Configurar e gerenciar contas de usuário

OnCommand Insight

NetApp
October 24, 2024

Índice

Configurar e gerenciar contas de usuário 1
Antes de começar 1
Passos 1
Resultados 2
Funções de usuário do Insight 2
Configurando o Insight para LDAP(s) 2
Alterando senhas de usuário 7
Editar uma definição de utilizador 8
Eliminar uma conta de utilizador 8

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 ative 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"o , 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 ative 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 ative 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 ative 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 ative 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 ative 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>\SANscreen\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
siga

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 ative 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 ative Directory. Implementações LDAP adicionais podem funcionar, mas não foram qualificadas com o Insight. Este procedimento pressupõe que você esteja usando o LDAP do Microsoft ative 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 conetar 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 ative 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**.

Informações sobre direitos autorais

Informações sobre marcas comerciais