivo para cada utilizador.
- Determine quais senhas usar.
- Atribua as funções de utilizador corretas.



Se você estiver importando um certificado LDAP e tiver alterado as senhas *Server.keystore* e/ou *Server.trustore* usando "administrador de segurança", reinicie o serviço *SANscreen* antes de importar o certificado LDAP.



As práticas recomendadas de segurança determinam que os administradores configurem o sistema operacional host para impedir o login interativo de usuários não-administradores/padrão.

## Passos

1. Abra o Insight em seu navegador.
2. Na barra de ferramentas Insight, clique em **Admin**.
3. Clique em **Configuração**.
4. Selecione a guia **Users** (usuários).
5. Para criar um novo usuário, clique no botão **ações** e selecione **Adicionar usuário**.

Introduza o endereço **Nome**, **Palavra-passe**, **e-mail** e selecione uma das funções do utilizador **funções** como Administrador, Utilizador ou convidado.

6. Para alterar as informações de um usuário, selecione-o na lista e clique no símbolo **Editar conta de usuário** à direita da descrição do usuário.
7. Para remover um usuário do sistema OnCommand Insight, selecione-o na lista e clique em **Excluir conta de usuário** à direita da descrição do usuário.

## Resultados

Quando um usuário faz login no OnCommand Insight, o servidor primeiro tenta se autenticar por meio do LDAP, se o LDAP estiver habilitado. Se o OnCommand Insight não conseguir localizar o usuário no servidor LDAP, ele pesquisará no banco de dados local do Insight.

## Funções de usuário do Insight

Cada conta de usuário recebe um dos três níveis de permissão possíveis.

- Guest permite que você faça login no Insight e visualize as várias páginas.
- O usuário permite todos os Privileges de nível de convidado, bem como acesso a operações do Insight, como definir políticas e identificar dispositivos genéricos. O tipo de conta de usuário não permite que você execute operações de origem de dados, nem adicionar ou editar quaisquer contas de usuário que não sejam suas.
- O administrador permite que você execute qualquer operação, incluindo adicionar novos usuários e gerenciar fontes de dados.

**Prática recomendada:** limite o número de usuários com permissões de Administrador criando a maioria das contas para usuários ou convidados.

## Configurando o Insight para LDAP(s)

O OnCommand Insight deve ser configurado com configurações LDAP (Lightweight Directory Access Protocol), conforme elas são configuradas no domínio LDAP

corporativo.

Antes de configurar o Insight para uso com LDAP ou LDAP seguro (LDAPS), anote a configuração do ativo Directory em seu ambiente corporativo. As configurações de insight devem corresponder às da configuração de domínio LDAP da sua organização. Consulte os conceitos abaixo antes de configurar o Insight para uso com LDAP e verifique com o administrador de domínio LDAP os atributos apropriados a serem usados em seu ambiente.

Para todos os usuários do Secure active Directory (ou seja, LDAPS), você deve usar o nome do servidor AD exatamente como está definido no certificado. Você não pode usar o endereço IP para login seguro do AD.



Se você alterou as senhas *Server.keystore* e/ou *Server.trustore* usando "[administrador de segurança](#)"o , reinicie o serviço *SANscreen* antes de importar o certificado LDAP.



O OnCommand Insight oferece suporte a LDAP e LDAPS por meio do Microsoft active Directory Server ou do Azure AD. Implementações LDAP adicionais podem funcionar, mas não foram qualificadas com o Insight. Os procedimentos nestes guias presumem que você está usando o LDAP do Microsoft active Directory versão 2 ou 3 (Lightweight Directory Access Protocol).

### Nome principal do usuário atributo:

O atributo Nome Principal do Usuário LDAP (*userPrincipalName*) é o que o Insight usa como atributo de nome de usuário. O Nome principal do usuário é garantido para ser globalmente único em uma floresta do ativo Directory (AD), mas em muitas grandes organizações, o nome principal de um usuário pode não ser imediatamente óbvio ou conhecido por eles. Sua organização pode usar uma alternativa ao atributo Nome principal do usuário para nome de usuário principal.

A seguir estão alguns valores alternativos para o campo Nome principal do usuário atributo:

- **SAMAccountName**

Este atributo de usuário é o nome de usuário legado pré-Windows 2000 NT - é isso que a maioria dos usuários está acostumada a fazer login em sua máquina pessoal Windows. Isso não é garantido para ser globalmente único em toda uma floresta AD.



*SAMAccountName* é sensível a maiúsculas e minúsculas para o atributo Nome Principal do Usuário.

- **mail**

Em ambientes AD com MS Exchange, esse atributo é o endereço de e-mail principal para o usuário final. Isso deve ser globalmente único em toda uma floresta do AD (e também familiar para usuários finais), ao contrário de seu atributo *userPrincipalName*. O atributo *mail* não existirá na maioria dos ambientes que não sejam do MS Exchange.

- **indicação**

Uma referência LDAP é a maneira de um controlador de domínio indicar a um aplicativo cliente que ele não tem uma cópia de um objeto solicitado (ou, mais precisamente, que ele não mantém a seção da árvore de diretórios onde esse objeto estaria, se de fato existir) e dando ao cliente uma localização que é mais provável de manter o objeto. O cliente, por sua vez, usa a referência como base para uma pesquisa de DNS para um controlador de domínio. Idealmente, as referências sempre fazem referência a um controlador de domínio que, de fato, detém o objeto. No entanto, é possível que o controlador de domínio

referido gere mais uma referência, embora geralmente não demore muito para descobrir que o objeto não existe e informar o cliente.



SAMAccountName é geralmente preferido em relação ao nome principal do usuário. SAMAccountName é único no domínio (embora possa não ser exclusivo na floresta do domínio), mas é o domínio string que os usuários normalmente usam para login (por exemplo, *NetApp\_username*). O Nome distinto é o nome exclusivo na floresta, mas geralmente não é conhecido pelos usuários.



Na parte do sistema Windows do mesmo domínio, você sempre pode abrir um prompt de comando e digitar SET para encontrar o nome de domínio adequado (USERDOMAIN). O nome de login do OCI será `USERDOMAIN\sAMAccountName` então .

Para o nome de domínio **mydomain.x.y.z.com**, use `DC=x, DC=y, DC=z, DC=com` no campo domínio no Insight.

### Portos:

A porta padrão para LDAP é 389 e a porta padrão para LDAPS é 636

URL típica para LDAPS: `ldaps://<ldap_server_host_name>:636`

Os registos estão em: `\\<install_directory>\SANSscreen\wildfly\standalone\log\ldap.log`

Por padrão, o Insight espera os valores anotados nos campos a seguir. Se essas alterações forem alteradas no ambiente do ative Directory, certifique-se de alterá-las na configuração LDAP do Insight.

Atributo de função
Membro Of
Atributo Mail
e-mail
Atributo Distinguished Name
DistinguishedName
Referência
sigla

### Grupos:

Para autenticar usuários com diferentes funções de acesso nos servidores OnCommand Insight e DWH, você deve criar grupos no ative Directory e inserir esses nomes de grupo nos servidores OnCommand Insight e DWH. Os nomes dos grupos abaixo são apenas exemplos; os nomes que você configura para LDAP no Insight devem corresponder aos configurados para o ambiente do ative Directory.

Grupo Insight	Exemplo
Grupo de administradores do servidor Insight	insight.server.admins
Grupo de administradores do Insight	insight.admins
Grupo de usuários do Insight	insight.users
Grupo de convidados Insight	insight.guests
Grupo de administradores de relatórios	insight.report.admins
Grupo de autores profissionais	insight.report.proauthors
Grupo de autores subordinados	insight.report.business.authors
Grupo de consumidores de relatórios	insight.report.business.consumers
Grupo de destinatários de relatórios	insight.report.destinatários

## Configurando definições de usuário usando LDAP

Para configurar o OnCommand Insight (OCI) para autenticação de usuário e autorização de um servidor LDAP, você deve ser definido no servidor LDAP como o administrador do servidor OnCommand Insight.

### Antes de começar

Você deve conhecer os atributos de usuário e grupo que foram configurados para o Insight no domínio LDAP.

Para todos os usuários do Secure active Directory (ou seja, LDAPS), você deve usar o nome do servidor AD exatamente como está definido no certificado. Você não pode usar o endereço IP para login seguro do AD.



Se você alterou as senhas *Server.keystore* e/ou *Server.trustore* usando "[administrador de segurança](#)"o , reinicie o serviço *SANscreen* antes de importar o certificado LDAP.

### Sobre esta tarefa

O OnCommand Insight suporta LDAP e LDAPS através do servidor Microsoft active Directory. Implementações LDAP adicionais podem funcionar, mas não foram qualificadas com o Insight. Este procedimento pressupõe que você esteja usando o LDAP do Microsoft active Directory versão 2 ou 3 (Lightweight Directory Access Protocol).

Os utilizadores LDAP são apresentados juntamente com os utilizadores definidos localmente na lista **Admin > Configuração > utilizadores**.

### Passos

1. Na barra de ferramentas Insight, clique em **Admin**.

2. Clique em **Configuração**.
3. Clique na guia **usuários**.
4. Desloque-se para a secção LDAP.
5. Clique em **Enable LDAP** (Ativar LDAP) para permitir a autenticação e autorização do utilizador LDAP.
6. Preencha os campos:

- **LDAP servers:** O Insight aceita uma lista separada por vírgulas de URLs LDAP. O Insight tenta se conectar aos URLs fornecidos sem validar para o protocolo LDAP.



Para importar os certificados LDAP, clique em **certificados** e importe automaticamente ou localize manualmente os arquivos de certificado.

O endereço IP ou o nome DNS utilizado para identificar o servidor LDAP é normalmente introduzido neste formato:

```
ldap://<ldap-server-address>:port
```

ou, se estiver usando a porta padrão:

```
ldap://<ldap-server-address>
```

+ Ao inserir vários servidores LDAP neste campo, certifique-se de que o número de porta correto seja usado em cada entrada.

- **User name:** Insira as credenciais de um usuário autorizado para consultas de pesquisa de diretório nos servidores LDAP.
- **Password:** Introduza a palavra-passe para o utilizador acima. Para confirmar esta palavra-passe no servidor LDAP, clique em **Validar**.

7. Se pretender definir este utilizador LDAP com mais precisão, clique em **Mostrar mais** e preencha os campos para os atributos listados.

Essas configurações devem corresponder aos atributos configurados no domínio LDAP. Verifique com o administrador do ativo Directory se não tiver certeza dos valores a serem inseridos nesses campos.

- **Admins grupo**

Grupo LDAP para usuários com o Insight Administrator Privileges. A predefinição é `insight.admins`.

- **Grupo de usuários**

Grupo LDAP para usuários com o Insight User Privileges. A predefinição é `insight.users`.

- **Grupos de hóspedes**

Grupo LDAP para usuários com o Insight Guest Privileges. A predefinição é `insight.guests`.

- **Server admins group**

Grupo LDAP para usuários com o Insight Server Administrator Privileges. A predefinição é `insight.server.admins`.

- **Tempo limite**

Tempo de espera para uma resposta do servidor LDAP antes do tempo limite, em milissegundos. O padrão é 2.000, o que é adequado em todos os casos e não deve ser modificado.

- **Domínio**

Nó LDAP onde o OnCommand Insight deve começar a procurar o usuário LDAP. Normalmente, este é o domínio de nível superior para a organização. Por exemplo:

```
DC=<enterprise>,DC=com
```

- **Nome principal do usuário atributo**

Atributo que identifica cada usuário no servidor LDAP. O padrão é `userPrincipalName`, que é globalmente único. O OnCommand Insight tenta corresponder o conteúdo deste atributo com o nome de usuário fornecido acima.

- **Atributo de função**

Atributo LDAP que identifica o ajuste do usuário dentro do grupo especificado. A predefinição é `memberOf`.

- \* Mail atributo\*

Atributo LDAP que identifica o endereço de e-mail do usuário. A predefinição é `mail`. Isso é útil se você quiser se inscrever em relatórios disponíveis no OnCommand Insight. O Insight coleta o endereço de e-mail do usuário na primeira vez que cada usuário faz login e não o procura depois disso.



Se o endereço de e-mail do usuário mudar no servidor LDAP, certifique-se de atualizá-lo no Insight.

- \* Nome distinto atributo\*

Atributo LDAP que identifica o nome distinto do usuário. O padrão é `distinguishedName`.

8. Clique em **Salvar**.

## Alterando senhas de usuário

Um usuário com administrador Privileges pode alterar a senha de qualquer conta de usuário do OnCommand Insight definida no servidor local.

## Antes de começar

Os seguintes itens devem ter sido concluídos:

- Notificações para qualquer pessoa que faça login na conta de usuário que você está modificando.
- Nova palavra-passe a ser utilizada após esta alteração.

## Sobre esta tarefa

Ao utilizar este método, não é possível alterar a palavra-passe de um utilizador validado através do LDAP.

## Passos

1. Inicie sessão com o administrador Privileges.
2. Na barra de ferramentas Insight, clique em **Admin**.
3. Clique em **Configuração**.
4. Clique na guia **usuários**.
5. Localize a linha que exibe a conta de usuário que você deseja modificar.
6. À direita das informações do usuário, clique em **Editar conta de usuário**.
7. Introduza a nova **Password** e, em seguida, introduza-a novamente no campo de verificação.
8. Clique em **Salvar**.

## Editar uma definição de utilizador

Um usuário com administrador Privileges pode editar uma conta de usuário para alterar o endereço de e-mail ou as funções do OnCommand Insight ou DWH e funções de relatório.

## Antes de começar

Determine o tipo de conta de usuário (OnCommand Insight, DWH ou uma combinação) que precisa ser alterada.

## Sobre esta tarefa

Para usuários LDAP, você só pode modificar o endereço de e-mail usando este método.

## Passos

1. Inicie sessão com o administrador Privileges.
2. Na barra de ferramentas Insight, clique em **Admin**.
3. Clique em **Configuração**.
4. Clique na guia **usuários**.
5. Localize a linha que exibe a conta de usuário que você deseja modificar.
6. À direita das informações do usuário, clique no ícone **Editar conta de usuário**.
7. Faça as alterações necessárias.



8. Clique em **Salvar**.

## Eliminar uma conta de utilizador

Qualquer utilizador com Privileges de administrador pode eliminar uma conta de utilizador, quer quando já não for utilizada (para uma definição de utilizador local), quer para forçar o OnCommand Insight a redescobrir as informações do utilizador na próxima vez que o utilizador iniciar sessão (para um utilizador LDAP).

### Passos

1. Faça login no OnCommand Insight com o Privileges do administrador.
2. Na barra de ferramentas Insight, clique em **Admin**.
3. Clique em **Configuração**.
4. Clique na guia **usuários**.
5. Localize a linha que exibe a conta de usuário que deseja excluir.
6. À direita das informações do usuário, clique no ícone **Excluir conta de usuário "x"**.
7. Clique em **Salvar**.

## Configurando uma mensagem de aviso de login

O OnCommand Insight permite que os administradores definam uma mensagem de texto personalizada que é exibida quando os usuários fazem login.

### Passos

1. Para definir a mensagem no servidor OnCommand Insight:
  - a. Navegue para o **Admin > Troubleshooting > Advanced Troubleshooting > Advanced Settings**
  - b. Introduza a sua mensagem de início de sessão na área de texto.
  - c. Clique na caixa de verificação **Cliente apresenta mensagem de aviso de início de sessão**.
  - d. Clique em **Salvar**.

A mensagem será exibida após o login para todos os usuários.

2. Para definir a mensagem no Data Warehouse (DWH) e Reporting (Cognos):
  - a. Navegue até **informações do sistema** e clique na guia **Aviso de login**.
  - b. Introduza a sua mensagem de início de sessão na área de texto.
  - c. Clique em **Salvar**.

A mensagem será exibida no início de sessão DWH e Cognos Reporting para todos os utilizadores.

## Ferramenta SecurityAdmin

O OnCommand Insight fornece recursos que permitem que os ambientes Insight operem

com segurança aprimorada. Esses recursos incluem criptografia, hash de senha e a capacidade de alterar senhas internas de usuário e pares de chaves que criptografam e descriptografam senhas. Você pode gerenciar esses recursos em todos os servidores no ambiente Insight usando a **SecurityAdmin Tool**.

## O que é a ferramenta SecurityAdmin?

A ferramenta de administração de segurança suporta alterações no conteúdo dos cofres, bem como fazer alterações coordenadas na instalação do OnCommand Insight.

Os principais usos para a ferramenta SecurityAdmin são para **Backup e Restore** da configuração de segurança (ou seja, Vault) e senhas. Por exemplo, você pode fazer backup do Vault em uma Unidade de aquisição local e restaurá-lo em uma Unidade de aquisição remota, garantindo a coordenação de senhas em todo o seu ambiente. Ou se você tiver vários servidores OnCommand Insight em seu ambiente, talvez queira fazer um backup do Vault do servidor e restaurá-lo para outros servidores para manter as senhas iguais. Estes são apenas dois exemplos de como o SecurityAdmin pode ser usado para garantir a coesão em seus ambientes.



É altamente recomendável **fazer backup do Vault** sempre que você fizer backup de um banco de dados OnCommand Insight. Se não o fizer, pode resultar em perda de acesso.

A ferramenta fornece os modos **interactive** e **command line**.

Muitas operações da SecurityAdmin Tool alteram o conteúdo do Vault e também fazem alterações na instalação, garantindo que o Vault e a instalação permaneçam sincronizados.

Por exemplo,

- Quando você altera uma senha de usuário do Insight, a entrada do usuário na tabela SANscreen.Users será atualizada com o novo hash.
- Quando você altera a senha de um usuário MySQL, a instrução SQL apropriada será executada para atualizar a senha do usuário na instância MySQL.

Em algumas situações, haverá várias alterações feitas na instalação:

- Quando você modifica o usuário dwh MySQL, além de atualizar a senha no banco de dados MySQL, várias entradas de Registro para ODBC também serão atualizadas.

Nas seções a seguir, o termo "mudanças coordenadas" é usado para descrever essas mudanças.

## Modos de execução

- Operação normal/padrão - o Serviço de servidor SANscreen deve estar em execução

Para o modo de execução padrão, a ferramenta SecurityAdmin requer que o serviço **servidor SANscreen** esteja em execução. O servidor é usado para autenticação, e muitas alterações coordenadas na instalação são feitas fazendo chamadas para o servidor.

- Operação direta - o Serviço de servidor SANscreen pode estar em execução ou parado.

Quando executado em uma instalação do OCI Server ou DWH, a ferramenta também pode ser executada no modo "direto". Neste modo, a autenticação e as alterações coordenadas são realizadas usando o banco de dados. O serviço servidor não é usado.

O funcionamento é o mesmo que o modo normal, com as seguintes exceções:

- A autenticação é suportada apenas para utilizadores de administração que não sejam de domínio. (Usuários cuja senha e funções estão no banco de dados, não LDAP).
- A operação "Substituir chaves" não é suportada.
- A etapa de re-criptografia da restauração do Vault é ignorada.
- A ferramenta também pode ser executada mesmo quando o acesso ao servidor e ao banco de dados não é possível (por exemplo, porque a senha raiz no cofre está incorreta).

Quando executado neste modo, a autenticação não é possível e, portanto, nenhuma operação com uma alteração coordenada para a instalação pode ser executada.

O modo de recuperação pode ser utilizado para:

- determine quais entradas do vault estão erradas (usando a operação verificar)
- substitua a senha raiz incorreta pelo valor correto. (Isso não altera a senha. O utilizador tem de introduzir a palavra-passe atual.)



Se a senha raiz no cofre estiver incorreta e a senha não for conhecida e não houver backup do cofre com a senha raiz correta, a instalação não poderá ser recuperada usando a ferramenta SecurityAdmin. A única maneira de recuperar a instalação é redefinir a senha da instância MySQL seguindo o procedimento documentado em <https://dev.mysql.com/doc/refman/8.4/en/resetting-permissions.html>. Depois de executar o procedimento de reinicialização, use a operação de senha armazenada correta para inserir a nova senha no cofre.

## Comandos

### Comandos irrestritos

Comandos irrestritos fazem quaisquer alterações coordenadas na instalação (exceto armazenamentos confiáveis). Comandos irrestritos podem ser executados sem autenticação do usuário.

Comando	Descrição
backup-vault	<p>Crie um arquivo zip contendo o cofre. O caminho relativo para os arquivos do Vault corresponderá ao caminho do Vault relativo à raiz da instalação.</p> <ul style="list-style-type: none"><li>• wildfly/standalone/configuration/vault/*</li><li>• acq/conf/vault/*</li></ul> <p>Observe que é altamente recomendável fazer backup do Vault sempre que você fizer backup de um banco de dados do OnCommand Insight.</p>
verifique se há teclas padrão	Verifique se as chaves do Vault correspondem às do Vault padrão usado em instâncias anteriores a 7.3.16.

palavra-passe guardada correta	<p>Substitua uma senha (incorreta) armazenada no cofre pela senha correta conhecida pelo usuário.</p> <p>Isso pode ser usado quando o Vault e a instalação não são consistentes.  <b>Observe que não altera a senha real na instalação.</b></p>
	<p>Altere a senha usada para um armazenamento de confiança e armazene a nova senha no cofre. A palavra-passe atual da loja de confiança tem de ser "conhecida".</p>
verifique-keystore	<p>verifique se os valores no cofre estão corretos:</p> <ul style="list-style-type: none"> <li>• Para usuários do OCI, o hash da senha corresponde ao valor no banco de dados</li> <li>• Para usuários MySQL, pode ser feita uma conexão de banco de dados</li> <li>• para keystores, o keystore pode ser carregado e suas chaves (se houver) lidas</li> </ul>
teclas de lista	<p>listar as entradas no cofre (sem mostrar o valor armazenado)</p>

### Comandos restritos

A autenticação é necessária para qualquer comando não oculto que faça alterações coordenadas na instalação:

Comando	Descrição
restaurar-vault-backup	<p>Substitui o Vault atual pelo Vault contido no arquivo de backup especificado.</p> <p>Executa todas as ações coordenadas para atualizar a instalação para corresponder às senhas no cofre restaurado:</p> <ul style="list-style-type: none"> <li>• Atualize as senhas de usuário de comunicação OCI</li> <li>• Atualize as senhas do usuário MySQL, incluindo root</li> <li>• para cada keystore, se a senha do keystore for "conhecida", atualize o keystore usando as senhas do cofre restaurado.</li> </ul> <p>Quando executado no modo normal, também lê cada valor criptografado da instância, descriptografa-o usando o serviço de criptografia do Vault atual, recriptografa-o usando o serviço de criptografia do Vault restaurado e armazena o valor recriptografado.</p>
sincronize-com-cofre	<p>Executa todas as ações coordenadas para atualizar a instalação para corresponder às senhas de usuário no cofre restaurado:</p> <ul style="list-style-type: none"> <li>• Atualiza as senhas de usuário de comunicação OCI</li> <li>• Atualiza as senhas do usuário MySQL, incluindo root</li> </ul>

alterar palavra-passe	Altera a senha no cofre e executa as ações coordenadas.
substitua as chaves	Crie um novo cofre vazio (que terá chaves diferentes do existente). Em seguida, copie as entradas do Vault atual para o novo Vault. Em seguida, lê cada valor encriptado da instância, descripta-o utilizando o serviço de encriptação do cofre atual, encripta-o novamente utilizando o serviço de encriptação do cofre restaurado e armazena o valor reencriptado.

## Ações coordenadas

### Cofre do servidor

_interno	atualizar hash de senha para usuário no banco de dados
aquisição	atualizar hash de senha para usuário no banco de dados  se o cofre de aquisição estiver presente, atualize também a entrada no cofre de aquisição
dwh_internal	atualizar hash de senha para usuário no banco de dados
cognos_admin	atualizar hash de senha para usuário no banco de dados  Se DWH e Windows, atualize SANscreen/cognos/analytics/Configuration/SANscreenAP.properties para definir a propriedade cognos.admin como a senha.
raiz	Execute SQL para atualizar a senha do usuário na instância do MySQL
inventário	Execute SQL para atualizar a senha do usuário na instância do MySQL

dwh	<p>Execute SQL para atualizar a senha do usuário na instância do MySQL</p> <p>Se DWH e Windows, atualize o Registro do Windows para definir as seguintes entradas relacionadas a ODBC para a nova senha:</p> <ul style="list-style-type: none"> <li>• HKEY_LOCAL_MACHINE/SOFTWARE/Wow6432Node ODBC.INI/dwh_Capacity/PWD</li> <li>• HKEY_LOCAL_MACHINE/SOFTWARE/Wow6432Node ODBC/dwh_Capacity_Efficiency/PWD</li> <li>• HKEY_LOCAL_MACHINE_SOFTWARE/Wow6432Node ODBC.INI/dwh_fs_util/PWD</li> <li>• HKEY_LOCAL_MACHINE/SOFTWARE/Wow6432Node ODBC.INI/dwh_inventory/PWD</li> <li>• HKEY_LOCAL_MACHINE/SOFTWARE/Wow6432Node ODBC.INI/dwh_performance/PWD</li> <li>• HKEY_LOCAL_MACHINE/SOFTWARE/Wow6432Node ODBC/dwh_ports/PWD</li> <li>• HKEY_LOCAL_MACHINE/SOFTWARE/Wow6432Node ODBC.INI/dwh_sa/PWD</li> <li>• HKEY_LOCAL_MACHINE/SOFTWARE/Wow6432Node ODBC.INI/dwh_cloud_cost/PWD</li> </ul>
dwhuser	Execute SQL para atualizar a senha do usuário na instância do MySQL
hosts	Execute SQL para atualizar a senha do usuário na instância do MySQL
keystore_password	reescreva o keystore com a nova senha - wildfly/standalone/configuration/server.keystore
truststore_password	reescreva o keystore com a nova senha - wildfly/standalone/configuration/server.trustore
key_password	reescreva o keystore com a nova senha - wildfly/standalone/configuration/sso.jks
cognos_archive	nenhum

### Aquisição do Vault

aquisição	nenhum
truststore_password	reescreva o keystore com a nova senha (se existir) - acq/conf/cert/client.keystore

### Executando a ferramenta Security Admin - linha de comando

A sintaxe para executar a ferramenta SA no modo de linha de comando é:

```
securityadmin [-s | -au] [-db] [-lu <user> [-lp <password>]] <additional-  
options>
```

where

```
-s                selects server vault  
-au              selects acquisition vault  
  
-db              selects direct operation mode  
  
-lu <user>       user for authentication  
-lp <password>   password for authentication  
<addition-options> specifies command and command arguments as  
described below
```

#### Notas:

- A opção "-i" pode não estar presente na linha de comando (uma vez que seleciona o modo interativo).
- para as opções "-s" e "-au":
  - "-s" não é permitido numa RAU
  - "-au" não é permitido na DWH
  - se nenhum dos dois estiver presente, então
    - O cofre do servidor é selecionado em servidor, DWH e Dual
    - O cofre de aquisição é selecionado na RAU
- As opções -lu e -lp são usadas para autenticação do usuário.
  - Se o <user> for especificado e o <password> não for, o usuário será solicitado a digitar a senha.
  - Se o <user> não for fornecido e a autenticação for necessária, o usuário será solicitado a fornecer o <user> e o <password>.

#### Comandos:

Comando	Utilização
palavra-passe guardada correta	<pre>securityadmin [-s</pre>

<p><code>-au] [-db] -pt &lt;key&gt; [&lt;value&gt;]</code></p> <p>where</p> <p><code>-pt</code> specifies the command ("put") <code>&lt;key&gt;</code> is the key <code>&lt;value&gt;</code> is the value. If not present, user will be prompted for value</p>	<p>backup-vault</p>
<p>securityadmin [-s</p>	<p><code>-au] [-db] -b [&lt;backup-dir&gt;]</code></p> <p>where</p> <p><code>-b</code> specified command <code>&lt;backup-dir&gt;</code> is the output directory. If not present, default location of SANscreen/backup/vault is used The backup file will be named ServerSecurityBackup-yyyy-MM-dd-HH-mm.zip</p>
<p>backup-vault</p>	<p>securityadmin [-s</p>
<p><code>-au] [-db] -ub &lt;backup-file&gt;</code></p> <p>where</p> <p><code>-ub</code> specified command ("upgrade-backup") <code>&lt;backup-file&gt;</code> The location to write the backup file</p>	<p>teclas de lista</p>
<p>securityadmin [-s</p>	<p><code>-au] [-db] -l</code></p> <p>where</p> <p><code>-l</code> specified command</p>



<p>teclas de verificação</p>	<pre>securityadmin [-s</pre>
<p>-au] [-db] -ck</p> <p>where</p> <p>-ck specified command</p> <p>exit code: 1 error 2 default key(s) 3 unique keys</p> <pre>securityadmin [-s</pre>	<p>verificar-keystore (servidor)</p>
<pre>securityadmin [-s] [-db] -v</pre> <p>where</p> <p>-v specified command</p>	<p>atualização</p>
<pre>securityadmin [-s</pre>	<p>-au] [-db] [-lu &lt;user&gt;] [-lp &lt;password&gt;] -u</p> <p>where</p> <p>-u specified command</p> <p>For server vault, if -lu is not present, then authentication will be performed for &lt;user&gt; = _internal and &lt;password&gt; = _internal's password from vault. For acquisition vault, if -lu is not present, then no authentication will be attempted</p> <pre>securityadmin [-s</pre>
<p>substitua as chaves</p>	<pre>securityadmin [-s</pre>

<p>-au] [-db] [-lu &lt;user&gt;] [-lp &lt;password&gt;] -rk</p> <p>where</p> <p>-rk specified command</p> <div data-bbox="136 331 461 403" style="border: 1px solid #ccc; height: 34px; width: 100%;"></div>	<p>restaurar-vault-backup</p>
<div data-bbox="136 449 461 588" style="border: 1px solid #ccc; padding: 5px;"> <p>securityadmin [-s</p> </div>	<p>-au] [-db] [-lu &lt;user&gt;] [-lp &lt;password&gt;] -r &lt;backup-file&gt;</p> <p>where</p> <p>-r specified command &lt;backup-file&gt; the backup file location</p> <div data-bbox="480 646 1487 718" style="border: 1px solid #ccc; height: 34px; width: 100%;"></div>
<p>alterar palavra-passe (servidor)</p>	<div data-bbox="480 760 1487 1222" style="border: 1px solid #ccc; padding: 10px;"> <p>securityadmin [-s] [-db] [-lu &lt;user&gt;] [-lp &lt;password&gt;] -up -un &lt;user&gt; -p [&lt;password&gt;] [-sh]</p> <p>where</p> <p>-up                    specified command ("update-password")</p> <p>-un &lt;user&gt;            entry ("user") name to update</p> <p>-p &lt;password&gt; new password. If &lt;password not supplied, user will be prompted.</p> <p>-sh                    for mySQL user, use strong hash</p> </div>
<p>alterar palavra-passe para utilizador de aquisição (aquisição)</p>	<div data-bbox="480 1268 1487 1646" style="border: 1px solid #ccc; padding: 10px;"> <p>securityadmin [-au] [-db] [-lu &lt;user&gt;] [-lp &lt;password&gt;] -up -p [&lt;password&gt;]</p> <p>where</p> <p>-up                    specified command ("update-password")</p> <p>-p &lt;password&gt; new password. If &lt;password not supplied, user will be prompted.</p> </div>

<p>alterar-senha para truststore_password (aquisição)</p>	<pre>securityadmin [-au] [-db] [-lu &lt;user&gt;] [-lp &lt;password&gt;] -utp -p [&lt;password&gt;]</pre> <p>where</p> <p>-utp                    specified command ("update-truststore-password")</p> <p>-p &lt;password&gt; new password. If &lt;password not supplied, user will be prompted.</p>
<p>sincronizar com cofre (servidor)</p>	<pre>securityadmin [-s] [-db] [-lu &lt;user&gt;] [-lp &lt;password&gt;] -sv &lt;backup-file&gt;</pre> <p>where</p> <p>-sv                    specified command</p>

## Executar a ferramenta de administração de segurança - modo interativo

### Interativo - Menu principal

Para executar a ferramenta SA no modo interativo, digite o seguinte comando:

```
securityadmin -i
```

Em um servidor ou instalação dupla, o SecurityAdmin solicitará ao usuário que selecione o servidor ou a unidade de aquisição local.

Detectados nós de servidor e Unidade de aquisição! Selecione o nó cuja segurança precisa ser reconfigurada:

```
1 - Server

2 - Local Acquisition Unit

9 - Exit

Enter your choice:
```

No DWH, "Server" (servidor) é selecionado automaticamente. Numa AU remota, a opção "Acquisition Unit" (Unidade de aquisição) será selecionada automaticamente.

## Interactive - servidor: Recuperação de senha root

No modo servidor, a ferramenta SecurityAdmin primeiro verificará se a senha raiz armazenada está correta. Caso contrário, a ferramenta exibirá a tela de recuperação de senha raiz.

```
ERROR: Database is not accessible

1 - Enter root password

2 - Get root password from vault backup

9 - Exit

Enter your choice:
```

Se a opção 1 estiver selecionada, o usuário será solicitado a digitar a senha correta.

```
Enter password (blank = don't change)
Enter correct password for 'root':
Se for introduzida a palavra-passe correta, é apresentado o seguinte.
```

```
Password verified. Vault updated
Pressionar ENTER exibirá o menu irrestrito do servidor.
```

Se for introduzida a palavra-passe errada, será apresentado o seguinte

```
Password verification failed - Access denied for user 'root'@'localhost'
(using password: YES)
Premir ENTER regressa ao menu de recuperação.
```

Se a opção 2 estiver selecionada, o usuário será solicitado a fornecer o nome de um arquivo de backup a partir do qual ler a senha correta:

```
Enter Backup File Location:
Se a senha do backup estiver correta, será exibido o seguinte.
```

```
Password verified. Vault updated
Pressionar ENTER exibirá o menu irrestrito do servidor.
```

Se a palavra-passe na cópia de segurança estiver incorreta, será apresentado o seguinte

```
Password verification failed - Access denied for user 'root'@'localhost'  
(using password: YES)  
Premir ENTER regressa ao menu de recuperação.
```

### **Interactive - servidor: Senha correta**

A ação "corrigir senha" é usada para alterar a senha armazenada no cofre para que ela corresponda à senha real exigida pela instalação. Este comando é útil em situações em que uma mudança na instalação foi feita por algo diferente da ferramenta securityadmin. Os exemplos incluem:

- A senha de um usuário SQL foi modificada pelo acesso direto ao MySQL.
- Um keystore é substituído ou a senha de um keystore é alterada usando keytool.
- Um banco de dados OCI foi restaurado e esse banco de dados tem senhas diferentes para os usuários internos

"Corrigir senha" primeiro solicitará ao usuário que selecione a senha que deseja armazenar o valor correto.

Replace incorrect stored password with correct password. (Does not change the required password)

Select User: (Enter 'b' to go Back)

- 1 - \_internal
- 2 - acquisition
- 3 - cognos\_admin
- 4 - cognos keystore
- 5 - dwh
- 6 - dwh\_internal
- 7 - dwhuser
- 8 - hosts
- 9 - inventory
- 10 - sso keystore
- 11 - server keystore
- 12 - root
- 13 - server truststore
- 14 - AU truststore

Enter your choice:

Depois de selecionar qual entrada corrigir, o usuário é solicitado a fornecer o valor.

- 1 - Enter {user} password
- 2 - Get {user} password from vault backup
- 9 - Exit

Enter your choice:

Se a opção 1 estiver selecionada, o usuário será solicitado a digitar a senha correta.

```
Enter password (blank = don't change)
Enter correct password for '{user}':
Se for introduzida a palavra-passe correta, é apresentado o seguinte.
```

```
Password verified. Vault updated
Pressionar ENTER retornará ao menu irrestrito do servidor.
```

Se for introduzida a palavra-passe errada, será apresentado o seguinte

```
Password verification failed - {additional information}
Vault entry not updated.
```

Pressionar ENTER retornará ao menu irrestrito do servidor.

Se a opção 2 estiver selecionada, o usuário será solicitado a fornecer o nome de um arquivo de backup a partir do qual ler a senha correta:

```
Enter Backup File Location:
Se a senha do backup estiver correta, será exibido o seguinte.
```

```
Password verified. Vault updated
Pressionar ENTER exibirá o menu irrestrito do servidor.
```

Se a palavra-passe na cópia de segurança estiver incorreta, será apresentado o seguinte

```
Password verification failed - {additional information}
Vault entry not updated.
```

Pressionar ENTER exibirá o menu irrestrito do servidor.

### Interativo - servidor: Verifique o conteúdo do Vault

Verificar o conteúdo do Vault verificará se o Vault tem chaves que correspondem ao Vault padrão distribuído com versões anteriores do OCI e verificará se cada valor no Vault corresponde à instalação.

Os resultados possíveis para cada chave são:

OK	O valor do cofre está correto
Não verificado	O valor não pode ser verificado em relação à instalação
RUIM	O valor não corresponde à instalação

Em falta

Falta uma entrada esperada.

```
Encryption keys secure: unique, non-default encryption keys detected
```

```
    cognos_admin: OK
      hosts: OK
    dwh_internal: OK
      inventory: OK
        dwhuser: OK
    keystore_password: OK
      dwh: OK
    truststore_password: OK
      root: OK
        _internal: OK
    cognos_internal: Not Checked
      key_password: OK
        acquisition: OK
    cognos_archive: Not Checked
    cognos_keystore_password: Missing
```

```
Press enter to continue
```

### Interactive - servidor: Backup

O backup solicitará o diretório no qual o arquivo zip de backup deve ser armazenado. O diretório já deve existir e o nome do arquivo será ServerSecurityBackup-yyyy-mm-dd-hh-mm.zip.

```
Enter backup directory location [C:\Program Files\SANscreen\backup\vault]
:
```

```
Backup Succeeded!   Backup File: C:\Program
Files\SANscreen\backup\vault\ServerSecurityBackup-2024-08-09-12-02.zip
```

### Interactive - servidor: Login

A ação de login é usada para autenticar um usuário e obter acesso a operações que modificam a instalação. O usuário deve ter Privileges de administrador. Ao executar com o servidor, qualquer usuário admin pode ser usado; ao executar no modo direto, o usuário deve ser um usuário local em vez de um usuário LDAP.



```
Authenticating via server. Enter user and password
```

```
UserName: admin
```

```
Password:
```

ou

```
Authenticating via database. Enter local user and password.
```

```
UserName: admin
```

```
Password:
```

Se a senha estiver correta e o usuário for um usuário admin, o menu restrito será exibido.

Se a palavra-passe estiver incorreta, será apresentado o seguinte:

```
Authenticating via database. Enter local user and password.
```

```
UserName: admin
```

```
Password:
```

```
Login Failed!
```

Se o usuário não for um administrador, o seguinte será exibido:

```
Authenticating via server. Enter user and password
```

```
UserName: user
```

```
Password:
```

```
User 'user' does not have 'admin' role!
```

### **Interativo - servidor: Menu restrito**

Depois de o utilizador iniciar sessão, a ferramenta apresenta o Menu restrito.

```
Logged in as: admin
```

```
Select Action:
```

```
2 - Change Password
```

```
3 - Verify Vault Contents
```

```
4 - Backup
```

```
5 - Restore
```

```
6 - Change Encryption Keys
```

```
7 - Fix installation to match vault
```

```
9 - Exit
```

```
Enter your choice:
```

### **Interactive - servidor: Alterar senha**

A ação "Change Password" (alterar palavra-passe) é utilizada para alterar uma palavra-passe de instalação para um novo valor.

"Change Password" (alterar palavra-passe) solicitará primeiro ao utilizador que selecione a palavra-passe que pretende alterar.

```
Change Password
Select User: (Enter 'b' to go Back)

1 - _internal
2 - acquisition
3 - cognos_admin
4 - cognos keystore
5 - dwh
6 - dwh_internal
7 - dwhuser
8 - hosts
9 - inventory
10 - sso keystore
11 - server keystore
12 - root
13 - server truststore
14 - AU truststore

Enter your choice:
```

Depois de selecionar qual entrada corrigir, se o usuário for um usuário MySQL, o usuário será perguntado se deseja hash forte para a senha

```
MySQL supports SHA-1 and SHA-256 password hashes. SHA-256 is stronger but
requires all clients use SSL connections
```

```
Use strong password hash? (Y/n): y
```

Em seguida, o usuário é solicitado a fornecer a nova senha.

```
New Password for '{user}':  
If the password is empty, the operation is cancelled.  
  
Password is empty - cancelling operation
```

Se for introduzida uma palavra-passe não vazia, é pedido ao utilizador que confirme a palavra-passe.

```
New Password for '{user}':  
  
Confirm New Password for '{user}':  
  
Password successfully updated for 'dwhuser'!
```

Se a alteração não for bem-sucedida, o erro ou a exceção serão exibidos.

### **Interactive - servidor: Restauração**

#### **Interactive - servidor: Alterar chaves de criptografia**

A ação alterar chaves de criptografia substituirá a chave de criptografia usada para criptografar as entradas do Vault e substituirá a chave de criptografia usada para o serviço de criptografia do Vault. Como a chave do serviço de criptografia é alterada, os valores criptografados no banco de dados serão recriptografados; eles serão lidos, descriptografados com a chave atual, criptografados com a nova chave e salvos de volta ao banco de dados.

Esta ação não é suportada no modo direto, uma vez que o servidor fornece a operação de recriptação para algum conteúdo de base de dados.

```
Replace encryption key with new key and update encrypted database values  
  
Confirm (y/N): y  
  
Change Encryption Keys succeeded! Restart 'Server' Service!
```

#### **Interactive - servidor: Corrigir instalação**

A ação Fix Installation atualizará a instalação. Todas as senhas de instalação que podem ser alteradas através da ferramenta securityadmin, exceto root, serão definidas para as senhas no cofre.

- As senhas dos usuários internos do OCI serão atualizadas.
- As senhas dos usuários MySQL, exceto root, serão atualizadas.
- As senhas dos keystores serão atualizadas.

```
Fix installation - update installation passwords to match values in vault

Confirm: (y/N): y

Installation update succeeded! Restart 'Server' Service.
```

A ação irá parar na primeira atualização mal sucedida e apresentar o erro ou exceção.

## Gerenciamento da segurança no servidor Insight

A `securityadmin` ferramenta permite gerenciar opções de segurança no servidor Insight. O gerenciamento de segurança inclui alterar senhas, gerar novas chaves, salvar e restaurar configurações de segurança criadas por você ou restaurar configurações para as configurações padrão.

### Sobre esta tarefa

Você usa a `securityadmin` ferramenta para gerenciar a segurança:

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

Consulte "[SecurityAdmin](#)" a documentação para obter mais informações.

## Gestão da segurança na unidade de aquisição local

A `securityadmin` ferramenta permite gerenciar opções de segurança no usuário de aquisição local (LAU). 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

Você deve ter `admin` o Privileges para executar tarefas de configuração de segurança.

### Sobre esta tarefa

Você usa a `securityadmin` ferramenta para gerenciar a segurança:

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

Consulte "[Ferramenta SecurityAdmin](#)" as instruções para obter mais informações.

## Gerenciamento de segurança em uma RAU

A `securityadmin` ferramenta permite gerenciar opções de segurança em RAUs.

Talvez seja necessário fazer backup ou restaurar uma configuração de cofre, alterar chaves de criptografia ou atualizar senhas para as unidades de aquisição.

### Sobre esta tarefa

Você usa a `securityadmin` ferramenta para gerenciar a segurança:

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

Um cenário para atualizar a configuração de segurança para o LAU/RAU é atualizar a senha do usuário 'aquisição' quando a senha para esse usuário tiver sido alterada no servidor. A LAU e todas as RAUs usam a mesma senha que a do usuário de 'aquisição' do servidor para se comunicar com o servidor.

O utilizador de 'aquisição' só existe no servidor Insight. A RAU ou LAU faz login como esse usuário quando eles se conectam ao servidor.

Consulte "[Ferramenta SecurityAdmin](#)" as instruções para obter mais informações.

## Gestão da segurança no Data Warehouse

A `securityadmin` ferramenta permite gerenciar opções de segurança no servidor Data Warehouse. O gerenciamento de segurança inclui a atualização de senhas internas para usuários internos no servidor DWH, a criação de backups da configuração de segurança ou a restauração de configurações para as configurações padrão.

### Sobre esta tarefa

Você usa a `securityadmin` ferramenta para gerenciar a segurança:

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

Consulte "[SecurityAdmin](#)" a documentação para obter mais informações.

## Alterando senhas internas de usuário do OnCommand Insight

As políticas de segurança podem exigir que você altere as senhas em seu ambiente OnCommand Insight. Algumas das senhas em um servidor existem em um servidor diferente no ambiente, exigindo que você altere a senha em ambos os servidores. Por exemplo, quando você altera a senha do usuário "inventário" no Insight Server, você deve corresponder à senha do usuário "inventário" no conector do servidor do Data Warehouse configurado para esse Insight Server.

### Antes de começar



Você deve entender as dependências das contas de usuário antes de alterar senhas. A falha na atualização de senhas em todos os servidores necessários resultará em falhas de comunicação entre os componentes do Insight.

## Sobre esta tarefa

A tabela a seguir lista as senhas de usuário internas do Insight Server e lista os componentes do Insight que têm senhas dependentes que precisam corresponder à nova senha.

Senhas do Insight Server	Alterações necessárias
_interno	
aquisição	LAU, RAU
dwh_internal	Armazém de dados
hosts	
inventário	Armazém de dados
raiz	

A tabela a seguir lista as senhas de usuário internas do Data Warehouse e lista os componentes do Insight que têm senhas dependentes que precisam corresponder à nova senha.

Senhas do Data Warehouse	Alterações necessárias
cognos_admin	
dwh	
dwh_internal (alterado usando a IU de configuração do conector do servidor)	Servidor Insight
dwhuser	
hosts	
Inventário (alterado usando a IU de configuração do conector do servidor)	Servidor Insight
raiz	

## Alterando senhas na IU de Configuração da conexão do servidor DWH

A tabela a seguir lista a senha do usuário para a LAU e lista os componentes do Insight que têm senhas dependentes que precisam corresponder à nova senha.

Palavras-passe LAU	Alterações necessárias
aquisição	Insight Server, RAU

## Alterar as senhas "inventário" e "dwh\_internal" usando a IU de Configuração de conexão do servidor

Se você precisar alterar as senhas "inventário" ou "dwh\_internal" para corresponder às do servidor Insight, use a IU do Data Warehouse.

### Antes de começar

Você deve estar conectado como administrador para executar esta tarefa.

### Passos

1. Faça login no Portal do Armazém de dados em <https://hostname/dwh>, onde hostname é o nome do sistema onde o Armazém de dados OnCommand Insight está instalado.
2. No painel de navegação à esquerda, clique em **Connectors**.

É apresentado o ecrã **Edit Connector** (Editar conetor).

#### Edit Connector

The screenshot shows the 'Edit Connector' form with the following fields and values:

- ID: 1
- Encryption: Enabled
- Name: Oci-stg06-s12r2.nane.netapp.com
- Host: Oci-stg06-s12r2.nane.netapp.com
- Database user name: inventory
- Database password: [masked]

At the bottom of the form, there is an 'Advanced' dropdown menu and four buttons: Save, Cancel, Test, and Remove.

3. Insira uma nova senha de "inventário" para o campo **Senha do banco de dados**.
4. Clique em **Salvar**
5. Para alterar a senha "dWH\_internal", clique em **Avançado**.

É apresentado o ecrã Edit Connector Advanced (Editar conetor avançado).



## Edit Connector

ID:	<input type="text" value="1"/>
Encryption:	<input type="text" value="Enabled"/>
Name:	<input type="text" value="Oci-stg06-s12r2.nane.netapp.com"/>
Host:	<input type="text" value="Oci-stg06-s12r2.nane.netapp.com"/>
Database user name:	<input type="text" value="inventory"/>
Database password:	<input type="password" value="....."/>
Server user name:	<input type="text" value="dwh_internal"/>
Server password:	<input type="password" value="....."/>
HTTPS port:	<input type="text" value="443"/>
TCP port:	<input type="text" value="3306"/>

Basic ^

6. Digite a nova senha no campo **Senha do servidor**:

7. Clique em Save (Guardar).

### Alterando a senha dwh usando a ferramenta Administração ODBC

Quando alterar a palavra-passe para o utilizador dwh no servidor Insight, a palavra-passe também tem de ser alterada no servidor Data Warehouse. Você usa a ferramenta Administrador de origem de dados ODBC para alterar a senha no Data Warehouse.

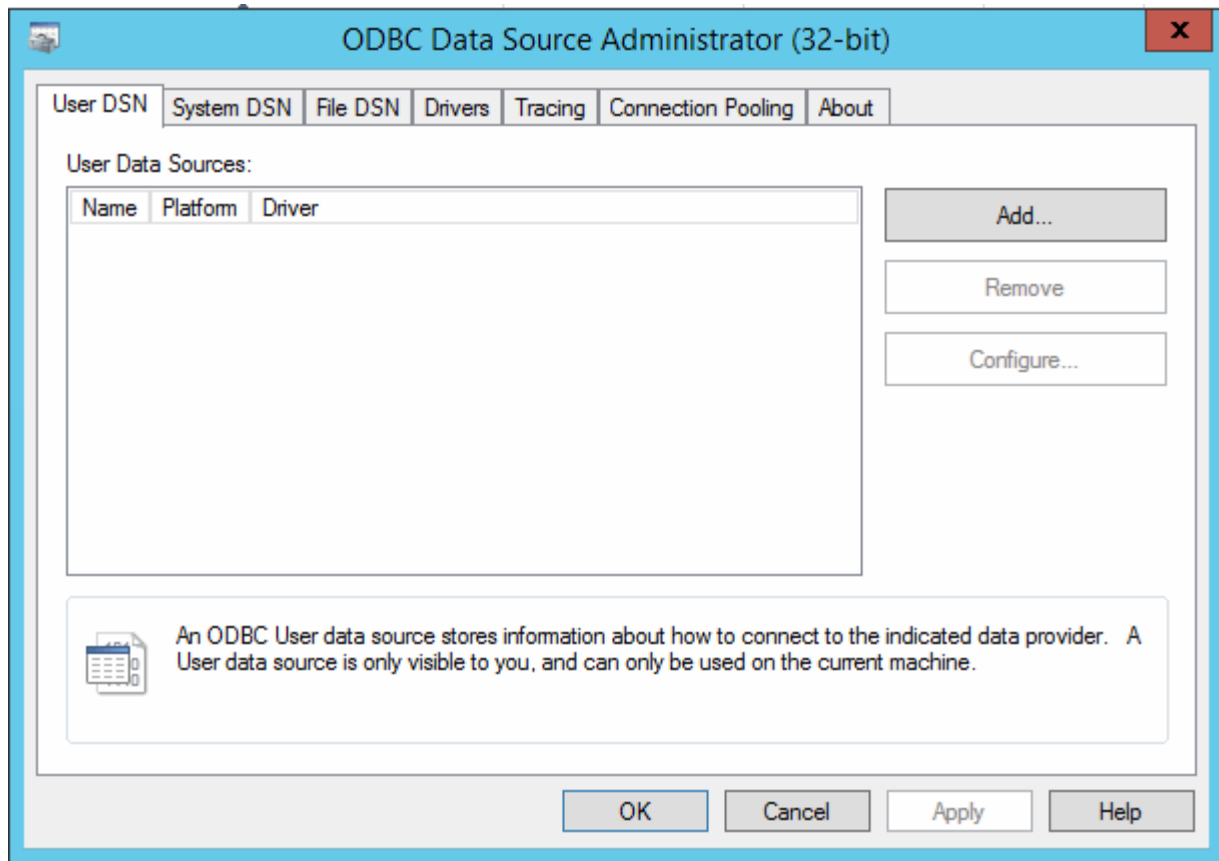
#### Antes de começar

Tem de efetuar um início de sessão remoto no servidor do Armazém de dados utilizando uma conta com o administrador Privileges.

#### Passos

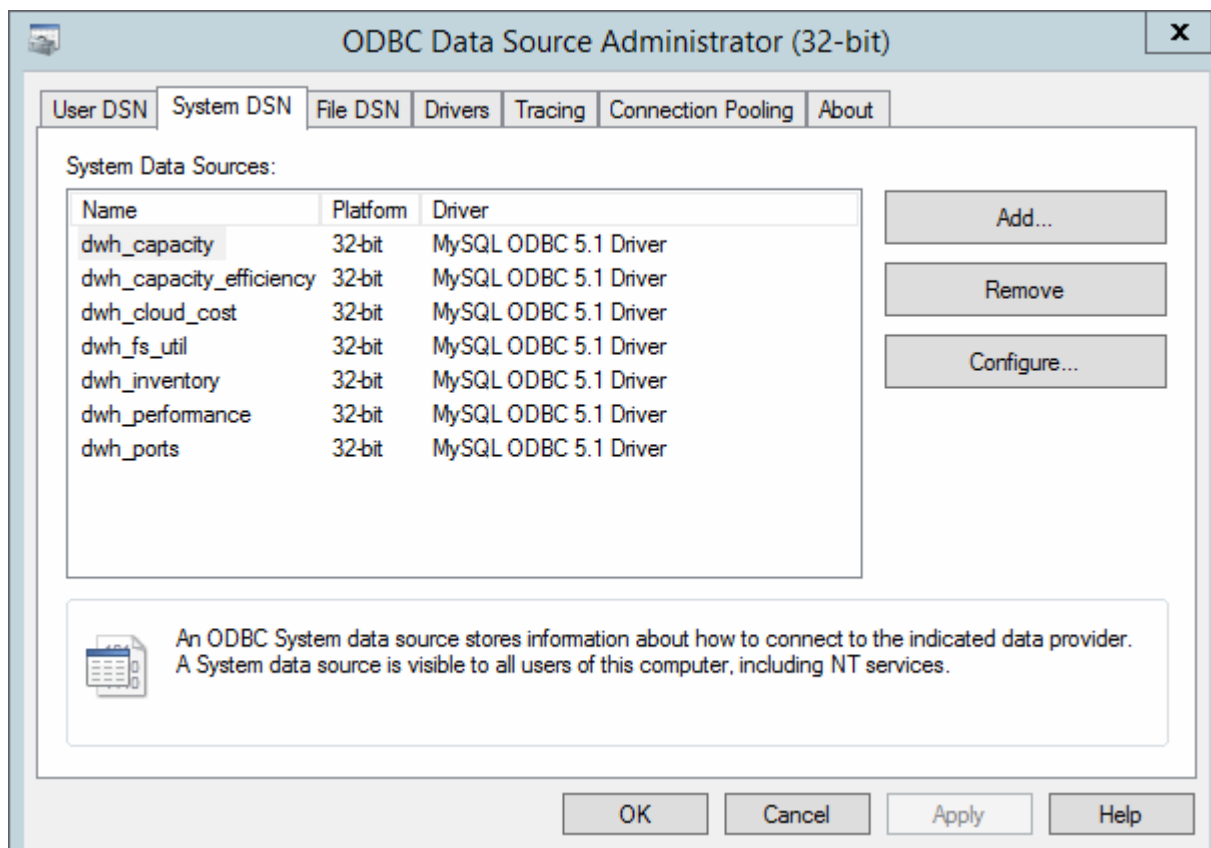
1. Faça um login remoto no servidor que hospeda esse Data Warehouse.
2. Acesse a ferramenta Administração ODBC em `C:\windows\SysWOW64\odbcad32.exe`

O sistema exibe a tela Administrador da fonte de dados ODBC.



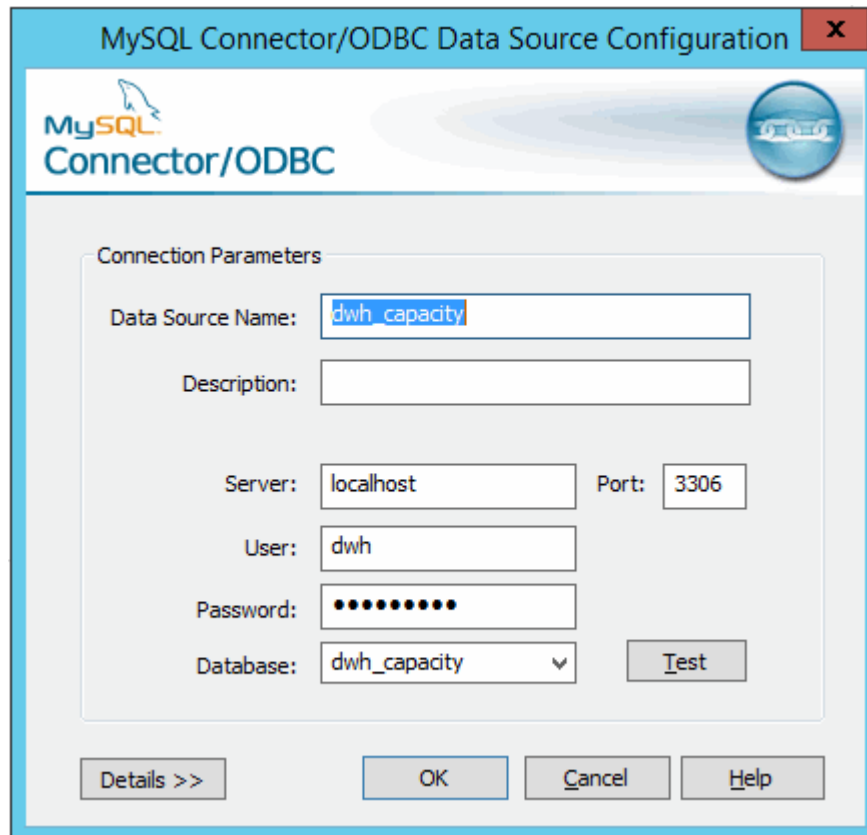
3. Clique em **System DSN**

São apresentadas as fontes de dados do sistema.



4. Selecione uma fonte de dados OnCommand Insight na lista.
5. Clique em **Configurar**

É apresentado o ecrã Data Source Configuration (Configuração da fonte de dados).



6. Introduza a nova palavra-passe no campo **Palavra-passe**.

## Suporte para Smart Card e certificado de login

O OnCommand Insight suporta o uso de cartões inteligentes (CAC) e certificados para autenticar usuários fazendo login nos servidores do Insight. Tem de configurar o sistema para ativar estas funcionalidades.

Depois de configurar o sistema para suportar CAC e certificados, navegar para uma nova sessão do OnCommand Insight resulta no navegador exibindo uma caixa de diálogo nativa fornecendo ao usuário uma lista de certificados pessoais para escolher. Esses certificados são filtrados com base no conjunto de certificados pessoais que foram emitidos por CAs confiáveis pelo servidor OnCommand Insight. Na maioria das vezes, há uma única escolha. Por padrão, o Internet Explorer ignora essa caixa de diálogo se houver apenas uma opção.



Para usuários do CAC, os cartões inteligentes contêm vários certificados, apenas um dos quais pode corresponder à CA confiável. O certificado CAC para *identification* deve ser utilizado.

Para obter as instruções de CAC e certificado mais atualizadas, consulte os seguintes artigos da base de conhecimento (login de suporte necessário):



- ["Como configurar a autenticação de cartão de acesso comum \(CAC\) para o OnCommand Insight"](#)
- ["Como configurar a autenticação de cartão de acesso comum \(CAC\) para o armazém de dados OnCommand Insight"](#)
- ["Como criar e importar um certificado assinado pela autoridade de certificação \(CA\) para o OnComand Insight e o Data Warehouse 7,3.x do OnCommand Insight"](#)
- ["Como criar um certificado autoassinado no OnCommand Insight 7,3.X instalado em um host Windows"](#)
- ["Como importar um certificado assinado pela autoridade de certificação \(CA\) do Cognos para o datawarehouse 7.3.3 e posterior do OnCommand"](#)

## Configurando hosts para Smart Card e login de certificado

Você deve fazer modificações na configuração do host do OnCommand Insight para oferecer suporte a logins de cartão inteligente (CAC) e certificado.

### Antes de começar

- O LDAP tem de estar ativado no sistema.
- O atributo LDAP `User principal account name` deve corresponder ao campo LDAP que contém a ID de um usuário.



Se você alterou as senhas `Server.keystore` e/ou `Server.trustore` usando "administrador de segurança", reinicie o serviço `SANscreen` antes de importar o certificado LDAP.

Para obter as instruções de CAC e certificado mais atualizadas, consulte os seguintes artigos da base de conhecimento (login de suporte necessário):



- ["Como configurar a autenticação de cartão de acesso comum \(CAC\) para o OnCommand Insight"](#)
- ["Como configurar a autenticação de cartão de acesso comum \(CAC\) para o armazém de dados OnCommand Insight"](#)
- ["Como criar e importar um certificado assinado pela autoridade de certificação \(CA\) para o OnComand Insight e o Data Warehouse 7,3.x do OnCommand Insight"](#)
- ["Como criar um certificado autoassinado no OnCommand Insight 7,3.X instalado em um host Windows"](#)
- ["Como importar um certificado assinado pela autoridade de certificação \(CA\) do Cognos para o datawarehouse 7.3.3 e posterior do OnCommand"](#)

### Passos

1. Use o `regedit` utilitário para modificar os valores do Registro no `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun2.0\SANscreen Server\Parameters\Java:`

- a. Altere a opção JVM\_Option DclientAuth=false para DclientAuth=true.
2. Faça backup do arquivo keystore: C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore
3. Abra um prompt de comando especificando Run as administrator
4. Excluir o certificado gerado automaticamente: C:\Program Files\SANscreen\java64\bin\keytool.exe -delete -alias "ssl certificate" -keystore C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore
5. Gerar um novo certificado: C:\Program Files\SANscreen\java64\bin\keytool.exe -genkey -alias "alias\_name" -keyalg RSA -sigalg SHA1withRSA -keysize 2048 -validity 365 -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -dname "CN=commonName,OU=orgUnit,O=orgName,L=localityNameI,S=stateName,C=countryName"
6. Gerar uma solicitação de assinatura de certificado (CSR): C:\Program Files\SANscreen\java64\bin\keytool.exe -certreq -sigalg SHA1withRSA -alias "alias\_name" -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -file C:\temp\server.csr"
7. Depois que o CSR for devolvido na etapa 6, importe o certificado e, em seguida, exporte o certificado no formato base-64 e coloque-o em "C:\temp" named servername.cer.
8. Extraia o certificado do keystore: C:\Program Files\SANscreen\java64\bin\keytool.exe -v -importkeystore -srckeystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -srcalias "alias\_name" -destkeystore "C:\temp\file.p12" -deststoretype PKCS12
9. Extraia uma chave privada do arquivo p12: openssl pkcs12 -in "C:\temp\file.p12" -out "C:\temp\servername.private.pem"
10. Mesclar o certificado base-64 que você exportou na etapa 7 com a chave privada: openssl pkcs12 -export -in "<folder>\<certificate>.cer" -inkey "C:\temp\servername.private.pem" -out "C:\temp\servername.new.p12" -name "servername.abc.123.yyy.zzz"
11. Importe o certificado mesclado para o keystore: C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -destkeystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -srckeystore "C:\temp\servername.new.p12" -srcstoretype PKCS12 -alias "alias\_name"
12. Importar o certificado raiz: C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -file "C:\<root\_certificate>.cer" -trustcacerts -alias "alias\_name"
13. Importe o certificado raiz para o Server.trustore: C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.trustore" -file "C:\<email\_certificate>.cer" -trustcacerts -alias "alias\_name"
14. Importar o certificado intermédio: C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.trustore" -file

```
"C:\<intermediate_certificate>.cer" -trustcacerts -alias "alias_name"
```

Repita esta etapa para todos os certificados intermediários.

15. Especifique o domínio no LDAP para corresponder a este exemplo.

16. Reinicie o servidor.

## Configurar um cliente para suportar Smart Card e login de certificado

As máquinas cliente requerem middleware e modificações nos navegadores para permitir o uso de Smart Cards e para login no certificado. Os clientes que já estão a utilizar cartões inteligentes não devem necessitar de modificações adicionais nas suas máquinas cliente.

### Antes de começar

Para obter as instruções de CAC e certificado mais atualizadas, consulte os seguintes artigos da base de conhecimento (login de suporte necessário):



- ["Como configurar a autenticação de cartão de acesso comum \(CAC\) para o OnCommand Insight"](#)
- ["Como configurar a autenticação de cartão de acesso comum \(CAC\) para o armazém de dados OnCommand Insight"](#)
- ["Como criar e importar um certificado assinado pela autoridade de certificação \(CA\) para o OnComand Insight e o Data Warehouse 7,3.x do OnCommand Insight"](#)
- ["Como criar um certificado autoassinado no OnCommand Insight 7,3.X instalado em um host Windows"](#)
- ["Como importar um certificado assinado pela autoridade de certificação \(CA\) do Cognos para o datawarehouse 7.3.3 e posterior do OnCommand"](#)

### Sobre esta tarefa

Os seguintes são os requisitos comuns de configuração do cliente:

- Instalando o middleware Smart Card, como o ActivClient ( <http://militarycac.com/activclient.htm>consulte )
- Modificação do navegador IE ( [http://militarycac.com/files/Making\\_AKO\\_work\\_with\\_Internet\\_Explorer\\_color.pdf](http://militarycac.com/files/Making_AKO_work_with_Internet_Explorer_color.pdf)consulte )
- Modificação do navegador Firefox ( <https://militarycac.com/firefox2.htm>consulte )

## Habilitando CAC em um servidor Linux

Algumas modificações são necessárias para habilitar o CAC em um servidor Linux OnCommand Insight.

A CA raiz deve ser importada para o repositório de confiança.

## Passos

1. Navegue para `/opt/netapp/oci/conf/`
2. Editar `wildfly.properties` e alterar o valor de `CLIENT_AUTH_ENABLED` para "verdadeiro"
3. Importe o "certificado raiz" que existe em  
`/opt/netapp/oci/wildfly/standalone/configuration/server.truststore`
4. Reinicie o servidor

## Configurando o Data Warehouse para Smart Card e login de certificado

Você deve modificar a configuração do Armazém de dados do OnCommand Insight para oferecer suporte a logins de cartão inteligente (CAC) e certificado.

### Antes de começar

- O LDAP tem de estar ativado no sistema.
- O atributo LDAP `User principal account name` deve corresponder ao campo LDAP que contém o número de ID de governo de um usuário.

A denominação comum (CN) armazenada em CAC emitidas pelo Governo é normalmente do seguinte formato: `first.last.ID`. Para alguns campos LDAP, como `sAMAccountName`, este formato é demasiado longo. Para esses campos, o OnCommand Insight extrai apenas o número de ID do CNS.



Se você alterou as senhas `Server.keystore` e/ou `Server.trustore` usando "administrador de segurança", reinicie o serviço `SANscreen` antes de importar o certificado LDAP.

Para obter as instruções de CAC e certificado mais atualizadas, consulte os seguintes artigos da base de conhecimento (login de suporte necessário):



- ["Como configurar a autenticação de cartão de acesso comum \(CAC\) para o OnCommand Insight"](#)
- ["Como configurar a autenticação de cartão de acesso comum \(CAC\) para o armazém de dados OnCommand Insight"](#)
- ["Como criar e importar um certificado assinado pela autoridade de certificação \(CA\) para o OnCommand Insight e o Data Warehouse 7,3.x do OnCommand Insight"](#)
- ["Como criar um certificado autoassinado no OnCommand Insight 7,3.X instalado em um host Windows"](#)
- ["Como importar um certificado assinado pela autoridade de certificação \(CA\) do Cognos para o datawarehouse 7.3.3 e posterior do OnCommand"](#)

## Passos

1. Use `regedit` para modificar os valores do Registro em  
`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun2.0\SANscreen Server\Parameters\Java`
  - a. Altere a opção `JVM_Option -DclientAuth=false` para `-DclientAuth=true`.

Para Linux, modifique o `clientAuth` parâmetro em `/opt/netapp/oci/scripts/wildfly.server`

2. Adicione autoridades de certificação (CAs) ao armazenamento de dados:

- a. Em uma janela de comando, vá para `..\SANscreen\wildfly\standalone\configuration`.
- b. Use o `keytool` utilitário para listar as CAs confiáveis: `C:\Program Files\SANscreen\java64\bin\keytool.exe -list -keystore server.trustore -storepass <password>` Consulte "[SecurityAdmin](#)" a documentação para obter mais informações sobre como definir ou alterar a senha para `Server_trustore`.

A primeira palavra em cada linha indica o alias da CA.

- c. Se necessário, forneça um arquivo de certificado da CA, geralmente um `.pem` arquivo. Para incluir as CAs do cliente com as CAs confiáveis do Data Warehouse, vá para `..\SANscreen\wildfly\standalone\configuration` e use o `keytool` comando de importação: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore server.trustore -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

`My_alias` é geralmente um alias que identificaria facilmente a CA na `keytool -list` operação.

3. No servidor OnCommand Insight, o `wildfly/standalone/configuration/standalone-full.xml` arquivo precisa ser modificado atualizando `Verify-client` para "REQUESTED" em `/subsystem=undertow/server=default-server/https-listener=default-https` para ativar CAC. Faça login no servidor Insight e execute o comando apropriado:

SO	Script
Windows	<code>&lt;install dir&gt;/SANscreen/wildfly/bin/enableCACforRemoteEJB.bat</code>
Linux	<code>/Opt/NetApp/oci/wildfly/bin/enableCACforRemoteEJB.sh</code>

Depois de executar o script, aguarde até que a recarga do servidor Wildfly esteja concluída antes de prosseguir para a próxima etapa.

4. Reinicie o servidor OnCommand Insight.

## Configurando o Cognos para login de cartão inteligente e certificado (OnCommand Insight 7.3.10 e posterior)

Você deve modificar a configuração do Armazém de dados do OnCommand Insight para oferecer suporte a logins de cartão inteligente (CAC) e certificado para o servidor Cognos.

### Antes de começar

Este procedimento destina-se a sistemas que executam o OnCommand Insight 7.3.10 e posterior.



Para obter as instruções de CAC e certificado mais atualizadas, consulte os seguintes artigos da base de conhecimento (login de suporte necessário):



- ["Como configurar a autenticação de cartão de acesso comum \(CAC\) para o OnCommand Insight"](#)
- ["Como configurar a autenticação de cartão de acesso comum \(CAC\) para o armazém de dados OnCommand Insight"](#)
- ["Como criar e importar um certificado assinado pela autoridade de certificação \(CA\) para o OnCommand Insight e o Data Warehouse 7,3.x do OnCommand Insight"](#)
- ["Como criar um certificado autoassinado no OnCommand Insight 7,3.X instalado em um host Windows"](#)
- ["Como importar um certificado assinado pela autoridade de certificação \(CA\) do Cognos para o datawarehouse 7.3.3 e posterior do OnCommand"](#)

## Passos

1. Adicione autoridades de certificação (CAs) à loja Cognos trustore.

a. Em uma janela de comando, vá para

```
..\SANSscreen\cognos\analytics\configuration\certs\
```

b. Use o `keytool` utilitário para listar as CAs confiáveis: "...". `keytool.exe -list -keystore CAMKeystore.jks -storepass <password>`

A primeira palavra em cada linha indica o alias da CA.

c. Se não existirem ficheiros adequados, forneça um ficheiro de certificado de CA, normalmente um `.pem` ficheiro.

d. Para incluir as CAs do cliente com as CAs confiáveis do OnCommand Insight, vá para

```
..\SANSscreen\cognos\analytics\configuration\certs\.
```

e. Use o `keytool` utilitário para importar o `.pem` arquivo: `..\..\ibm-jre\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

`my_alias` Geralmente é um alias que identificaria facilmente a CA na `keytool -list` operação.

f. Quando for solicitada uma senha, insira a senha do arquivo `/SANSscreen/bin/cognos_info.dat`.

g. Responda `yes` quando solicitado a confiar no certificado.

2. Para ativar o modo CAC, faça o seguinte:

a. Configure a página de logout do CAC, seguindo as seguintes etapas:

- Logon no portal Cognos (o usuário deve fazer parte do grupo Administradores do sistema, ou seja, `cognos_admin`)
- (Apenas para 7.3.10 e 7,3.11) clique em Gerenciar → Configuração → sistema → Segurança
- (Apenas para 7.3.10 e 7,3.11) Introduza `cacLogout.html` contra a URL Redirect Logout
- Feche o navegador.

b. Executar `..\SANSscreen\bin\cognos_cac\enableCognosCAC.bat`

c. Inicie o serviço IBM Cognos. Aguarde que o serviço Cognos seja iniciado.

3. Para desativar o modo CAC, faça o seguinte:

- a. Executar `..\SANSscreen\bin\cognos_cac\disableCognosCAC.bat`
- b. Inicie o serviço IBM Cognos. Aguarde que o serviço Cognos seja iniciado.
- c. (Apenas para 7.3.10 e 7,3.11) Desconfigure a página de logout do CAC, seguindo os seguintes passos:
  - Logon no portal Cognos (o usuário deve fazer parte do grupo Administradores do sistema, ou seja, cognos\_admin)
  - Clique em Gerenciar "→ Configuração "→ sistema "→ Segurança
  - Digite cacLogout.html contra o URL de redirecionamento de logout '→ aplicar
  - Feche o navegador.

## Importação de certificados SSL assinados pela CA para Cognos e DWH (Insight 7.3.10 e posterior)

Você pode adicionar certificados SSL para habilitar autenticação e criptografia aprimoradas para seu ambiente Data Warehouse e Cognos.

### Antes de começar

Este procedimento destina-se a sistemas que executam o OnCommand Insight 7.3.10 e posterior.

Para obter as instruções de CAC e certificado mais atualizadas, consulte os seguintes artigos da base de conhecimento (login de suporte necessário):



- ["Como configurar a autenticação de cartão de acesso comum \(CAC\) para o OnCommand Insight"](#)
- ["Como configurar a autenticação de cartão de acesso comum \(CAC\) para o armazém de dados OnCommand Insight"](#)
- ["Como criar e importar um certificado assinado pela autoridade de certificação \(CA\) para o OnComand Insight e o Data Warehouse 7,3.x do OnCommand Insight"](#)
- ["Como criar um certificado autoassinado no OnCommand Insight 7,3.X instalado em um host Windows"](#)
- ["Como importar um certificado assinado pela autoridade de certificação \(CA\) do Cognos para o datawarehouse 7.3.3 e posterior do OnCommand"](#)

### Sobre esta tarefa

Tem de ter admin Privileges para executar este procedimento.

### Passos

1. Pare o Cognos usando a ferramenta IBM Cognos Configuration. Feche o Cognos.
2. Crie cópias de segurança das `..\SANSscreen\cognos\analytics\configuration` pastas e `..\SANSscreen\cognos\analytics\temp\cam\freshness`
3. Gerar uma solicitação de criptografia de certificado do Cognos. Em uma janela Admin CMD, execute:
  - a. `cd "\Program Files\sansscreen\cognos\analytics\bin"`

- b. `ThirdPartyCertificateTool.bat -java:local -c -e -p <password> -a RSA -r c:\temp\encryptRequest.csr -d "CN=server.domain.com,O=NETAPP,C=US" -H "server.domain.com" -I "ipaddress"`. Nota: Aqui -H e -I são para adicionar subjetivAltNames como dns e ipaddress.
  - c. Para <password>, use a senha do arquivo `/SANscreen/bin/cognos_info.dat`.
4. Abra o `c:\temp\encryptRequest.csr` arquivo e copie o conteúdo gerado.
5. Insira o conteúdo `cryptRequest.csr` e gere o certificado usando o portal de assinatura CA.
6. Faça o download dos certificados em cadeia incluindo o certificado raiz usando o formato PKCS7  

Isso fará o download do arquivo `fqdn.p7b`
7. Obtenha um cert no formato `.p7b` da sua CA. Use um nome que o marque como o certificado para o servidor Web do Cognos.
8. O `ThirdPartyCertificateTool.bat` não importa toda a cadeia, portanto são necessárias várias etapas para exportar todos os certificados. Divida a cadeia exportando-as individualmente da seguinte forma:
  - a. Abra o certificado `.p7b` em "Crypto Shell Extensions".
  - b. Navegue no painel esquerdo para ""certificados"".
  - c. Clique com o botão direito do rato em CA raiz > todas as tarefas > Exportar.
  - d. Selecione Base64 saída.
  - e. Insira um nome de arquivo identificando-o como o certificado raiz.
  - f. Repita as etapas 8a a 8e para exportar todos os certificados separadamente para arquivos `.cer`.
  - g. Nomeie os arquivos `intermediateX.cer` e `cognos.cer`.
9. Ignore esta etapa se você tiver apenas um certificado de CA, caso contrário, mesclar `root.cer` e `intermediateX.cer` em um arquivo.
  - a. Abra o `root.cer` com o bloco de notas e copie o conteúdo.
  - b. Abra o `Intermediate.cer` com o bloco de notas e anexe o conteúdo do 9a (intermediário primeiro e raiz seguinte).
  - c. Salve o arquivo como `chain.cer`.
10. Importe os certificados para o keystore do Cognos usando o prompt Admin CMD:
  - a. `cd "arquivos de programas" SANscreen`
  - b. `ThirdPartyCertificateTool.bat -Java:local -i -T -r c: /Temp/root.cer`
  - c. `ThirdPartyCertificateTool.bat -Java:local -i -T -r c: /Temp/intermediate.cer`
  - d. `ThirdPartyCertificateTool.bat -Java:local -i -e -r c`
11. Abra a configuração do IBM Cognos.
  - a. Selecione Configuração local → Segurança → criptografia → Cognos
  - b. Altere "usar CA de terceiros?" para verdadeiro.
  - c. Salve a configuração.
  - d. Reinicie o Cognos
12. Exporte o certificado Cognos mais recente para o `cognos.crt` usando o prompt Admin CMD:
  - a. `cd "C: Arquivos de programas" SANscreen`

- b. `-Storetype PKCS12 -storepass <password> -alias Encryption keytool.exe`
  - c. Para `<password>`, use a senha do arquivo `/SANscreen/bin/cognos_info.dat`.
13. Faça uma cópia de segurança da trustore do servidor DWH  
`em..\SANscreen\wildfly\standalone\configuration\server.trustore`
  14. Importe o arquivo "c: cognos.crt" para o repositório DWH para estabelecer uma comunicação SSL entre o Cognos e o DWH, usando a janela de prompt do Admin CMD.
    - a. `cd "C: Arquivos de programas" SANscreen`
    - b. `keytool.exe -importcert -file c: /temp/cognos.crt -keystore wildfly/standalone/configuration/server.trustore -storepass <password> -alias cognos3rdca`
    - c. Para `<password>`, use a senha do arquivo `/SANscreen/bin/cognos_info.dat`.
  15. Reinicie o serviço SANscreen.
  16. Execute um backup da DWH para garantir que a DWH se comunique com o Cognos.
  17. As etapas a seguir devem ser executadas mesmo quando apenas o "certificado ssl" é alterado e os certificados padrão do Cognos são mantidos inalterados. Caso contrário, a Cognos pode reclamar do novo certificado SANscreen ou não conseguir criar um backup DWH.
    - a. `cd "%SANSCREEN_HOME%cognos\analytics\bin\"`
    - b. `"%SANSCREEN_HOME%java64\bin\keytool.exe" -exportcert -file "c:\temp\sanscreen.cer" -keystore "%SANSCREEN_HOME%wildfly\standalone\configuration\server.keystore" -storepass <password> -alias "ssl certificate"`
    - c. `ThirdPartyCertificateTool.bat -java:local -i -T -r "c:\temp\sanscreen.cer"`

Normalmente, essas etapas são executadas como parte do processo de importação de certificados Cognos descrito em ["Como importar um certificado assinado pela autoridade de certificação \(CA\) do Cognos para o datawarehouse 7.3.3 e posterior do OnCommand"](#)

## Importando certificados SSL

Você pode adicionar certificados SSL para habilitar autenticação e criptografia aprimoradas para melhorar a segurança do seu ambiente OnCommand Insight.

### Antes de começar

Você deve garantir que seu sistema atenda ao nível mínimo de bits necessário (1024 bits).

### Sobre esta tarefa



É altamente recomendável fazer backup do Vault antes de atualizar.

Consulte ["Ferramenta SecurityAdmin"](#) as instruções para obter mais informações sobre o Vault e o gerenciamento de senhas.

### Passos

1. Crie uma cópia do arquivo keystore original: `cp c:\Program`

```
Files\SANscreen\wildfly\standalone\configuration\server.keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore.old
```

2. Listar o conteúdo do keystore: `C:\Program Files\SANscreen\java64\bin\keytool.exe -list -v -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore"`

O sistema exibe o conteúdo do keystore. Deve haver pelo menos um certificado no keystore, "ssl certificate".

3. Eliminar o "ssl certificate": `keytool -delete -alias "ssl certificate" -keystore c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
4. Gerar uma nova chave: `C:\Program Files\SANscreen\java64\bin\keytool.exe -genkey -alias "ssl certificate" -keyalg RSA -keysize 2048 -validity 365 -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore"`
  - a. Quando solicitado o nome e sobrenome, insira o nome de domínio totalmente qualificado (FQDN) que você pretende usar.
  - b. Forneça as seguintes informações sobre sua organização e estrutura organizacional:
    - País: Abreviatura ISO de duas letras para o seu país (por exemplo, EUA)
    - Estado ou Província: Nome do estado ou província onde a sede da sua organização está localizada (por exemplo, Massachusetts)
    - Localidade: Nome da cidade onde está localizada a sede da sua organização (por exemplo, Waltham)
    - Nome da organização: Nome da organização que possui o nome de domínio (por exemplo, NetApp)
    - Nome da unidade organizacional: Nome do departamento ou grupo que usará o certificado (por exemplo, suporte)
    - Nome do domínio/ Nome comum: O FQDN usado para pesquisas DNS do seu servidor (por exemplo, www.example.com) o sistema responde com informações semelhantes às seguintes: `Is CN=www.example.com, OU=support, O=NetApp, L=Waltham, ST=MA, C=US correct?`
  - c. Digite Yes quando o Nome Comum (CN) for igual ao FQDN.
  - d. Quando for solicitada a senha da chave, digite a senha ou pressione a tecla Enter para usar a senha existente do keystore.

5. Gerar um arquivo de solicitação de certificado: `C:\Program Files\SANscreen\java64\bin\keytool.exe -certreq -alias "ssl certificate" -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -file c:\localhost.csr`

O `c:\localhost.csr` arquivo é o arquivo de solicitação de certificado que foi gerado recentemente.

6. Envie o `c:\localhost.csr` arquivo à autoridade de certificação (CA) para aprovação.

Uma vez que o arquivo de solicitação de certificado seja aprovado, você deseja que o certificado seja devolvido em `.der` formato. O arquivo pode ou não ser retornado como um `.der` arquivo. O formato de arquivo padrão é `.cer` para os serviços Microsoft CA.

As CAs da maioria das organizações usam um modelo de cadeia de confiança, incluindo uma CA raiz,

que muitas vezes está offline. Ele assinou os certificados para apenas algumas CAs filhas, conhecidas como CAs intermediárias.

Você deve obter a chave pública (certificados) para toda a cadeia de confiança - o certificado da CA que assinou o certificado para o servidor OnCommand Insight e todos os certificados entre essa CA de assinatura até a CA raiz organizacional, inclusive.

Em algumas organizações, ao enviar uma solicitação de assinatura, você pode receber uma das seguintes opções:

- Um arquivo PKCS12 que contém seu certificado assinado e todos os certificados públicos na cadeia de confiança
- Um .zip arquivo que contém arquivos individuais (incluindo seu certificado assinado) e todos os certificados públicos na cadeia de confiança
- Apenas o seu certificado assinado

Você deve obter os certificados públicos.

7. Importe o certificado aprovado para Server.keystore: C:\Program

```
Files\SANscreen\java64\bin\keytool.exe -importcert -alias OCI.hostname.com
-file c:\localhost2.DER -keystore "c:\Program
Files\SANscreen\wildfly\standalone\configuration\server.keystore"
```

- a. Quando solicitado, insira a senha do keystore.

É apresentada a seguinte mensagem: Certificate reply was installed in keystore

8. Importar o certificado aprovado para Server.trustore: C:\Program

```
Files\SANscreen\java64\bin\keytool.exe -importcert -alias OCI.hostname.com
-file c:\localhost2.DER -keystore "c:\Program
Files\SANscreen\wildfly\standalone\configuration\server.trustore"
```

- a. Quando solicitado, introduza a palavra-passe do armazenamento de dados.

É apresentada a seguinte mensagem: Certificate reply was installed in trustore

9. Edite o SANscreen\wildfly\standalone\configuration\standalone-full.xml arquivo:

Substitua a seguinte cadeia de caracteres alias alias="cbc-oci-02.muccbc.hq.netapp.com":. Por exemplo:

```
<keystore path="server.keystore" relative-to="jboss.server.config.dir"
keystore-password="{VAULT::HttpsRealm::keystore_password::1}" alias="cbc-oci-
02.muccbc.hq.netapp.com" key-
password="{VAULT::HttpsRealm::key_password::1}"/>
```

10. Reinicie o serviço do servidor SANscreen.

Quando o Insight estiver em execução, você pode clicar no ícone de cadeado para exibir os certificados instalados no sistema.

Se você vir um certificado contendo informações "emitidas para" que correspondam às informações "emitidas por", você ainda terá um certificado autoassinado instalado. Os certificados autoassinados gerados pelo instalador do Insight têm uma expiração de 100 anos.

A NetApp não pode garantir que este procedimento irá remover avisos de certificado digital. O NetApp não pode controlar como as estações de trabalho do usuário final são configuradas. Considere os seguintes cenários:

- O Microsoft Internet Explorer e o Google Chrome utilizam a funcionalidade de certificado nativo da Microsoft no Windows.

Isso significa que, se os administradores do Active Directory enviarem os certificados de CA da sua organização para os trustores de certificados do usuário final, os usuários desses navegadores verão os avisos de certificado desaparecerem quando os certificados autoassinados do OnCommand Insight forem substituídos pelo certificado assinado pela infra-estrutura interna da CA.

- Java e Mozilla Firefox têm suas próprias lojas de certificados.

Se os administradores do sistema não automatizarem a ingestão dos certificados CA nos armazenamentos de certificados confiáveis desses aplicativos, o uso do navegador Firefox pode continuar gerando avisos de certificado por causa de um certificado não confiável, mesmo quando o certificado autoassinado foi substituído. Obter a cadeia de certificados da sua organização instalada no trustore é um requisito adicional.

## Configuração de backups semanais para seu banco de dados Insight

Você pode querer configurar backups semanais automáticos para seu banco de dados Insight para proteger seus dados. Esses backups automáticos substituem os arquivos no diretório de backup especificado.

### Sobre esta tarefa

**Prática recomendada:** Quando você está configurando o backup semanal do banco de dados OCI, você precisa armazenar os backups em um servidor diferente do que o Insight está usando, caso esse servidor falhe. Não armazene backups manuais no diretório de backup semanal, pois cada backup semanal substitui os arquivos no diretório.

O arquivo de backup conterá o seguinte:

- Dados de inventário
- Até 7 dias de dados de performance

### Passos

1. Na barra de ferramentas Insight, clique em **Admin > Setup**.
2. Clique no separador **Backup & Archive** (cópia de segurança e arquivo).
3. Na seção Backup semanal, selecione **Ativar backup semanal**.
4. Introduza o caminho para o **local de cópia de segurança**. Isso pode estar no no servidor Insight local ou em um servidor remoto acessível a partir do servidor Insight.



A configuração do local de backup está incluída no próprio backup, portanto, se você restaurar o backup em outro sistema, esteja ciente de que o local da pasta de backup pode ser inválido no novo sistema. Verifique duas vezes as definições de local de cópia de segurança depois de restaurar uma cópia de segurança.

5. Selecione a opção **Limpeza** para manter os dois últimos ou os cinco últimos backups.
6. Clique em **Salvar**.

## Resultados

Você também pode ir para **Admin > Troubleshooting** para criar um backup sob demanda.

## O que está incluído no backup

Backups semanais e sob demanda podem ser usados para solução de problemas ou migração.

O backup semanal ou sob demanda inclui o seguinte:

- Dados de inventário
- Dados de desempenho (se selecionados para inclusão no backup)
- Fontes de dados e configurações de fonte de dados
- Pacotes de integração
- Unidades de aquisição remota
- Configurações ASUP/proxy
- Definições de localização de cópia de segurança
- Definições de localização de arquivo
- Definições de notificação
- Usuários
- Políticas de performance
- Entidades e aplicações empresariais
- Regras e definições de resolução do dispositivo
- Painéis e widgets
- Painéis e widgets de página de ativos personalizados
- Consultas
- Anotações e regras de anotação

O backup semanal não inclui:

- Configurações da ferramenta de segurança / informações do Vault (backup via processo CLI separado)
- Logs (podem ser salvos em um arquivo .zip sob demanda)
- Dados de desempenho (se não forem selecionados para inclusão no backup)
- Licenças





Se você optar por incluir dados de desempenho no backup, o backup dos últimos sete dias de dados será feito. Os dados restantes estarão no arquivo se você tiver esse recurso ativado.

## Arquivamento de dados de desempenho

O OnCommand Insight 7,3 apresenta a capacidade de arquivar dados de performance diariamente. Isso complementa a configuração e os backups de dados de desempenho limitado.

A OnCommand Insight retém até 90 dias de dados de desempenho e violação. No entanto, ao criar um backup desses dados, apenas as informações mais recentes são incluídas no backup. O arquivamento permite salvar o restante dos dados de desempenho e carregá-los conforme necessário.

Quando a localização do arquivo estiver configurada e o arquivamento estiver ativado, uma vez por dia o Insight arquivará os dados de desempenho do dia anterior para todos os objetos no local do arquivo. O arquivo de cada dia é mantido na pasta de arquivo em um arquivo separado. O arquivamento acontece em segundo plano e continuará enquanto o Insight estiver em execução.

Os 90 dias mais recentes de arquivos são retidos; arquivos de arquivo com mais de 90 dias são excluídos à medida que os mais novos são criados.

### Habilitando o arquivamento de desempenho

Para ativar o arquivamento de dados de desempenho, siga estes passos.

#### Passos

1. Na barra de ferramentas, clique em **Admin > Setup**.
2. Selecione o separador **Backup & Archive** (cópia de segurança e arquivo).
3. Na seção Arquivo de desempenho, verifique se a opção Ativar arquivo de desempenho\*\* está marcada.
4. Especifique uma localização de arquivo válida.

Não é possível especificar uma pasta na pasta de instalação do Insight.

Prática recomendada: Não especifique a mesma pasta para o arquivo que o local de backup do Insight.

5. Clique em **Salvar**.

O processo de arquivo é Tratado em segundo plano e não interfere com outras atividades do Insight.

### A carregar arquivo de performance

Para carregar o arquivo de dados de desempenho, siga estas etapas.

#### Antes de começar

Antes de carregar o arquivo de dados de desempenho, é necessário restaurar um backup semanal ou manual válido.

## Passos

1. Na barra de ferramentas, clique em **Admin > Troubleshooting**.
2. Na seção Restaurar, em **carregar arquivo de desempenho**, clique em **carregar**.



O carregamento do arquivo é Tratado em segundo plano. O carregamento do arquivo completo pode demorar muito tempo, pois os dados de desempenho arquivados de cada dia são preenchidos no Insight. O estado do carregamento do arquivo é apresentado na seção de arquivo desta página.

## Configurando seu e-mail

Você precisa configurar o OnCommand Insight para acessar o sistema de e-mail para que o OnCommand Insight Server possa usar seu e-mail para fornecer relatórios, aos quais você assina e transportar informações de suporte para solução de problemas para o suporte técnico da NetApp.

### Pré-requisitos de configuração de e-mail

Antes de configurar o OnCommand Insight para acessar seu sistema de e-mail, você precisa descobrir o nome do host ou o endereço IP para identificar o servidor de e-mail (SMTP ou Exchange) e alocar uma conta de e-mail para relatórios do OnCommand Insight.

Peça ao administrador de e-mail para criar uma conta de e-mail para o OnCommand Insight. Você precisará das seguintes informações:

- O nome do host ou o endereço IP para identificar o servidor de e-mail (SMTP ou Exchange) usado pela sua organização. Você pode encontrar essas informações através do aplicativo que você usa para ler seu e-mail. No Microsoft Outlook, por exemplo, você pode encontrar o nome do servidor exibindo a configuração da sua conta: Ferramentas - Contas de e-mail - Exibir ou alterar a conta de e-mail existente.
- Nome da conta de e-mail através da qual o OnCommand Insight enviará relatórios regulares. A conta deve ser um endereço de e-mail válido na sua organização. (A maioria dos sistemas de e-mail não enviará mensagens a menos que sejam enviadas de um usuário válido.) Se o servidor de e-mail precisar de um nome de usuário e senha para enviar e-mails, obtenha essas informações do administrador do sistema.

### Configurando seu e-mail para o Insight

Se os usuários quiserem receber relatórios do Insight em suas contas de e-mail, você precisará configurar o servidor de e-mail para habilitar esse recurso.

## Passos

1. Na barra de ferramentas Insight, clique em **Admin** e selecione **notificações**.
2. Role para baixo até a seção **Email** da página.
3. Na caixa **Server**, insira o nome do servidor SMTP na sua organização, que é identificado usando um nome de host ou um endereço IP (*nnn.nnn.nnn.nnn* format).

Se você especificar um nome de host, verifique se o nome pode ser resolvido através do DNS.

4. Na caixa **Nome de utilizador**, introduza o seu nome de utilizador.
5. Na caixa **Senha**, insira a senha para acessar o servidor de e-mail, que é necessária somente se o servidor SMTP estiver protegido por senha. Esta é a mesma senha que você usa para fazer login no aplicativo que permite ler seu e-mail. Se for necessária uma palavra-passe, tem de a introduzir uma segunda vez para verificação.
6. Na caixa **e-mail do remetente**, insira a conta de e-mail do remetente que será identificada como remetente em todos os relatórios do OnCommand Insight.

Esta conta deve ser uma conta de e-mail válida dentro da sua organização.

7. Na caixa **assinatura de e-mail**, insira o texto que deseja inserir em cada e-mail enviado.
8. Na caixa destinatários, clique **+em** , insira um endereço de e-mail e clique em **OK**.

Para editar um endereço de e-mail, selecione o endereço e clique **✎em** . Para excluir um endereço de e-mail, selecione o endereço e clique **✕em** .

9. Para enviar um e-mail de teste para destinatários especificados, clique **✓em** .
10. Clique em **Salvar**.

## Configurar notificações SNMP

O OnCommand Insight suporta notificações SNMP para alterações de configuração e de política de caminho global, bem como violações. Por exemplo, as notificações SNMP são enviadas quando os limites da fonte de dados são excedidos.

### Antes de começar

O seguinte deve ter sido concluído:

- Identificar o endereço IP do servidor que consolida traps para cada tipo de evento.

Poderá ter de consultar o administrador do sistema para obter esta informação.

- Identificar o número da porta através da qual a máquina designada obtém traps SNMP, para cada tipo de evento.

A porta padrão para traps SNMP é 162.

- Compilando o MIB em seu site.

O MIB proprietário vem com o software de instalação para suportar OnCommand Insight traps. O MIB NetApp é compatível com todos os softwares de gerenciamento SNMP padrão e pode ser encontrado no servidor Insight em `<install_dir>\SANscreen\MIBS\sanscreen.mib`.

### Passos

1. Clique em **Admin** e selecione **notificações**.
2. Role para baixo até a seção **SNMP** da página.

3. Clique em **ações** e selecione **Adicionar fonte de armadilha**.
4. Na caixa de diálogo **Adicionar destinatários de trap SNMP**, insira estes valores:

- **IP**

O endereço IP para o qual o OnCommand Insight envia mensagens de intercetção SNMP.

- **Porto**

O número da porta para a qual o OnCommand Insight envia mensagens de intercetção SNMP.

- \* String da Comunidade\*

Use "public" para mensagens de intercetção SNMP.

5. Clique em **Salvar**.

## Habilitando o recurso syslog

Você pode identificar um local para o log das violações do OnCommand Insight e alertas de desempenho, bem como mensagens de auditoria e ativar o processo de log.

### Antes de começar

- Você deve ter o endereço IP do servidor no qual armazenar o log do sistema.
- Você deve saber o nível de instalação que corresponde ao tipo de programa que está registrando a mensagem, como LOCAL1 ou USUÁRIO.

### Sobre esta tarefa

O syslog inclui os seguintes tipos de informações:

- Mensagens de violação
- Alertas de performance
- Opcionalmente, auditar mensagens de log

As seguintes unidades são usadas no syslog:

- Métricas de utilização: Porcentagem
- Métricas de tráfego: MB
- Taxa de tráfego: MB/s

### Passos

1. Na barra de ferramentas Insight, clique em **Admin** e selecione **notificações**.
2. Role para baixo até a seção **Syslog** da página.
3. Marque a caixa de seleção **Ativar syslog**.
4. Se desejar, marque a caixa de seleção **Send audit** (Enviar auditoria\*). Novas mensagens de log de auditoria serão enviadas para o syslog, além de serem exibidas na página Auditoria. Observe que as mensagens de log de auditoria já existentes não serão enviadas para o syslog; somente as mensagens de

log recém-geradas serão enviadas.

5. No campo **Server**, insira o endereço IP do servidor de log.

Você pode especificar uma porta personalizada anexando-a após dois pontos no final do IP do servidor (por exemplo, servidor:porta). Se a porta não for especificada, a porta syslog padrão do 514 será usada.

6. No campo **Facility**, selecione o nível de instalação que corresponde ao tipo de programa que está a registrar a mensagem.

7. Clique em **Salvar**.

## Conteúdo do syslog Insight

Você pode habilitar um syslog em um servidor para coletar mensagens de violação do Insight e alerta de desempenho que incluem dados de utilização e tráfego.

### Tipos de mensagens

O syslog Insight lista três tipos de mensagens:

- Violações do caminho DE SAN
- Violações gerais
- Alertas de performance

### Dados fornecidos

As descrições de violação incluem os elementos envolvidos, a hora do evento e a gravidade relativa ou prioridade da violação.

Os alertas de performance incluem esses dados:

- Porcentagens de utilização
- Tipos de tráfego
- Taxa de tráfego medida em MB

## Configurando o desempenho e garanta notificações de violação

O OnCommand Insight oferece suporte a notificações de desempenho e garante violações. Por padrão, o Insight não envia notificações para essas violações; você deve configurar o Insight para enviar e-mails, para enviar mensagens syslog para o servidor syslog ou para enviar notificações SNMP quando ocorrer uma violação.

### Antes de começar

Você deve ter configurado métodos de envio de e-mail, syslog e SNMP para violações.

## Passos

1. Clique em **Admin > notificações**.
2. Clique em **Eventos**.
3. Na seção **Eventos de violações de desempenho** ou **garantir eventos de violações**, clique na lista do método de notificação (**Email**, **Syslog** ou **SNMP**) desejado e selecione o nível de gravidade (**Aviso e acima** ou **crítico**) para a violação.
4. Clique em **Salvar**.

## Configurando notificações de eventos no nível do sistema

O OnCommand Insight suporta notificações para eventos no nível do sistema, como falhas de unidade de aquisição ou erros de origem de dados. Para receber notificações, você deve configurar o Insight para enviar e-mails quando um ou mais desses eventos ocorrerem.

### Antes de começar

Você deve ter configurado destinatários de e-mail para receber notificações em **Admin > notificações > métodos de envio**.

## Passos

1. Clique em **Admin > notificações**.
2. Clique em **Eventos**.
3. Na seção **Eventos de Alerta do sistema e-mail**, selecione o nível de gravidade (**Aviso e acima** ou **crítico**) para a notificação ou escolha **não enviar** se você não quiser receber notificações de eventos no nível do sistema.
4. Clique em **Salvar**.
5. Clique em **Admin > Alertas do sistema** para configurar os próprios alertas.
6. Para adicionar um novo alerta, clique em \*Adicionar\* e dê ao alerta um **Nome** exclusivo. Você também pode clicar no ícone do lado direito para **Editar** um alerta existente.
7. Escolha o **tipo de evento** no qual alertar, por exemplo *Falha da Unidade de aquisição*.
8. Escolha um intervalo **Snooze** para suprimir notificações sobre eventos duplicados do tipo selecionado para o intervalo de tempo selecionado. Se você selecionar *nunca*, receberá notificações repetidas uma vez por minuto até que o evento não esteja mais acontecendo.
9. Escolha um **severidade** (Aviso ou Crítica) para a notificação de evento.
10. As notificações por e-mail serão enviadas para a lista global de destinatários de e-mail por padrão ou você pode clicar no link fornecido para substituir a lista global e enviar notificações para destinatários específicos.
11. Clique em **Salvar** para adicionar o alerta.

## Configurando o processamento ASUP

Todos os produtos NetApp são equipados com recursos automatizados para fornecer o

melhor suporte possível aos clientes. O suporte automatizado (ASUP) envia periodicamente informações predefinidas e específicas para o suporte ao Cliente. Você pode controlar as informações a serem encaminhadas para o NetApp e com que frequência elas são enviadas.

## Antes de começar

Você deve configurar o OnCommand Insight para encaminhar dados antes que quaisquer dados sejam enviados.

## Sobre esta tarefa

Os dados ASUP são encaminhados usando o protocolo HTTPS.

## Passos

1. Na barra de ferramentas Insight, clique em **Admin**.
2. Clique em **Configuração**.
3. Clique na guia **ASUP e Proxy**.
4. Na seção **ASUP**, selecione **Ativar ASUP** para ativar a instalação ASUP.
5. Se você quiser alterar suas informações corporativas, atualize os seguintes campos:
  - **Nome da empresa**
  - **Nome do site**
  - **O que enviar**: Logs, dados de configuração, dados de desempenho
6. Clique em **Test Connection** para garantir que a conexão especificada funcione.
7. Clique em **Salvar**.
8. Na seção **Proxy**, escolha se deseja **Ativar Proxy** e especifique suas informações proxy **host**, **port** e **user**.
9. Clique em **Test Connection** para garantir que o proxy especificado funcione.
10. Clique em **Salvar**.

## O que está incluído no pacote AutoSupport (ASUP)

O pacote AutoSupport contém o backup do banco de dados, bem como informações estendidas.

O pacote AutoSupport inclui o seguinte:

- Dados de inventário
- Dados de performance (se selecionados para inclusão no ASUP)
- Fontes de dados e configurações de fonte de dados
- Pacotes de integração
- Unidades de aquisição remota
- Configurações ASUP/proxy
- Definições de localização de cópia de segurança

- Definições de localização de arquivo
- Definições de notificação
- Usuários
- Políticas de performance
- Entidades e aplicações empresariais
- Regras e definições de resolução do dispositivo
- Painéis e widgets
- Painéis e widgets de página de ativos personalizados
- Consultas
- Anotações e regras de anotação
- Registos
- Licenças
- Estado da aquisição/fonte de dados
- Status do MySQL
- Informações do sistema

O pacote AutoSupport não inclui:

- Configurações da ferramenta de segurança / informações do Vault (backup via processo CLI separado)
- Dados de performance (se não forem selecionados para inclusão no ASUP)



Se você optar por incluir dados de performance no ASUP, os últimos sete dias de dados serão incluídos. Os dados restantes estarão no arquivo se você tiver esse recurso ativado. Os dados de arquivamento não estão incluídos no ASUP.

## Definindo aplicativos

Se quiser rastrear dados associados a aplicativos específicos em execução no ambiente, é necessário definir esses aplicativos.

### Antes de começar

Se você quiser associar o aplicativo a uma entidade de negócios, você já deve ter criado a entidade de negócios.

### Sobre esta tarefa

Você pode associar aplicativos aos seguintes ativos: Hosts, máquinas virtuais, volumes, volumes internos, qtrees, compartilhamentos e hipervisores.

### Passos

1. Faça login na IU da Web do OnCommand Insight.
2. Clique em **Gerenciar** e selecione **aplicativos**.



Depois de definir um aplicativo, a página aplicativos exibe o nome do aplicativo, sua prioridade e, se aplicável, a entidade comercial associada ao aplicativo.

3. Clique em **Add**.

A caixa de diálogo Adicionar aplicativo é exibida.

4. Insira um nome exclusivo para o aplicativo na caixa **Nome**.

5. Clique em **Priority** (prioridade) e selecione a prioridade (crítica, alta, média ou baixa) para a aplicação no seu ambiente.

6. Se você planeja usar este aplicativo com uma entidade de negócios, clique em **entidade de negócio** e selecione a entidade na lista.

7. **Opcional:** Se você não usar compartilhamento de volume, clique para desmarcar a caixa **Validar compartilhamento de volume**.

Isso requer a licença assure. Defina isso quando quiser garantir que cada host tenha acesso aos mesmos volumes em um cluster. Por exemplo, os hosts em clusters de alta disponibilidade geralmente precisam ser mascarados para os mesmos volumes para permitir o failover; no entanto, os hosts em aplicativos não relacionados geralmente não têm necessidade de acessar os mesmos volumes físicos. Além disso, as políticas regulatórias podem exigir que você impeça explicitamente que aplicativos não relacionados acessem os mesmos volumes físicos por motivos de segurança.

8. Clique em **Salvar**.

A aplicação é apresentada na página aplicações. Se você clicar no nome do aplicativo, o Insight exibirá a página de ativos do aplicativo.


## Depois de terminar

Depois de definir um aplicativo, você pode ir para uma página de ativos para host, máquina virtual, volume, volume interno ou hipervisor para atribuir um aplicativo a um ativo.

## Atribuindo aplicativos aos ativos

Depois de definir aplicativos com ou sem entidades de negócios, você pode associar os aplicativos aos ativos.

### Passos


1. Faça login na IU da Web do OnCommand Insight.
2. Localize o ativo (host, máquina virtual, volume ou volume interno) ao qual você deseja aplicar o aplicativo fazendo um dos seguintes procedimentos:
  - Clique em **Dashboard**, selecione **Assets Dashboard** e clique no ativo.
  - Clique **Q**-na barra de ferramentas para exibir a caixa **pesquisar ativos**, digite o nome do ativo e, em seguida, selecione o ativo na lista.
3. Na seção **dados do usuário** da página de ativo, posicione o cursor sobre o nome do aplicativo atualmente atribuído ao ativo (se não houver nenhum aplicativo atribuído, **nenhum** será exibido) e clique  em (Editar aplicativo).

A lista de aplicativos disponíveis para a exibição do ativo selecionado. As aplicações que estão

atualmente associadas ao ativo são precedidas por uma marca de verificação.

4. Você pode digitar na caixa pesquisar para filtrar os nomes dos aplicativos ou rolar a lista para baixo.
5. Selecione as aplicações que pretende associar ao ativo.

Você pode atribuir vários aplicativos ao host, à máquina virtual e ao volume interno; no entanto, você só pode atribuir um aplicativo ao volume.


6. Clique  para atribuir o aplicativo ou aplicativos selecionados ao ativo.

Os nomes dos aplicativos aparecem na seção dados do usuário; se o aplicativo estiver associado a uma entidade comercial, o nome da entidade comercial também aparecerá nesta seção.


## Editar aplicações

Talvez você queira alterar a prioridade de um aplicativo, a entidade de negócios associada a um aplicativo ou o status do compartilhamento de volume.

### Passos

1. Faça login na IU da Web do OnCommand Insight.
2. Clique em **Gerenciar** e selecione **aplicativos**.
3. Posicione o cursor sobre a aplicação que pretende editar e clique  em .

A caixa de diálogo Editar aplicativo é exibida.

4. Faça qualquer um dos seguintes procedimentos:
    - Clique em **Priority** e selecione uma prioridade diferente.
-  Não é possível alterar o nome da aplicação.
- Clique em **entidade de negócio** e selecione uma entidade de negócio diferente para associar o aplicativo ou selecione **nenhum** para remover a associação do aplicativo com a entidade de negócios.
  - Clique para limpar ou selecione **Validar compartilhamento de volume**.

 Esta opção só está disponível se você tiver a licença assure.


5. Clique em **Salvar**.

## Eliminar aplicações

Você pode querer excluir um aplicativo quando ele não atende mais a uma necessidade em seu ambiente.

### Passos

1. Faça login na IU da Web do Insight.
2. Clique em **Gerenciar** e selecione **aplicativos**.

3. Posicione o cursor sobre a aplicação que pretende eliminar e clique  em .

É apresentada uma caixa de diálogo de confirmação, perguntando se pretende eliminar a aplicação.

4. Clique em **OK**.

## Sua hierarquia de entidades empresariais

Você pode definir entidades de negócios para acompanhar e gerar relatórios sobre os dados do seu ambiente em um nível mais granular.

No OnCommand Insight, a hierarquia de entidades empresariais contém estes níveis:

- **O Locatário** é usado principalmente por provedores de serviços para associar recursos a um cliente, por exemplo, NetApp.
- **Linha de Negócios (LOB)** é uma linha de negócios ou linha de produtos dentro de uma empresa, por exemplo, armazenamento de dados.
- **Business Unit** representa uma unidade de negócio tradicional, como Legal ou Marketing.
- **Project** é frequentemente usado para identificar um projeto específico dentro de uma unidade de negócios para a qual você deseja estorno de capacidade. Por exemplo, "Patentes" pode ser um nome de projeto para a unidade de negócios jurídica e "Eventos de vendas" pode ser um nome de projeto para a unidade de negócios de Marketing. Observe que os nomes de nível podem incluir espaços.

Você não é obrigado a usar todos os níveis no design de sua hierarquia corporativa.

## Projetando sua hierarquia de entidades empresariais

Você precisa entender os elementos de sua estrutura corporativa e o que precisa ser representado nas entidades de negócios porque elas se tornam uma estrutura fixa em seu banco de dados OnCommand Insight. Você pode usar as seguintes informações para configurar suas entidades de negócios. Lembre-se de que você não precisa usar todos os níveis de hierarquia para coletar dados nessas categorias.

### Passos

1. Examine cada nível da hierarquia de entidades de negócios para determinar se esse nível deve ser incluído na hierarquia de entidades de negócios da sua empresa:
  - **O nível de Locatário** é necessário se a sua empresa for um ISP e você quiser rastrear o uso dos recursos do cliente.
  - **Linha de Negócios (LOB)** é necessária na hierarquia se os dados para diferentes linhas de produtos precisarem ser rastreados.
  - **Unidade de Negócios** é necessária se você precisar rastrear dados para diferentes departamentos. Esse nível da hierarquia é muitas vezes valioso na separação de um recurso que um departamento usa que outros departamentos não.
  - **Nível Projeto** pode ser usado para trabalho especializado dentro de um departamento. Esses dados podem ser úteis para identificar, definir e monitorar as necessidades de tecnologia de um projeto separado em comparação com outros projetos de uma empresa ou departamento.
2. Crie um gráfico mostrando cada entidade de negócio com os nomes de todos os níveis dentro da

entidade.

3. Verifique os nomes na hierarquia para ter certeza de que eles serão auto-explicativos nas visualizações e relatórios do OnCommand Insight.
4. Identificar todos os aplicativos associados a cada entidade de negócios.

## Criação de entidades empresariais

Depois de projetar a hierarquia de entidades de negócios para sua empresa, você pode configurar aplicativos e, em seguida, associar as entidades de negócios aos aplicativos. Esse processo cria a estrutura de entidades de negócios em seu banco de dados do OnCommand Insight.

### Sobre esta tarefa

Associar aplicativos a entidades de negócios é opcional; no entanto, é uma prática recomendada.

### Passos

1. Faça login na IU da Web do Insight.
2. Clique em **Gerenciar** e selecione **entidades empresariais**.

A página entidades empresariais é exibida.

3. Clique **+ Add** para começar a construir uma nova entidade.

A caixa de diálogo **Add Business Entity** é exibida.

4. Para cada nível de entidade (locatário, linha de negócio, Unidade de negócio e Projeto), você pode fazer qualquer um dos seguintes procedimentos:
  - Clique na lista nível de entidade e selecione um valor.
  - Digite um novo valor e pressione Enter.
  - Deixe o valor do nível da entidade como N/A se você não quiser usar o nível da entidade para a entidade de negócio.
5. Clique em **Salvar**.

## Atribuindo entidades de negócios a ativos

Você pode atribuir uma entidade de negócios a um ativo ( host, porta, armazenamento, switch, máquina virtual, qtree, compartilhamento, volume ou volume interno) sem ter associado a entidade de negócios a um aplicativo; no entanto, as entidades de negócios são atribuídas automaticamente a um ativo se esse ativo estiver associado a um aplicativo relacionado a uma entidade de negócios.



### Antes de começar

Você já deve ter criado uma entidade de negócios.

## Sobre esta tarefa

Embora você possa atribuir entidades de negócios diretamente aos ativos, é recomendável atribuir aplicativos a ativos e, em seguida, atribuir entidades de negócios a ativos.


## Passos

1. Faça login na IU da Web do OnCommand Insight.
2. Localize o ativo ao qual você deseja aplicar a entidade de negócios fazendo um dos seguintes procedimentos:
  - Clique no ativo no Painel de ativos.
  - Clique  na barra de ferramentas para exibir a caixa **pesquisar ativos**, digite o nome do ativo e, em seguida, selecione o ativo na lista.
3. Na seção **dados do usuário** da página de ativo, posicione o cursor sobre **nenhum** ao lado de **entidades empresariais** e clique  em .

A lista de entidades comerciais disponíveis é exibida.

4. Digite a caixa **pesquisar** para filtrar a lista de uma entidade específica ou rolar a lista para baixo; selecione uma entidade de negócio na lista.

Se a entidade comercial escolhida estiver associada a um aplicativo, o nome do aplicativo será exibido. Neste caso, a palavra "served" aparece ao lado do nome da entidade comercial. Se você quiser manter a entidade apenas para o ativo e não para o aplicativo associado, você pode substituir manualmente a atribuição do aplicativo.

5. Para substituir um aplicativo derivado de uma entidade de negócios, coloque o cursor sobre o nome do aplicativo e clique  em , selecione outra entidade de negócios e selecione outro aplicativo na lista.


## Atribuir entidades de negócios ou remover entidades de negócios de vários ativos

Você pode atribuir entidades de negócios ou remover entidades de negócios de vários ativos usando uma consulta em vez de ter que atribuí-las ou removê-las manualmente.

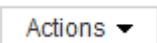
### Antes de começar

Você já deve ter criado as entidades de negócios que deseja adicionar aos ativos desejados.


## Passos

1. Crie uma nova consulta ou abra uma consulta existente.
2. Se desejado, filtre os ativos aos quais você deseja adicionar entidades de negócios.
3. Selecione os ativos desejados na lista ou clique   para selecionar **All**.

O botão **ações** é exibido.

4. Para adicionar uma entidade de negócio aos ativos selecionados, clique  em . Se o tipo de ativo selecionado puder ter entidades de negócio atribuídas a ele, você verá a opção de menu para **Adicionar entidade de negócio**. Selecione esta opção.
5. Selecione a entidade comercial desejada na lista e clique em **Salvar**.

Qualquer nova entidade de negócios que você atribua substitui todas as entidades de negócios que já foram atribuídas ao ativo. A atribuição de aplicativos a ativos também substituirá as entidades de negócios atribuídas da mesma maneira. A atribuição de entidades de negócios ao como ativo também pode substituir quaisquer aplicativos atribuídos a esse ativo.

6. Para remover uma entidade de negócio atribuída aos ativos, clique  e selecione **Remover entidade de negócio**.
7. Selecione a entidade comercial desejada na lista e clique em **Excluir**.

## Definir anotações

Ao personalizar o OnCommand Insight para controlar dados de acordo com seus requisitos empresariais, você pode definir quaisquer anotações especializadas necessárias para fornecer uma visão completa dos dados: Por exemplo, fim de vida útil do ativo, data center, local de criação, camada de storage ou volume e nível de serviço de volume interno.

### Passos

1. Liste qualquer terminologia do setor à qual os dados do ambiente devem ser associados.
2. Liste a terminologia corporativa à qual os dados do ambiente devem ser associados, o que ainda não está sendo rastreado usando as entidades de negócios.
3. Identifique quaisquer tipos de anotação padrão que você possa ser capaz de usar.
4. Identifique quais anotações personalizadas você precisa criar.

## Usando anotações para monitorar seu ambiente

Ao personalizar o OnCommand Insight para rastrear dados para seus requisitos corporativos, você pode definir notas especializadas, chamadas *anotações*, e atribuí-las aos seus ativos. Por exemplo, você pode anotar 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.
- Utilizar o utilitário de importação de anotações para importar anotações.
- Filtrar ativos por suas anotações.
- Agrupar dados em relatórios com base em anotações e gerar esses relatórios.

Consulte o *Guia de relatórios do OnCommand Insight* para obter mais informações sobre relatórios.

## Gerir tipos de anotação

O OnCommand Insight fornece alguns tipos de anotação padrão, como ciclo de vida do ativo (aniversário ou fim da vida útil), localização do prédio ou data center e nível, que você pode personalizar para mostrar em seus relatórios. Pode definir valores para tipos de anotação predefinidos ou criar os seus próprios tipos de anotação personalizados. Mais tarde, você pode editar esses valores.

### Tipos de anotação predefinidos

O OnCommandInsight fornece alguns tipos de anotação padrão. Essas anotações podem ser usadas para filtrar ou agrupar dados e filtrar relatórios de 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 seguinte lista os tipos de anotação predefinidos. Pode editar qualquer um destes nomes de anotação de acordo com as suas necessidades.

Tipos de anotação	Descrição	Tipo
Alias	Nome amigável para um recurso.	Texto
Aniversário	Data em que o dispositivo foi ou será colocado online.	Data
Edifício	Localização física dos recursos de host, armazenamento, switch e fita.	Lista
Cidade	Localização do município dos recursos de host, armazenamento, switch e fita.	Lista
Grupo de recursos de computação	Atribuição de grupo usada pela fonte de dados de sistemas de arquivos Host e VM.	Lista
Continente	Localização geográfica dos recursos de host, armazenamento, switch e fita.	Lista

País	Localização nacional dos recursos de host, armazenamento, switch e fita.	Lista
Data center	Localização física do recurso e está disponível para hosts, matrizes de armazenamento, switches e fitas.	Lista
Ligação direta	Indica (Sim ou não) se um recurso de armazenamento estiver conectado diretamente aos hosts.	Booleano
Fim da vida	Data em que um dispositivo será colocado off-line, por exemplo, se a concessão expirou ou o hardware estiver sendo retirado.	Data
Alias de tecido	Nome fácil de usar para um tecido.	Texto
Piso	Localização de um dispositivo em um piso de um edifício. Pode ser definido para hosts, matrizes de armazenamento, switches e fitas.	Lista
Quente	Dispositivos já em uso pesado regularmente ou no limite de capacidade.	Booleano
Nota	Comentários que você deseja associados a um recurso.	Texto
Rack	Rack no qual o recurso reside.	Texto
Quarto	Sala dentro de um prédio ou outro local de recursos de host, armazenamento, switch e fita.	Lista
SAN	Partição lógica da rede. Disponível em hosts, matrizes de armazenamento, fitas, switches e aplicativos.	Lista



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
Estado/Província	Estado ou província em que o recurso está localizado.	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	Inclui opções predefinidas para configurar categorias para switches. Normalmente, essas designações permanecem durante a vida útil do dispositivo, embora você possa editá-las, se necessário. 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, Service Level, Tier e violation Severity são anotações no nível do sistema, que você não pode excluir ou renomear; você pode alterar apenas os valores atribuídos.

## Como as anotações são atribuídas

Pode atribuir anotações manualmente ou automaticamente utilizando regras de anotação. O OnCommand Insight também atribui automaticamente algumas anotações na aquisição de ativos e por herança. Quaisquer anotações que você atribuir a um ativo aparecem na seção dados do usuário da página de ativo.

As anotações são atribuídas das seguintes formas:

- Pode atribuir uma anotação manualmente a um ativo.

Se uma anotação for atribuída diretamente a um ativo, a anotação aparece como texto normal numa página de ativo. As anotações que são atribuídas manualmente sempre têm precedência sobre anotações que são herdadas ou atribuídas por regras de anotação.

- Você pode criar uma regra de anotação para atribuir automaticamente anotações a ativos do mesmo tipo.

Se a anotação for atribuída por regra, o Insight exibirá o nome da regra ao lado do nome da anotação em uma página de ativo.

- O Insight associa automaticamente um nível de camada a um modelo de camada de storage para agilizar a atribuição de anotações de storage aos seus recursos na aquisição de ativos.

Certos recursos de storage são automaticamente associados a um nível predefinido (camada 1 e camada 2). Por exemplo, o nível de armazenamento Symmetrix é baseado na família Symmetrix e VMAX e está associado ao nível 1. Você pode alterar os valores padrão para atender aos requisitos de nível. Se a anotação for atribuída pelo Insight (por exemplo, Tier), você verá "System-Defined" quando posicionar o cursor sobre o nome da anotação em uma página de ativo.

- Alguns recursos (filhos de um ativo) podem derivar a anotação de nível predefinido do ativo (pai).

Por exemplo, se você atribuir uma anotação a um armazenamento, a anotação Tier será derivada de todos os pools de armazenamento, volumes internos, volumes, qtrees e compartilhamentos pertencentes ao armazenamento. Se uma anotação diferente for aplicada a um volume interno do armazenamento, a anotação é posteriormente derivada de todos os volumes, qtrees e compartilhamentos. "derivado" aparece ao lado do nome da anotação em uma página de ativo.

## Associar custos com anotações

Antes de executar relatórios relacionados aos custos, você deve associar os custos às anotações em nível de serviço, nível de switch e nível do sistema, o que permite o chargeback para os usuários de storage com base no uso real da produção e na capacidade replicada. Por exemplo, para o nível de nível, você pode ter valores de nível de ouro e prata e atribuir um custo mais alto ao nível de ouro do que ao nível de prata.

## Passos

1. Faça login na IU do Insightweb.
2. Clique em Gerenciar e selecione **Anotações**.


É apresentada a página Annotation (Anotação).

3. Posicione o cursor sobre a anotação nível de serviço, nível de comutação ou nível e clique  em .

A caixa de diálogo Editar anotação é exibida.

4. Insira os valores de todos os níveis existentes no campo **custo**.

As anotações nível e nível de serviço têm valores de nível automático e armazenamento de objetos, respectivamente, que não é possível remover.

5. Clique  para adicionar níveis adicionais.

6. Clique em **Salvar** quando terminar.

### Criar anotações personalizadas

Usando anotações, você pode adicionar dados personalizados específicos de negócios que correspondem às necessidades da sua empresa aos ativos. Embora o OnCommand Insight 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 do switch, número de portas e estatísticas de desempenho. Os dados que você adiciona usando anotações não são descobertos pelo Insight.

#### Passos

1. Faça login na IU da Web do Insight.
2. Clique em **Gerenciar** e selecione **Anotações**.

A página Anotações apresenta a lista de anotações.

3. Clique  em .

A caixa de diálogo **Add Annotation** (Adicionar anotação) é exibida.

4. Digite um nome e uma descrição nos campos **Nome** e **Descrição**.

Pode introduzir até 255 caracteres nestes campos.



Os nomes de anotação que começam ou terminam com um ponto "." não são suportados.

5. Clique em **Type** e, em seguida, selecione uma das seguintes opções que representa o tipo de dados permitidos nesta anotação:

- Booleano

Isso 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

Isso pode criar 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** quando criar esta lista, quando outros estiverem a atribuir este tipo de anotação num dispositivo, poderão adicionar mais valores à lista.

- Número

Isto cria um campo onde o utilizador que atribui a anotação pode introduzir um número. Por exemplo, se o tipo de anotação for "Floor", o usuário poderá selecionar o valor tipo de "Number" e inserir o número do piso.

- Texto

Isso cria um campo que permite texto de forma livre. Por exemplo, você pode inserir "Idioma" como tipo de anotação, selecionar "texto" como o tipo de valor e inserir um idioma como um 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.

6. Se selecionar **List** como tipo de anotação, faça o seguinte:

- 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.

- Introduza um valor e um nome nos campos **valor** e **Descrição**.

- Clique  para adicionar valores adicionais.

- Clique  para remover um valor.

7. Clique em **Salvar**.

As suas anotações aparecem na lista na página Anotações.

## Informações relacionadas

["Importar e exportar dados do utilizador"](#)


## 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 na IU da Web do OnCommand Insight.
2. Localize o ativo ao qual deseja aplicar a anotação, fazendo uma das seguintes opções:
  - Clique no ativo no Painel de ativos.
  - Clique  na barra de ferramentas para exibir a caixa **pesquisar ativos**, digite o tipo ou o nome do ativo e selecione o ativo na lista exibida.

A página de ativos é exibida.

3. Na seção **dados do usuário** da página de ativo, clique  em .

A caixa de diálogo Adicionar anotação é exibida.

4. Clique em **Annotation** e selecione uma anotação na lista.
5. Clique em **value** e faça um dos seguintes procedimentos, 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.
6. Clique em **Salvar**.
7. Se pretender alterar o valor da anotação depois de a atribuir, clique  em e selecione um valor diferente.

Se a anotação for do tipo de lista para o qual a opção **Add values dinamicamente após a atribuição de anotações** está selecionada, você pode digitar para adicionar um novo valor além de selecionar um valor existente.

### Modificar anotações

Talvez você queira alterar o nome, a descrição ou os valores de uma anotação ou excluir uma anotação que não deseja mais usar.

### Passos

1. Faça login na IU do OnCommand Insightweb.
2. Clique em **Gerenciar** e selecione **Anotações**.

É apresentada a página Anotações.

3. Posicione o cursor sobre a anotação que pretende editar e clique  em .

A caixa de diálogo **Edit Annotation** (Editar anotação) é exibida.

4. Pode efetuar as seguintes modificações numa anotação:

a. Altere o nome, a descrição ou ambos.

No entanto, note que pode introduzir um máximo de 255 caracteres para o nome e descrição e não pode alterar o tipo de qualquer anotação. Além disso, para anotações no nível do sistema, não é possível alterar o nome ou a descrição; no entanto, pode adicionar ou remover valores se a anotação for um tipo de lista.



Se uma anotação personalizada for publicada no Data Warehouse e você renomeá-la, você perderá dados históricos.

a. Para adicionar outro valor a uma anotação do tipo de lista, clique **+ Add** em .

b. Para remover um valor de uma anotação do tipo de lista, clique  em .

Não é possível eliminar um valor de anotação se esse valor estiver associado a uma anotação contida numa regra de anotação, consulta ou política de desempenho.

5. Clique em **Salvar** quando terminar.

## Depois de terminar

Se você vai usar anotações no Data Warehouse, você precisa forçar uma atualização de anotações no Data Warehouse. Consulte o *Guia de Administração do Armazém de dados do OnCommand Insight*.

## Eliminar anotações


Pode querer eliminar uma anotação que já não pretende utilizar. Não é possível eliminar uma anotação no nível do sistema ou uma anotação que seja utilizada numa regra de anotação, consulta ou política de desempenho.

## Passos

1. Faça login na IU da Web do OnCommand Insight.

2. Clique em **Gerenciar** e selecione **Anotações**.

É apresentada a página Anotações.

3. Posicione o cursor sobre a anotação que pretende eliminar e clique  em .

É apresentada uma caixa de diálogo de confirmação.

4. Clique em **OK**.

## Atribuir anotações a ativos usando regras de anotação

Para atribuir automaticamente anotações a ativos com base nos critérios definidos, configure regras de anotação. O OnCommand Insight atribui as anotações aos ativos com base nessas regras. O Insight também fornece duas regras de anotação padrão, que você pode modificar para atender às suas necessidades ou remover se não quiser

usá-las.

### Regras de anotação de armazenamento predefinidas

Para agilizar a atribuição de anotações de storage aos seus recursos, o OnCommand Insight inclui 21 regras de anotação padrão, que associam um nível de camada a um modelo de camada de storage. Todos os seus recursos de storage são automaticamente associados a uma categoria após a aquisição dos ativos em seu ambiente.

As regras de anotação padrão aplicam anotações de nível da seguinte forma:

- Camada 1, camada de qualidade de storage

A anotação Tier 1 é aplicada aos seguintes fornecedores e suas famílias especificadas: EMC (Symmetrix), HDS (HDS9500V, HDS9900, HDS9900V, R600, R700, USP r, USP V), IBM (DS8000), NetApp (FAS6000 ou FAS6200) e Violino (memória).

- Camada 2, camada de qualidade de storage

A anotação Tier 2 é aplicada aos seguintes fornecedores e suas famílias especificadas: HP (3PARPAR StoreServ ou EVA), EMC (CLARiiON), HDS (AMS ou D800), IBM (XIV) e NetApp (FAS3000, FAS3100 e FAS3200).

Você pode editar as configurações padrão dessas regras para corresponder aos requisitos de nível ou removê-las se não precisar delas.

### 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. Faça login na IU da Web do OnCommand Insight.
2. Clique em **Manage** e selecione **Annotation rules**.

A página regras de anotação exibe a lista de regras de anotação existentes.

3. Clique **+ Add** em .

A caixa de diálogo Adicionar regra é exibida.

#### 4. 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 o OnCommand Insight deve usar 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.

#### 5. Clique em **Salvar**.

6. Clique em **Executar todas as regras** se quiser executar todas as regras imediatamente; caso contrário, as regras são executadas em um intervalo programado regularmente.

### Definir precedência de regra de anotação

Por padrão, o OnCommand Insight avalia as regras de anotação sequencialmente; no entanto, você pode configurar a ordem na qual o OnCommand Insight avalia as regras de anotação se desejar que o Insight avalie regras em uma ordem específica.

### Passos

1. Faça login na IU do Insightweb.
2. Clique em **Manage** e selecione **Annotation rules**.

A página regras de anotação exibe a lista de regras de anotação existentes.

3. Posicione o cursor sobre uma regra de anotação.

As setas de precedência aparecem à direita da regra.

4. Para mover uma regra para cima ou para baixo na lista, clique na seta para cima ou na seta para baixo.

Por padrão, novas regras são adicionadas sequencialmente à lista de regras. Anotações definidas manualmente em páginas de ativos individuais têm precedência sobre anotações baseadas em regras quando o Insight avalia as regras de anotação.

### 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. Faça login na IU do OnCommand Insightweb.
2. Clique em **Manage** e selecione **Annotation rules**.

A página regras de anotação exibe a lista de regras de anotação existentes.



3. Localize a regra que você deseja modificar:
  - Na página regras de anotação, pode filtrar as regras de anotação introduzindo um valor na caixa de filtro.
  - Clique em um número de página para navegar pelas regras de anotação por página se houver mais regras do que ajustar em uma página.
4. Execute um dos seguintes procedimentos para exibir a caixa de diálogo **Editar regra**:
  - Se estiver na página regras de Anotação, posicione o cursor sobre a regra de anotação e clique  em .
  - Se você estiver em uma página de ativo, posicione o cursor sobre a anotação associada à regra, posicione o cursor sobre o nome da regra quando ela for exibida e clique no nome da regra.
5. Faça as alterações necessárias e clique em **Salvar**.


### Eliminar regras de anotação

Você pode excluir uma regra de anotação quando a regra não for mais necessária para monitorar os objetos na rede.

### Passos

1. Faça login na IU do OnCommand Insightweb.
2. Clique em **Manage** e selecione **Annotation rules**.

A página regras de anotação exibe a lista de regras de anotação existentes.

3. Localize a regra que você deseja excluir:
  - Na página regras de anotação, pode filtrar as regras de anotação introduzindo um valor na caixa de filtro.
  - Clique em um número de página para navegar pelas regras de anotação por página se houver mais regras do que encaixar em uma única página.
4. Aponte o cursor sobre a regra que pretende eliminar e, em seguida, clique  em .

Uma mensagem de confirmação é exibida, solicitando se deseja excluir a regra.

5. Clique em **OK**.

### Importar valores de anotação

Se você mantiver anotações em objetos SAN (como armazenamento, hosts e máquinas virtuais) em um arquivo CSV, poderá importar essas informações para o OnCommand Insight. Você pode importar aplicativos, entidades de negócios ou anotações, como camada e construção.

### Sobre esta tarefa

Aplicam-se as seguintes regras:

- Se um valor de anotação estiver vazio, essa anotação será removida do objeto.
- Ao anotar volumes ou volumes internos, o nome do objeto é uma combinação de nome de

armazenamento e nome do volume usando o traço e o separador de seta (→):

```
<storage_name>-><volume_name>
```

- Quando o armazenamento, os switches ou as portas são anotados, a coluna da aplicação é ignorada.
- As colunas de Tenant, Line\_of\_Business, Business\_Unit e Project compõem uma entidade de negócio.

Qualquer um dos valores pode ser deixado vazio. Se um aplicativo já estiver relacionado com uma entidade de negócios diferente dos valores de entrada, o aplicativo será atribuído à nova entidade de negócios.

Os seguintes tipos de objeto e chaves são suportados no utilitário de importação:

Tipo	Chave
Host	id-><id> ou ou <Name> <IP>
VM	id-><id> ou <Name>
Pool de storage	id-><id> ou '<Storage_name>'→<Storage_Pool_name>
Volume interno	id-><id> ou '<Storage_name>'→<Internal_volume_name>
Volume	id-><id> ou '<Storage_name>'→<Volume_name>
Armazenamento	id-><id> ou ou <Name> <IP>
Interrutor	id-><id> ou ou <Name> <IP>
Porta	id-><id> ou <WWN>
Partilhar	id-><id> ou <Storage Name>-><Internal Volume Name>-><Share Name>-><Protocol> <Qtree> é opcional se houver uma qtree padrão.
Qtree	id-><id> ou <Storage Name>-><Internal Volume Name>-><Qtree Name>

O arquivo CSV deve usar o seguinte formato:

```

, , <Annotation Type> [, <Annotation Type> ...]
[, Application] [, Tenant] [, Line_Of_Business] [,
Business_Unit] [, Project]

<Object Type Value 1>, <Object Key 1>, <Annotation Value> [,
<Annotation Value> ...] [, <Application>] [, <Tenant>] [,
<Line_Of_Business>] [, <Business_Unit>] [, <Project>]

...

<Object Type Value N>, <Object Key N>, <Annotation Value> [,
<Annotation Value> ...] [, <Application>] [, <Tenant>] [,
<Line_Of_Business>] [, <Business_Unit>] [, <Project>]

```

## Passos

1. Faça login na IU da Web do Insight.
2. Clique em **Admin** e selecione **Troubleshooting**.  
É apresentada a página Resolução de problemas.
3. Na seção **outras tarefas** da página, clique no link **Portal OnCommand Insight**.
4. Clique em **Insight Connect API**.
5. Inicie sessão no portal.
6. Clique em **Utilitário de importação de anotação**.
7. Salve o .zip arquivo, descompacte-o e leia o readme.txt arquivo para obter informações adicionais e amostras.
8. Coloque o arquivo CSV na mesma pasta que o .zip arquivo.
9. Na janela da linha de comando, digite o seguinte:

```

java -jar rest-import-utility.jar [-username] [-ppassword]
[-aserver name or IP address] [-bbatch size] [-ccase
sensitive:true/false]
[-lextra logging:true/false] csv filename

```

A opção -l, que permite o Registro extra, e a opção -c, que permite a sensibilidade do caso, são definidas como false por padrão. Portanto, você deve especificá-los somente quando quiser usar os recursos.



Não há espaços entre as opções e seus valores.



As palavras-chave a seguir são reservadas e impedem que os usuários as especifiquem como nomes de anotação: - Aplicação - prioridade\_aplicação - Tenant - Line\_of\_Business - Business\_Unit - erros de projeto são gerados se você tentar importar um tipo de anotação usando uma das palavras-chave reservadas. Se você criou nomes de anotação usando essas palavras-chave, você deve modificá-los para que a ferramenta de utilitário de importação possa funcionar corretamente.



O utilitário de importação de anotações requer Java 8 ou Java 11. Certifique-se de que um deles está instalado antes de executar o utilitário de importação. Recomenda-se usar o OpenJDK 11 mais recente.

## Atribuindo anotações a vários ativos usando uma consulta

A atribuição de uma anotação a um grupo de ativos ajuda a identificar ou utilizar mais facilmente esses ativos relacionados em consultas ou painéis.

### Antes de começar

As anotações que você deseja atribuir a ativos devem ter sido criadas anteriormente.

### Sobre esta tarefa

Você pode simplificar a tarefa de atribuir uma anotação a vários ativos usando uma consulta. Por exemplo, se pretender atribuir uma anotação de endereço personalizado a todas as suas matrizes numa localização específica do centro de dados.

### Passos

1. Crie uma nova consulta para identificar os ativos nos quais você deseja atribuir uma anotação. Clique em **consultas** > \* Nova consulta\*.
2. Na lista suspensa **Search for...**, escolha **Storage**. Você pode definir filtros para restringir ainda mais a lista de armazenamentos exibida.
3. Na lista de armazenamentos exibida, selecione um ou mais clicando na caixa de seleção ao lado do nome de armazenamento. Você também pode selecionar todos os armazenamentos exibidos clicando na caixa de seleção principal na parte superior da lista.
4. Quando tiver selecionado todos os armazenamentos desejados, clique em **ações** > **Editar anotação**.

O sistema exibe a caixa de diálogo Adicionar anotação.

5. Selecione **Anotação** e **valor** que deseja atribuir aos armazenamentos e clique em **Salvar**.

Se estiver a apresentar a coluna para essa anotação, esta será apresentada em todos os armazenamentos selecionados.

6. Agora você pode usar a anotação para filtrar armazenamentos em um widget ou consulta. Em um widget, você pode fazer o seguinte:
  - a. Crie um dashboard ou abra um já existente. Adicione uma **variável** e escolha a anotação que você definiu nos armazenamentos acima. A variável é adicionada ao painel de instrumentos.
  - b. No campo variável que você acabou de adicionar, clique em **any** e insira o valor apropriado para filtrar. Clique na marca de verificação para guardar o valor da variável.

- c. Adicione um widget. Na consulta do widget, clique no botão **Filter by\*\*** e selecione a anotação apropriada na lista.
- d. Clique em **any** e selecione a variável de anotação que você adicionou acima. As variáveis que você criou começam com "" e são exibidas na lista suspensa.
- e. Defina quaisquer outros filtros ou campos que desejar e clique em **Salvar** quando o widget for personalizado de acordo com o seu gosto.

O widget no painel apresenta os dados apenas para os armazenamentos aos quais atribuiu a anotação.

## Consulta de ativos

As consultas permitem que você monitore e solucione problemas de sua rede pesquisando os ativos em seu ambiente em um nível granular com base em critérios selecionados pelo usuário (anotações e métricas de desempenho). Além disso, as regras de anotação, que atribuem automaticamente anotações a ativos, exigem uma consulta.

### Ativos usados em consultas e dashboards

As consultas de insight e widgets de painel podem ser usadas com uma ampla gama de tipos de ativos

Os seguintes tipos de ativos podem ser usados em consultas, widgets de painel e páginas de ativos personalizadas. 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
- Interruptor

- Fita
- VMDK
- Máquina virtual
- Volume
- Zona
- Membro da zona

## Criando uma consulta

Você pode criar uma consulta para permitir que você pesquise os ativos em seu ambiente em um nível granular. As consultas permitem que você corte dados adicionando filtros e, em seguida, classificando os resultados para visualizar os dados de inventário e desempenho em uma exibição.

### Sobre esta tarefa

Por exemplo, você pode criar uma consulta para volumes, adicionar um filtro para localizar armazenamentos específicos associados ao volume selecionado, adicionar um filtro para encontrar uma anotação específica, como o 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.

Quando uma nova fonte de dados é adicionada que adquire ativos ou qualquer anotação ou atribuição de aplicativo é feita, você pode consultar esses ativos, anotações ou aplicativos após as consultas serem indexadas, o que ocorre em um intervalo programado regularmente.

### Passos

1. Faça login na IU da Web do OnCommand Insight.
2. Clique em **consultas** e selecione \* Nova consulta\*.
3. Clique em **Selecionar tipo de recurso** e selecione um tipo de ativo.


Quando um recurso é selecionado para uma consulta, várias colunas padrão são exibidas automaticamente; você pode remover essas colunas ou adicionar novas a qualquer momento.

4. Na caixa de texto **Nome**, digite o nome do ativo ou digite uma parte do texto para filtrar os nomes dos ativos.


Você pode usar qualquer uma das seguintes opções sozinho ou combinado para refinar sua pesquisa em qualquer caixa de texto na página Nova consulta:

- 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.

5. Clique  em para exibir os ativos.

6. Para adicionar um critério, clique  em e execute um dos seguintes procedimentos:

- Digite para procurar um critério específico e selecione-o.
- Role para baixo a lista e selecione um critério.
- Insira um intervalo de valores se você escolher uma métrica de desempenho como IOPS - leitura (IO/s). As anotações padrão fornecidas pelo Insight são indicadas por ; é possível ter anotações com nomes duplicados.

Uma coluna é adicionada à lista resultados da consulta para os critérios e os resultados da consulta nas atualizações da lista.

7. Opcionalmente, você pode clicar  para remover uma anotação ou métrica de desempenho dos resultados da consulta.

Por exemplo, se sua consulta mostrar latência máxima e taxa de transferência máxima para datastores e você quiser mostrar apenas latência máxima na lista de resultados da consulta, clique neste botão e desmarque a caixa de seleção **throughput - máximo**. A coluna throughput - Max (MB/s) é removida da lista de resultados da consulta.



Dependendo do número de colunas exibidas na tabela de resultados da consulta, talvez você não consiga exibir colunas adicionais adicionadas. Você pode remover uma ou mais colunas até que as colunas desejadas fiquem visíveis.

8. Clique em **Salvar**, insira um nome para a consulta e clique em **Salvar** novamente.

Se você tiver uma conta com uma função de administrador, poderá criar painéis personalizados. Um painel personalizado pode incluir qualquer um dos widgets da Biblioteca de widgets, vários dos quais permitem representar os resultados da consulta em um painel personalizado. Para obter mais informações sobre painéis personalizados, consulte o *Guia de Introdução ao OnCommand Insight*.

## Informações relacionadas

["Importar e exportar dados do utilizador"](#)

## 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 na IU da Web do OnCommand Insight.
2. Clique em **consultas** e selecione **Mostrar todas as consultas**.
3. Você pode alterar a forma como as consultas são exibidas fazendo qualquer um dos seguintes procedimentos:

- Você pode inserir texto na caixa **filtro** para pesquisar para exibir consultas específicas.
- 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.
- 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.
- 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 Insight faz o polling automático de suas fontes 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 querer exportar os resultados de uma consulta para um arquivo .CSV para importar os dados para outro aplicativo.

### Passos

1. Faça login na IU da Web do OnCommand Insight.
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 .CSV ficheiro.
5. Execute um dos seguintes procedimentos:
  - Clique em **abrir com** e em **OK** para abrir o arquivo com o Microsoft Excel e salvar o arquivo em um local específico.
  - Clique em **Salvar arquivo** e em **OK** para salvar o arquivo na pasta Downloads. Apenas os atributos para as colunas exibidas serão exportados. Algumas colunas exibidas, particularmente aquelas que fazem parte de relacionamentos aninhados complexos, não são exportadas.



Quando uma vírgula aparece no nome de um ativo, a exportação encerra o nome em aspas, preservando o nome do ativo e o formato .csv adequado.

Ao exportar resultados da consulta, esteja ciente de que **todas** linhas na tabela de resultados serão exportadas, não apenas as selecionadas ou exibidas na tela, até um máximo de 10.000 linhas.

E



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:

E



- Open a new sheet in Excel.
  - On the "Data" tab, choose "From Text".
  - Locate the desired .CSV file and click "Import".
  - In the Import wizard, choose "Delimited" and click Next.
  - Choose "Comma" for the delimiter and click Next.
  - Select the desired columns and choose "Text" for the column data format.
  - Click Finish.
- Your objects should show in Excel in the proper format.

E


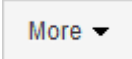
## Modificando consultas

Você pode alterar os critérios associados a uma consulta quando quiser alterar os critérios de pesquisa dos ativos que você está consultando.

### Passos

1. Faça login na IU do Insightweb.
2. Clique em **consultas** e selecione **Mostrar todas as consultas**.


A página consultas é exibida.

3. Clique no nome da consulta.
4. Para remover um critério da consulta, clique  em .
5. Para adicionar um critério à consulta, clique  em e selecione um critério na lista.
6. Execute um dos seguintes procedimentos:
  - Clique em **Salvar** para salvar a consulta com o nome que foi usado inicialmente.
  - Clique em **Salvar como** para salvar a consulta com outro nome.
  - Clique em **Renomear** para alterar o nome da consulta que você usou inicialmente.
  - Clique em **Revert** para alterar o nome da consulta de volta para aquele que você usou inicialmente.

## Eliminar consultas

Você pode excluir consultas quando elas não coletarem mais informações úteis sobre seus ativos. Não é possível excluir uma consulta se ela for usada em uma regra de anotação.

### Passos

1. Faça login na IU do Insightweb.
2. Clique em **consultas** e selecione **Mostrar todas as consultas**.  
A página consultas é exibida.
3. Posicione o cursor sobre a consulta que deseja excluir e clique  em .  
É apresentada uma mensagem de confirmação, perguntando se pretende eliminar a consulta.
4. Clique em **OK**.



## Atribuir vários aplicativos ou remover vários aplicativos de ativos

Você pode atribuir vários aplicativos ou remover vários aplicativos de ativos usando uma consulta em vez de ter que atribuí-los ou removê-los manualmente.

### Antes de começar

Você já deve ter criado uma consulta que encontre todos os ativos que você editar.

### Passos

1. Clique em **consultas** e selecione **Mostrar todas as consultas**.  
A página consultas é exibida.
2. Clique no nome da consulta que encontra os ativos.  
A lista de ativos associados à consulta é exibida.
3. Selecione os ativos desejados na lista ou clique  ▼ para selecionar **All**.  
O botão **ações** é exibido.
4. Para adicionar um aplicativo aos ativos selecionados, clique  em e selecione **Editar aplicativo**.
  - a. Clique em **Application** e selecione um ou mais aplicativos.  
Você pode selecionar vários aplicativos para hosts, volumes internos e máquinas virtuais; no entanto, você pode selecionar apenas um aplicativo para um volume.
  - b. Clique em **Salvar**.
5. Para remover um aplicativo atribuído aos ativos, clique  e selecione **Remover aplicativo**.

- a. Selecione a aplicação ou aplicações que pretende remover.
- b. Clique em **Excluir**.

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.

## Editar ou remover várias anotações de ativos

Você pode editar várias anotações para ativos ou remover várias anotações de ativos usando uma consulta em vez de ter que editá-las ou removê-las manualmente.

### Antes de começar

Você já deve ter criado uma consulta que encontre todos os ativos que deseja editar.

### Passos

1. Clique em **consultas** e selecione **Mostrar todas as consultas**.

A página consultas é exibida.

2. Clique no nome da consulta que encontra os ativos.

A lista de ativos associados à consulta é exibida.

3. Selecione os ativos desejados na lista ou clique  ▼ para selecionar **All**.

O botão **ações** é exibido.

4. Para adicionar uma anotação aos ativos ou editar o valor de uma anotação atribuída aos ativos, clique

em e selecione **Editar anotação**.

- a. Clique em **Anotação** e selecione uma anotação para a qual deseja alterar o valor ou selecione uma nova anotação para atribuí-la a todos os ativos.
- b. Clique em **value** e selecione um valor para a anotação.
- c. Clique em **Salvar**.

5. Para remover uma anotação atribuída aos ativos, clique  em e selecione **Remover anotação**.

- a. Clique em **Annotation** e selecione a anotação que pretende remover dos ativos.
- b. Clique em **Excluir**.

## Copiando valores de tabela

Você pode copiar valores em tabelas 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.

## 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 cujo comprimento exceda a largura da coluna da tabela, indicada por elipses (...), passe o cursor sobre o campo e clique no ícone da área de transferência. 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. Observe também que somente campos que incluem valores únicos (ou seja, não listas) têm o ícone de cópia.

## Gerenciamento de políticas de performance

O OnCommand Insight permite que você crie políticas de desempenho para monitorar sua rede em busca de vários limites e gerar alertas quando esses limites forem ultrapassados. Usando políticas de desempenho, você pode detetar uma violação de um limite imediatamente, identificar a implicação e analisar o impacto e a causa raiz do problema de uma maneira que permita uma correção rápida e eficaz.

Uma política de desempenho permite definir limites em quaisquer objetos (armazenamento de dados, disco, hipervisor, volume interno, porta, armazenamento, nó de storage, pool de armazenamento, VMDK, máquina virtual e volume) com contadores de desempenho relatados (por exemplo, IOPS total). Quando ocorre uma violação de um limite, o Insight a deteta e reporta na página de ativos associados, exibindo um círculo sólido vermelho; por alerta por e-mail, se configurado; e no Painel de violações ou em qualquer painel personalizado que denuncie violações.

O Insight fornece algumas políticas de desempenho padrão, que podem ser modificadas ou excluídas se não forem aplicáveis ao seu ambiente, para os seguintes objetos:

- Hipervisor

Há políticas de troca do ESX e utilização do ESX.

- Volume e volume internos

Há duas políticas de latência para cada recurso, uma anotada para a camada 1 e outra anotada para a camada 2.

- Porta

Há uma política para BB crédito zero.

- Nó de storage

Existe uma política para a utilização de nós.

- Máquina virtual

Há troca de VM e políticas de CPU e memória ESX.

- Volume

Há latência por camada e políticas de volume desalinhadas.

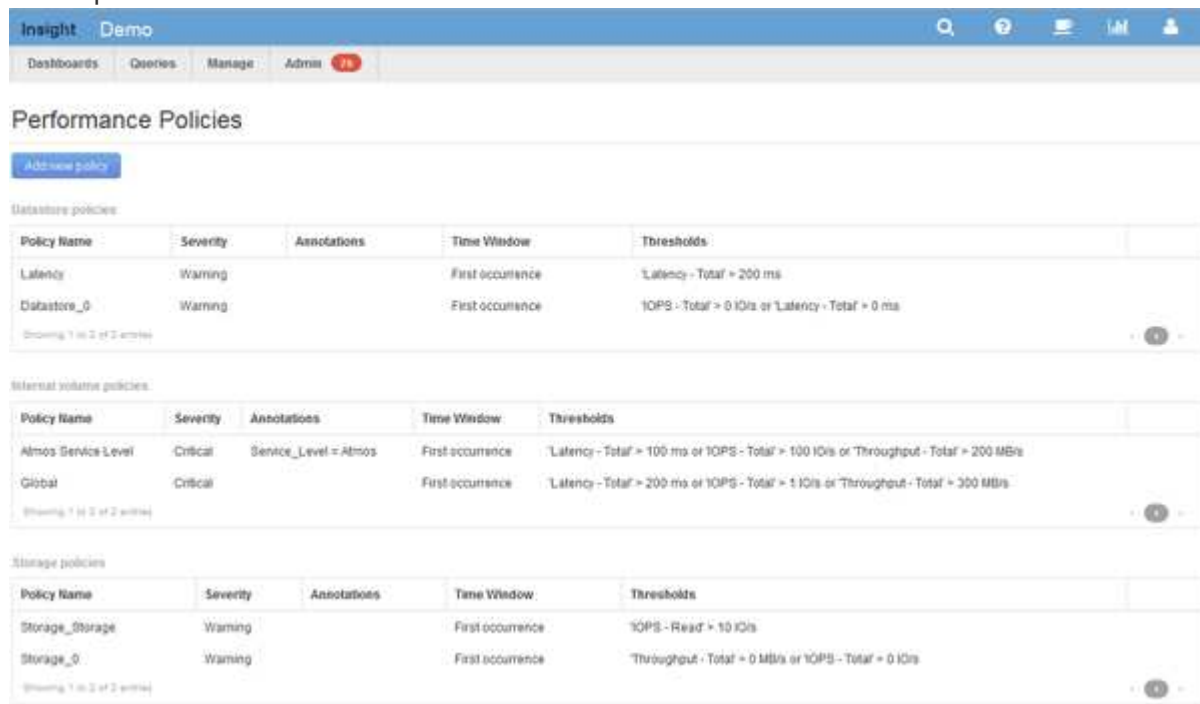
## Criação de políticas de desempenho

Você cria políticas de desempenho para definir limites que acionam alertas para notificá-lo sobre problemas relacionados aos recursos da rede. Por exemplo, você pode criar uma política de performance para alertá-lo quando a utilização total de pools de storage for superior a 60%.

### Passos

1. Abra o OnCommand Insight no seu navegador.
2. Selecione **Gerenciar > políticas de desempenho**.

É apresentada a página políticas de desempenho.



The screenshot shows the 'Performance Policies' page in OnCommand Insight. It features a navigation bar at the top with 'Inaight Demo' and a search bar. Below the navigation bar, there are tabs for 'Dashboards', 'Queries', 'Manage', and 'Admin'. The main content area is titled 'Performance Policies' and includes a '+ Add new policy' button. The page is divided into three sections, each with a table of policies:

- Database policies:**

Policy Name	Severity	Annotations	Time Window	Thresholds
Latency	Warning		First occurrence	'Latency - Total' = 200 ms
Databases_0	Warning		First occurrence	'IOPS - Total' > 0 I/Os or 'Latency - Total' = 0 ms
- Internal volume policies:**

Policy Name	Severity	Annotations	Time Window	Thresholds
Almos Service Level	Critical	Service_Level = Almos	First occurrence	'Latency - Total' = 100 ms or 'IOPS - Total' > 100 I/Os or 'Throughput - Total' > 200 MB/s
Global	Critical		First occurrence	'Latency - Total' = 200 ms or 'IOPS - Total' > 1 I/Os or 'Throughput - Total' > 300 MB/s
- Storage policies:**

Policy Name	Severity	Annotations	Time Window	Thresholds
Storage_storage	Warning		First occurrence	'IOPS - Read' > 10 I/Os
Storage_0	Warning		First occurrence	'Throughput - Total' = 0 MB/s or 'IOPS - Total' = 0 I/Os

As políticas são organizadas por objeto e são avaliadas na ordem em que aparecem na lista para esse objeto.

3. Clique em **Adicionar nova política**.

A caixa de diálogo Adicionar política é exibida.

4. No campo **Nome da política**, insira um nome para a política.

Você deve usar um nome diferente de todos os outros nomes de política para o objeto. Por exemplo, você não pode ter duas políticas chamadas de latência para um volume interno; no entanto, você pode ter uma política de latência para um volume interno e outra política de latência para um volume diferente. A melhor prática é sempre usar um nome exclusivo para qualquer política, independentemente do tipo de objeto.

5. Na lista **Apply to Objects of type** (aplicar a objetos do tipo), selecione o tipo de objeto ao qual a política se aplica.
6. Na lista **com anotação**, selecione um tipo de anotação, se aplicável, e introduza um valor para a anotação na caixa **valor** para aplicar a política apenas a objetos que tenham este conjunto de anotações específico.

7. Se você selecionou **Port** como o tipo de objeto, na lista **Connected to**, selecione à qual a porta está conetada.
8. Na lista **Apply after a window of** (aplicar após uma janela de\*), selecione quando um alerta for levantado para indicar uma violação de limite.

A primeira opção de ocorrência aciona um alerta quando um limite é excedido na primeira amostra de dados. Todas as outras opções acionam um alerta quando o limite é cruzado uma vez e é continuamente cruzado durante pelo menos o período de tempo especificado.

9. Na lista **com gravidade**, selecione a gravidade da violação.
10. Por padrão, os alertas de e-mail sobre violações de política serão enviados aos destinatários na lista global de e-mails. Você pode substituir essas configurações para que os alertas de uma política específica sejam enviados para destinatários específicos.
  - Clique no link para abrir a lista destinatários e clique no botão \* para adicionar destinatários. Os alertas de violação dessa política serão enviados a todos os destinatários da lista.
11. Clique no link **any** na seção **Create alert (criar alerta) se qualquer um dos itens a seguir for true** para controlar como os alertas são acionados:
  - \* qualquer \*

Esta é a configuração padrão, que cria alertas quando qualquer um dos limites relacionados a uma política é cruzado.

- **todos**

Essa configuração cria um alerta quando todos os limites de uma política são cruzados. Quando você seleciona **All**, o primeiro limite que você cria para uma política de desempenho é chamado de regra principal. Você deve garantir que o limite de regra principal seja a violação que você está mais preocupado com a política de desempenho.

12. Na seção **criar alerta se**, selecione um contador de desempenho e um operador e insira um valor para criar um limite.
13. Clique em **Adicionar limite** para adicionar mais limites.
14. Para remover um limite, clique no ícone da lixeira.
15. Marque a caixa de seleção **Parar processamento de outras políticas se o alerta for gerado** se desejar que a política pare de processar quando ocorrer um alerta.

Por exemplo, se você tiver quatro políticas para armazenamentos de dados e a segunda diretiva estiver configurada para interromper o processamento quando um alerta ocorrer, a terceira e a quarta políticas não serão processadas enquanto uma violação da segunda diretiva estiver ativa.

16. Clique em **Salvar**.

A página políticas de desempenho é exibida e a política de desempenho é exibida na lista de políticas para o tipo de objeto.

## Precedência de avaliação da política de desempenho

A página políticas de desempenho agrupa as políticas por tipo de objeto e o Insight avalia as políticas na ordem em que elas aparecem na lista de políticas de desempenho do objeto. Você pode alterar a ordem na qual o Insight avalia as políticas para mostrar as

informações mais importantes para você em sua rede.

O Insight avalia todas as políticas que são aplicáveis a um objeto sequencialmente quando amostras de dados de desempenho são levadas para o sistema para esse objeto; no entanto, dependendo das anotações, nem todas as políticas se aplicam a um grupo de objetos. Por exemplo, suponha que o volume interno tenha as seguintes políticas:

- Política 1 (a política padrão fornecida pelo Insight)
- Política 2 (com uma anotação de "nível de Serviço" Prata" com a opção **Parar processamento de políticas adicionais se o alerta for gerado**)
- Política 3 (com uma anotação do "nível de Serviço" Gold")
- Política 4

Para um nível de volume interno com uma anotação Gold, o Insight avalia a Política 1, ignora a Diretiva 2 e, em seguida, avalia a Diretiva 3 e a Diretiva 4. Para um nível não anotado, o Insight avalia pela ordem das políticas; assim, o Insight avalia somente a Política 1 e a Política 4. Para um nível de volume interno com uma anotação Silver, o Insight avalia a Política 1 e a Política 2; no entanto, se um alerta for acionado quando o limite da política for cruzado uma vez e for continuamente cruzado para a janela de tempo especificada na política, o Insight não avaliará mais as outras políticas na lista enquanto avalia os contadores atuais para o objeto. Quando o Insight captura o próximo conjunto de amostras de desempenho para o objeto, ele novamente começa a avaliar as políticas de desempenho para o objeto por filtro e depois por ordem.

### Alterar a precedência de uma política de desempenho

Por padrão, o Insight avalia sequencialmente as políticas de um objeto. Você pode configurar a ordem na qual o Insight avalia as políticas de desempenho. Por exemplo, se você tiver uma política configurada para interromper o processamento quando ocorrer uma violação para o armazenamento de nível Gold, poderá colocar essa política primeiro na lista e evitar ver mais violações genéricas para o mesmo ativo de armazenamento.

#### Passos

1. Abra o Insight em seu navegador.
2. No menu **Gerenciar**, selecione **políticas de desempenho**.

A página políticas de desempenho é exibida.

3. Passe o cursor sobre um nome de política na lista de políticas de desempenho de um tipo de objeto.

As setas de precedência aparecem à direita da política.

4. Para mover uma política para cima na lista, clique na seta para cima; para mover uma política para baixo na lista, clique na seta para baixo.

Por padrão, novas políticas são adicionadas sequencialmente à lista de políticas de um objeto.


### Editando políticas de desempenho

Pode editar políticas de desempenho existentes e predefinidas para alterar a forma como o Insight monitoriza as condições de interesse para si na sua rede. Por exemplo, você pode querer alterar o limite de uma política.

## Passos

1. Abra o Insight em seu navegador.
2. No menu **Gerenciar**, selecione **políticas de desempenho**.

A página políticas de desempenho é exibida.

3. Passe o cursor sobre um nome de política na lista de políticas de desempenho de um objeto.
4. Clique  em .

A caixa de diálogo Editar política é exibida.

5. Faça as alterações necessárias.

Se você alterar qualquer opção que não seja o nome da política, o Insight excluirá todas as violações existentes dessa política.

6. Clique em **Salvar**.


## Excluindo políticas de desempenho

Você pode excluir uma política de desempenho se achar que ela não é mais aplicável ao monitoramento dos objetos em sua rede.

### Passos

1. Abra o Insight em seu navegador.
2. No menu **Gerenciar**, selecione **políticas de desempenho**.

A página políticas de desempenho é exibida.

3. Passe o cursor sobre o nome de uma política na lista de políticas de desempenho de um objeto.
4. Clique  em .

É apresentada uma mensagem a perguntar se pretende eliminar a política.

5. Clique em **OK**.

## Importar e exportar dados do utilizador

As funções de importação e exportação permitem exportar anotações, regras de anotação, consultas, políticas de desempenho e painéis personalizados para um único arquivo. Esse arquivo pode então ser importado para diferentes servidores OnCommand Insight.

As funções de exportação e importação são suportadas apenas entre servidores que executam a mesma versão do OnCommand Insight.

Para exportar ou importar dados de usuário, clique em **Admin** e selecione **Setup** e, em seguida, escolha a guia **Import/Export user data**.



Durante a operação de importação, os dados são adicionados, mesclados ou substituídos, dependendo dos objetos e tipos de objetos que estão sendo importados.

- Tipos de anotação

- Adiciona uma anotação se não existir nenhuma anotação 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.



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.

- Regras de anotação

- Adiciona uma regra de anotação se não existir nenhuma regra de anotação com o mesmo nome no sistema de destino.
- Substitui uma regra de anotação se existir uma regra de anotação com o mesmo nome no sistema de destino.



As regras de anotação dependem de consultas e anotações. Tem de verificar a precisão de todas as regras de anotação após a conclusão da operação de importação.

- Políticas

- Adiciona uma política se não existir nenhuma política com o mesmo nome no sistema de destino.
- Substitui uma política se existir uma política com o mesmo nome no sistema de destino.



As políticas podem estar desordenadas após a conclusão da operação de importação. Você deve verificar a ordem de política após a importação. As políticas que dependem de anotações podem falhar se as anotações estiverem incorretas. Você deve verificar todas as dependências de anotação após a importação.

E

- Consultas

- Adiciona uma consulta se não existir nenhuma consulta com o mesmo nome no sistema de destino.
- Substitui uma consulta se existir uma consulta com o mesmo nome no sistema de destino, mesmo que o tipo de recurso da consulta seja diferente.



Se o tipo de recurso de uma consulta for diferente, após a importação, todos os widgets do painel que usam essa consulta podem exibir resultados indesejados ou incorretos. Você deve verificar todos os widgets baseados em consulta para obter precisão após a importação. As consultas que dependem de anotações podem falhar se as anotações estiverem incorretas. Você deve verificar todas as dependências de anotação após a importação.

E

- Dashboards

- Adiciona um painel se não existir nenhum painel com o mesmo nome no sistema de destino.
- Substitui um dashboard se existir um dashboard com o mesmo nome no sistema de destino, mesmo que o tipo de recurso da consulta seja diferente.



Você deve verificar todos os widgets baseados em consulta nos painéis para a precisão após a importação. Se o servidor de origem tiver vários painéis com o mesmo nome, todos eles serão exportados. No entanto, apenas o primeiro será importado para o servidor de destino. Para evitar erros durante a importação, você deve garantir que seus painéis tenham nomes exclusivos antes de exportá-los.

E

## 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.