



Configurando o Insight para LDAP(s)

OnCommand Insight

NetApp
October 24, 2024

Índice

- Configurando o Insight para LDAP(s) 1
 - Configurando definições de usuário usando LDAP 3

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", 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 registros 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 ativo 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 ativo 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 ativo 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", reinicie o serviço *SANscreen* antes de importar o certificado LDAP.

Sobre esta tarefa

O OnCommand Insight suporta LDAP e LDAPS através do servidor Microsoft ativo Directory. Implementações LDAP adicionais podem funcionar, mas não foram qualificadas com o Insight. Este procedimento pressupõe que você esteja usando o LDAP do Microsoft ativo 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 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**.

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 INTERRUPÇÃO 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.