为LDAP配置Insight

OnCommand Insight

NetApp
October 24, 2024

目录

为LDAP配置Insight

OnCommand Insight 必须使用在公司LDAP域中配置的轻型目录访问协议(LDAP)设置进行配置。

在配置Insight以与LDAP或安全LDAP (LDAPS)结合使用之前、请记下企业环境中的Active Directory配置。Insight设置必须与您组织的LDAP域配置中的设置匹配。在配置Insight以用于LDAP之前、请查看以下概念、并与LDAP域管理员联系、了解要在您的环境中使用的正确属性。

对于所有安全Active Directory (例如LDAPS)用户、您必须使用证书中定义的AD服务器名称。不能使用IP地址进行安全AD登录。

如果使用更改了_server.keystore_和/或_server.trustore_pands，请"安全管理员"在导入SANscreen证书之前重新启动_ldap_服务。

OnCommand Insight 通过Microsoft Active Directory服务器或Azure AD支持LDAP和LDAPS。其他LDAP实施可能有效、但尚未通过Insight认证。这些指南中的过程假定您使用的是Microsoft Active Directory版本2或3 LDAP (轻型目录访问协议)。

用户主体名称属性：

Insight使用LDAP User Principal Name属性(userPrincipalName)作为username属性。用户主体名称保证在Active Directory (AD)林中具有全局唯一性、但在许多大型组织中、用户主体名称可能不会立即为其所识别或识别。您的组织可能会在主用户名中使用User Principal Name属性的替代项。

以下是User Principal Name属性字段的一些备用值：

- * sAMAccountName*

  此用户属性是旧版Windows 2000 NT之前的用户名、大多数用户都习惯使用此用户登录到其个人Windows计算机。这并不能保证在整个AD林中具有全局唯一性。

  对于User Principal Name属性、sAMAccountName区分大小写。

- 邮件

  在使用MS Exchange的AD环境中、此属性是最终用户的主电子邮件地址。与userPrincipalName属性不同、此属性在整个AD林中应具有全局唯一性(最终用户也很熟悉)。大多数非MS Exchange环境中都不存在邮件属性。

- 转介

  LDAP转介是指域控制器向客户端应用程序指示其没有所请求对象的副本(或者更准确地说、 它不会保留目录树中该对象所在的部分(如果该对象确实存在)、并为客户端提供更可能持有该对象的位置。而客户端又会使用转介作为对域控制器进行DNS搜索的基础。理想情况下、转介始终引用确实持有该对象的域控制器。但是、转介到的域控制器可能会生成另一个转介、但通常不需要很长时间才能发现对象不存在并通知客户端。

sAMAccountName通常优先于用户主体名称。sAMAccountName在域中是唯一的(虽然在域林中可能不是唯一的)、但它是用户通常用于登录的字符串域(例如、*NetApp\username*)。Distinguished Name是林中的唯一名称、但通常不为用户所知。

在同一域的Windows系统部分上、您可以始终打开命令提示符并键入set以查找正确的域名(USERDOMAIN=)。然后、OCI登录名将为 `USERDOMAIN\sAMAccountName`。

域名*：mydomain.x.y.z.com *、请使用 `DC=x,DC=y,DC=z,DC=com` 在Insight的域字段中。

- 端口 * ：

LDAP的默认端口为389、LDAPS的默认端口为636

LDAPS的典型URL： `ldaps://<ldap_server_host_name>:636`

日志位于：`\\<install directory>\SANscreen\wildfly\standalone\log\ldap.log`

默认情况下、Insight需要以下字段中记录的值。如果这些更改在Active Directory环境中发生、请务必在Insight LDAP配置中进行更改。

Role属性
成员
Mail属性
邮件
Distinguished Name属性
distinguishedName
转介
请遵循

组：

要对OnCommand Insight 和DWH服务器中具有不同访问角色的用户进行身份验证、您必须在Active Directory中创建组、并在OnCommand Insight 和DWH服务器中输入这些组名称。以下组名称仅为示例；您在Insight中为LDAP配置的名称必须与为Active Directory环境设置的名称匹配。

Insight Group	示例
Insight服务器管理员组	insight.server.admins

Insight管理员组	insight.m管理员
Insight用户组	insight.users
Insight来宾组	insight.guests
报告管理员组	insight.report.管理员
报告专业作者组	insight.report.proauthors
报告作者组	insight.report.business.authors
报告使用者组	insight.report.business.consumers
报告收件人组	insight.report.recipients

使用LDAP配置用户定义

要从LDAP服务器配置OnCommand Insight (OCI)以进行用户身份验证和授权、必须在LDAP服务器中将您定义为OnCommand Insight 服务器管理员。

开始之前

您必须知道在LDAP域中为Insight配置的用户和组属性。

对于所有安全Active Directory (例如LDAPS)用户、您必须使用证书中定义的AD服务器名称。不能使用IP地址进行安全AD登录。

如果使用更改了_server.keystore_和/或_server.trustore_pands，请"安全管理员"在导入SANscreen证书之前重新启动_ldap_服务。

关于此任务

OnCommand Insight 通过Microsoft Active Directory服务器支持LDAP和LDAPS。其他LDAP实施可能有效、但尚未通过Insight认证。此操作步骤 假定您使用的是Microsoft Active Directory版本2或3 LDAP (轻型目录访问协议)。

LDAP用户与本地定义的用户一起显示在*管理*>菜单：设置[用户]列表中。

步骤

1. 在Insight工具栏上、单击*管理*。
2. 单击*设置*。
3. 单击*用户*选项卡。

4. 滚动到LDAP部分。
5. 单击*启用LDAP*以允许LDAP用户进行身份验证和授权。
6. 填写以下字段：

   ◦ `LDAP servers`：Insight接受以逗号分隔的LDAP URL列表。Insight会尝试连接到提供的URL、而不验证LDAP协议。

   要导入LDAP证书、请单击*证书*、然后自动导入或手动查找证书文件。

   用于标识LDAP服务器的IP地址或DNS名称通常采用以下格式输入：

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

   或者、如果使用默认端口：

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

   + 在此字段中输入多个LDAP服务器时、请确保在每个条目中使用正确的端口号。

   ◦ `User name`：输入在LDAP服务器上有权进行目录查找查询的用户的凭据。

   ◦ `Password`：输入上述用户的密码。要在LDAP服务器上确认此密码、请单击*验证*。

7. 如果要更精确地定义此LDAP用户、请单击*显示更多*并填写列出属性的字段。

   这些设置必须与LDAP域中配置的属性匹配。如果您不确定要为这些字段输入的值、请咨询Active Directory管理员。

   ◦ 管理员组

     具有Insight管理员权限的用户的LDAP组。默认值为 `insight.admins`。

   ◦ 用户组

     具有Insight用户权限的用户的LDAP组。默认值为 `insight.users`。

   ◦ 来宾组

     具有Insight来宾权限的用户的LDAP组。默认值为 `insight.guests`。

   ◦ 服务器管理员组

     具有Insight Server管理员权限的用户的LDAP组。默认值为 `insight.server.admins`。

   ◦ 超时

     超时前等待LDAP服务器响应的时间长度、以毫秒为单位。默认值为2、000、这在所有情况下都是足够的、不应修改。

- 域

  OnCommand Insight 应开始查找LDAP用户的LDAP节点。通常、这是组织的顶级域。例如：

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

- 用户主体名称属性

  用于标识LDAP服务器中每个用户的属性。默认值为 `userPrincipalName`、全局唯一。OnCommand Insight 会尝试将此属性的内容与上述提供的用户名进行匹配。

- 角色属性

  用于确定用户是否适合指定组的LDAP属性。默认值为 `memberOf`。

- 邮件属性

  用于标识用户电子邮件地址的LDAP属性。默认值为 `mail`。如果您要订阅OnCommand Insight 提供的报告、此功能非常有用。Insight会在每个用户首次登录时获取用户的电子邮件地址、之后不会查找该地址。

  ⓘ 如果LDAP服务器上的用户电子邮件地址发生变化、请务必在Insight中对其进行更新。

- 可分辨名称属性

  用于标识用户可分辨名称的LDAP属性。默认值为 `distinguishedName`。

8. 单击 * 保存 * 。