



設定LDAP的Insight OnCommand Insight

NetApp
October 24, 2024

目錄

設定LDAP的Insight	1
使用LDAP設定使用者定義	3

設定LDAP的Insight

必須在公司LDAP網域中設定使用輕量型目錄存取傳輸協定（LDAP）設定OnCommand Insight。

在將Insight設定為搭配LDAP或安全LDAP（LDAPS）使用之前、請先記下公司環境中的Active Directory組態。Insight設定必須符合貴組織LDAP網域組態中的設定。在設定Insight與LDAP搭配使用之前、請先檢閱下列概念、並洽詢您的LDAP網域管理員、以瞭解您環境中要使用的適當屬性。

對於所有安全的Active Directory（即LDAPS）使用者、您必須使用與憑證中定義完全相同的AD伺服器名稱。您無法使用IP位址進行安全的AD登入。



如果您使用變更 `_server.keystore` 和 / 或 `_server.trustore` 密碼"安全性管理"、請在匯入 LDAP 憑證之前重新啟動 SANscreen 服務。



支援透過Microsoft Active Directory伺服器或Azure AD的LDAP和LDAPS OnCommand Insight。其他LDAP實作可能仍可運作、但尚未符合Insight資格。本指南中的程序假設您使用的是Microsoft Active Directory版本2或3 LDAP（輕量型目錄存取傳輸協定）。

使用者主要名稱屬性：

LDAP使用者主要名稱屬性（`userPrincipalName`）是Insight做為使用者名稱屬性的用途。使用者主要名稱保證在Active Directory（AD）樹系中具有全域唯一性、但在許多大型組織中、使用者的主要名稱可能並不立即顯而易見或已知。您的組織可能會針對主要使用者名稱使用User Principal Name屬性以外的其他選項。

以下是使用者主要名稱屬性欄位的一些替代值：

- `* sAMAccountName*`

此使用者屬性是舊版Windows 2000 NT使用者名稱、這是大多數使用者習慣登入其個人Windows機器的方式。這在整個AD樹系中並不保證是全域唯一的。



`SamAccountName`對User主體名稱屬性區分大小寫。

- 郵件

在使用MS Exchange的AD環境中、此屬性是終端使用者的主要電子郵件地址。這應該在整個AD樹系中具有全域唯一性（也適用於終端使用者）、不同於其`userPrincipalName`屬性。郵件屬性不存在於大多數非MS Exchange環境中。

- 推薦

LDAP參照是網域控制器向用戶端應用程式指出它沒有所要求物件的複本（或更精確地說、它不會保留目錄樹狀結構中該物件所在的區段（如果實際上存在）、並提供用戶端較有可能保留該物件的位置。用戶端會使用參照做為DNS搜尋網域控制器的基礎。理想情況下、參照一律會參照確實包含物件的網域控制器。不過、雖然通常不會花很長時間來發現物件不存在、並通知用戶端、但參照網域控制器仍有可能產生另一個參照。



SamAccountName通常比使用者主要名稱更受歡迎。SamAccountName在網域中是唯一的（雖然在網域樹系中可能不是唯一的）、但它是使用者通常用於登入的字串網域（例如、*NetApp\username*）。辨別名稱是樹系中的唯一名稱、但使用者通常不知道。



在同一個網域的Windows系統部分、您可以隨時開啟命令提示字元、然後輸入set以尋找適當的網域名稱（USERDOMAIN=）。然後OCI登入名稱將會是 USERDOMAIN\sAMAccountName。

如需網域名稱* mydomain.x.y.z.com、請使用 DC=x, DC=y, DC=z, DC=com 在Insight的Domain（網域）欄位中。

連接埠：

LDAP的預設連接埠為389、LDAPS的預設連接埠為636

LDAPS的一般URL：`ldaps://<ldap_server_host_name>:636`

記錄位於：`\\<install_directory>\SANscreen\wildfly\standalone\log\ldap.log`

根據預設、Insight會預期下列欄位中所註明的值。如果Active Directory環境中有這些變更、請務必在Insight LDAP組態中加以變更。

角色屬性
成員
郵件屬性
郵件
辨別名稱屬性
區分名稱
推薦
追蹤

群組：

若要驗證OnCommand Insight 使用者在支援對象架構和DWH伺服器中具有不同存取角色、您必須在Active Directory中建立群組、並在OnCommand Insight 支援對象架構和DWH伺服器中輸入這些群組名稱。下列群組名稱僅為範例、您在Insight中為LDAP設定的名稱必須符合為Active Directory環境設定的名稱。

Insight Group	範例
Insight伺服器管理員群組	insight.server.admins

Insight系統管理員群組	Insight。管理員
Insight使用者群組	insight.users
Insight Guest群組	Insight、訪客
報告管理員群組	INSIGHT。report.管理員
報告專業作者群組	insight.report.proauthors
報告作者群組	insight.report.business.authors
報告使用者群組	INSIGHT。report.business。消費者
報告收件者群組	INSIGHT。report.Recipients

使用LDAP設定使用者定義

若要從OnCommand Insight LDAP伺服器設定使用者驗證和授權的功能（OCI）、您必須在LDAP伺服器中定義OnCommand Insight 為「支援伺服器管理員」。

開始之前

您必須知道已在LDAP網域中針對Insight設定的使用者和群組屬性。

對於所有安全的Active Directory（即LDAPS）使用者、您必須使用與憑證中定義完全相同的AD伺服器名稱。您無法使用IP位址進行安全的AD登入。



如果您使用變更 `_server.keystore` 和 / 或 `_server.trustore` 密碼"安全性管理"、請在匯入 LDAP 憑證之前重新啟動 SANscreen 服務。

關於這項工作

支援透過Microsoft Active Directory伺服器的LDAP和LDAPS OnCommand Insight。其他LDAP實作可能仍可運作、但尚未符合Insight資格。此程序假設您使用的是Microsoft Active Directory版本2或3 LDAP（輕量型目錄存取傳輸協定）。

LDAP使用者與本機定義的使用者一起顯示在*管理*>功能表：設定[使用者]清單中。

步驟

1. 在Insight工具列上、按一下*管理*。
2. 按一下*設定*。
3. 按一下「使用者」索引標籤。

4. 捲動至 LDAP 區段。
5. 按一下*「啟用LDAP*」以允許LDAP使用者驗證與授權。
6. 填寫欄位：

- LDAP servers：Insight接受以逗號分隔的LDAP URL列表。Insight會嘗試連線至提供的URL、但不驗證LDAP傳輸協定。



若要匯入LDAP憑證、請按一下*憑證*、然後自動匯入或手動尋找憑證檔案。

用於識別LDAP伺服器的IP位址或DNS名稱通常是以下列格式輸入：

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

或者、如果使用預設連接埠：

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

+ 在此欄位中輸入多個LDAP伺服器時、請確定每個項目都使用正確的連接埠號碼。

- User name：輸入授權用於LDAP伺服器上目錄查詢的使用者認證。
- Password：輸入上述使用者的密碼。若要在LDAP伺服器上確認此密碼、請按一下*驗證*。

7. 如果您想更精確地定義此LDAP使用者、請按一下*顯示更多*、然後填入所列屬性的欄位。

這些設定必須符合LDAP網域中設定的屬性。如果您不確定要輸入這些欄位的值、請洽詢Active Directory管理員。

- 管理員群組

LDAP群組、適用於具有Insight Administrator權限的使用者。預設為 insight.admins。

- 使用者群組

LDAP群組、適用於具有Insight使用者權限的使用者。預設為 insight.users。

- 來賓群組

LDAP群組、適用於具有Insight Guest權限的使用者。預設為 insight.guests。

- 伺服器管理員群組

LDAP群組、適用於具有Insight Server Administrator權限的使用者。預設為 insight.server.admins。

- 超時

在逾時之前等待LDAP伺服器回應的時間長度（以毫秒為單位）。預設值為2、000、在所有情況下都足

夠、不應修改。

- 網域

應從LDAP節點OnCommand Insight 開始尋找LDAP使用者。通常這是組織的頂層網域。例如：

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

- 使用者主要名稱屬性

用於識別LDAP伺服器中每個使用者的屬性。預設為 `userPrincipalName` 是全球獨一無二的。嘗試將此屬性的內容與上述提供的使用者名稱配對OnCommand Insight。

- 角色屬性

可識別使用者符合指定群組的LDAP屬性。預設為 `memberOf`。

- 郵件屬性

用於識別使用者電子郵件地址的LDAP屬性。預設為 `mail`。如果您想訂閱OnCommand Insight 可從下列網站取得的報告、此功能非常實用：Insight會在每位使用者第一次登入時取回使用者的電子郵件地址、之後不會再尋找。



如果使用者的電子郵件地址在LDAP伺服器上變更、請務必在Insight中更新。

- 辨別名稱屬性

識別使用者辨別名稱的LDAP屬性。預設為 `distinguishedName`。

8. 按一下「* 儲存 *」。

版權資訊

Copyright © 2024 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 <http://www.netapp.com/TM> 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。