安全性與認證管理

SnapManager for SAP

NetApp
April 19, 2024

This PDF was generated from https://docs.netapp.com/zh-tw/snapmanager-sap/windows/concept-what-user-authentication-is.html on April 19, 2024. Always check docs.netapp.com for the latest.

目錄

安全性與認證管理

您可以套用使用者驗證來管理SnapManager 功能的安全性。使用者驗證方法可讓您存取資源、例如儲存庫、主機和設定檔。

當您使用命令列介面（CLI）或圖形使用者介面（GUI）執行作業時SnapManager 、即可擷取儲存庫和設定檔的認證資料集。支援儲存先前安裝的認證資料。SnapManager

儲存庫和設定檔可以使用密碼加以保護。認證是為使用者設定的物件密碼、而且不會在物件本身上設定密碼。

您可以執行下列工作來管理驗證和認證：

- 透過操作時的密碼提示或使用「msap認證集」命令來管理使用者驗證。

  設定儲存庫、主機或設定檔的認證。

- 檢視管理您有權存取之資源的認證資料。
- 清除所有資源（主機、儲存庫和設定檔）的使用者認證。
- 刪除個別資源（主機、儲存庫和設定檔）的使用者認證。

> 如果儲存庫資料庫位於Windows主機上、則本機或系統管理員使用者與網域使用者必須擁有相同的認證資料。

什麼是使用者驗證

執行此功能的主機上、使用作業系統（OS）登入來驗證使用者。SnapManager SnapManager您可以透過操作時的密碼提示或使用SMO認證來啟用使用者驗證、您可以在作業時透過密碼提示或使用「msap認證集」來啟用使用者驗證。

使用者驗證需求取決於執行作業的位置。

- 如果SnapManager 該驗證用戶端與SnapManager 該支援主機位於同一部伺服器上、您就會獲得作業系統認證資料的驗證。

  系統不會提示您輸入密碼、因為您已經登入SnapManager 執行此伺服器的主機。

- 如果SnapManager 支援的是不同SnapManager 主機上的支援服務器、SnapManager 那麼就需要用兩個作業系統認證來驗證您的身分。

  如果您尚未將作業系統認證資料儲存在您的支援者認證快取中、則系統會提示您輸入任何作業的密碼。SnapManager SnapManager如果您輸入「shmsap認證集-host'」命令、您會將OS認證儲存在SnapManager 您的「支援資訊」認證快取檔案中、SnapManager 因此、針對任何作業、不會提示輸入密碼。

如果您已通過SnapManager 驗證使用此伺服器、您將被視為有效使用者。任何作業的有效使用者都必須是執行作業的主機上有效的使用者帳戶。例如、如果您執行實體複本作業、應該能夠登入目的地主機以進行實體複本。

SAP的支援可能無法授權在中央Active Directory服務中建立的使用者、例如LDAP和ADS。SnapManager為了確保驗證不會失敗、您必須將可設定的「auth.disableServerAuthorization」設定為* true*。

身為有效使用者、您可以使用下列方式來管理認證：

- 或者、您可以設定SnapManager 將使用者認證資料儲存在SnapManager 靜態使用者認證檔案中。

  根據預設SnapManager 、不儲存主機認證資料。例如、如果您有需要存取遠端主機的自訂指令碼、您可能會想要變更此設定。遠端複製作業是SnapManager 一個需要遠端主機使用者登入認證的功能不穩定作業範例。若要SnapManager 讓使用者主機登入認證資料記住SnapManager 在「支援資訊」使用者認證快取中、請在「smsap.config」檔案中將「host.ecents.persist」屬性設為* true*。

- 您可以授權使用者存取儲存庫。
- 您可以授權使用者存取設定檔。
- 您可以檢視所有使用者認證資料。
- 您可以清除所有資源（主機、儲存庫和設定檔）的使用者認證。
- 您可以刪除個別資源（主機、儲存庫和設定檔）的認證資料。

儲存加密密碼以供自訂指令碼使用

根據預設、SnapManager 不將主機認證資料儲存在使用者認證快取中。不過、您可以變更此設定。您可以編輯「smsap.config」檔案、以便儲存主機認證資料。

關於這項工作

「smsap.config」檔案位於「<預設安裝位置>\properties\smsap.config」

步驟

1. 編輯「smsap.config」檔案。
2. 將「*host.inbentions.f*堅持」設為* true*。

授權存取儲存庫

使用支援的支援功能、您可以設定資料庫使用者存取儲存庫的認證資料。SnapManager使用認證資料、您可以限制或禁止存取SnapManager 「介紹主機」、儲存庫、設定檔和資料庫。

關於這項工作

如果您使用「認證集」命令來設定認證、SnapManager 則不會提示輸入密碼。

您可以在安裝SnapManager 過程中設定使用者認證資料。

步驟

1. 輸入下列命令：

   h.**smsap**認證集**-reposit -dbname** ***repo_service_name*****-host** ***repo_host*****-login-username_[-password_repo_password_]-port** ***repo_port***

授權存取設定檔

使用支援的支援功能、您可以設定設定檔的密碼、以防止未獲授權的存取。SnapManager

步驟

1. 輸入下列命令：

   Check Alignment of PHs>"**smsap**認證集**-profile -name** ***profile_name*****[-password_]**

檢視使用者認證資料

您可以列出您有權存取的主機、設定檔和儲存庫。

步驟

1. 若要列出您有權存取的資源、請輸入下列命令：

   '* smsap認證清單*'

檢視使用者認證的範例

此範例顯示您有權存取的資源。

```
smsap credential list
```

```
Credential cache for OS user "user1":
Repositories:
Host1_test_user@SMSAPREPO/hotspur:1521
Host2_test_user@SMSAPREPO/hotspur:1521
user1_1@SMSAPREPO/hotspur:1521
Profiles:
HSDBR (Repository: user1_2_1@SMSAPREPO/hotspur:1521)
PBCASM (Repository: user1_2_1@SMSAPREPO/hotspur:1521)
HSDB (Repository: Host1_test_user@SMSAPREPO/hotspur:1521) [PASSWORD NOT
SET]
Hosts:
Host2
Host5
```

清除所有主機、儲存庫和設定檔的使用者認證

您可以清除資源（主機、儲存庫和設定檔）的認證快取。這會刪除執行命令之使用者的所有資源認證。清除快取之後、您必須再次驗證認證資料、才能存取這些安全的資源。

步驟

1. 若要清除您的認證資料、請從SnapManager CLI輸入「shmsap認證資料清除」命令、或從SnapManager 該程式碼GUI選取*管理*>*認證資料*>*清除快取*。
2. 結束SnapManager 功能GUI。

> ◦ 如果您已從SnapManager 無法使用的圖形介面上清除認證快取、就不需要離開SnapManager 此圖形介面。
> ◦ 如果您已從SnapManager 無法使用的CLI清除認證快取、則必須重新啟動SnapManager 圖形化介面。
> ◦ 如果您已手動刪除加密的認證檔案、則必須SnapManager 重新啟動該圖形使用者介面。

3. 若要再次設定認證、請重複此程序、為儲存庫、設定檔主機和設定檔設定認證。如需再次設定使用者認證的其他資訊、請參閱「清除認證快取後設定認證」。

清除認證快取後、請設定認證資料

清除快取以移除儲存的使用者認證資料之後、您可以設定主機、儲存庫和設定檔的認證資料。

關於這項工作

您必須確保為先前提供的儲存庫、設定檔主機和設定檔設定相同的使用者認證。設定使用者認證時、會建立加密的認證檔案。

認證檔案位於「C：\Documents and Settings\Administrator\Application Data \NetApp\smsap\3.3.0」。

如果儲存庫下方沒有儲存庫、請從SnapManager 圖形化使用者介面（GUI）執行下列步驟：

步驟

1. 按一下*工作*>*新增現有儲存庫*以新增現有儲存庫。
2. 請執行下列步驟來設定儲存庫的認證：
   a. 在儲存庫上按一下滑鼠右鍵、然後選取*「Open*（開啟*）」。
   b. 在「儲存庫認證」視窗中、輸入使用者認證資料。
3. 請執行下列步驟來設定主機的認證：
   a. 在儲存庫下的主機上按一下滑鼠右鍵、然後選取*「Open*（開啟*）」。
   b. 在「Host Credentials驗證」（主機認證驗證）視窗中、輸入使用者認證資料。
4. 請執行下列步驟來設定設定檔的認證：
   a. 在主機下的設定檔上按一下滑鼠右鍵、然後選取*「Open*（開啟*）」。

b. 在「Profile Credentials驗證」視窗中、輸入使用者認證資料。

刪除個別資源的認證資料

您可以刪除任何一項安全資源的認證資料、例如設定檔、儲存庫或主機。這可讓您只移除一項資源的認證、而非清除所有資源的使用者認證。

刪除儲存庫的使用者認證

您可以刪除認證資料、讓使用者無法再存取特定儲存庫。此命令可讓您只移除一項資源的認證、而非清除所有資源的使用者認證。

步驟

1. 若要刪除使用者的儲存庫認證、請輸入下列命令：

   h.**smsap**認證刪除**-reposit -dbname *repo_service_name*-host *repo_host*-login-username_-port *repo_port***

刪除主機的使用者認證資料

您可以刪除主機的認證資料、讓使用者無法再存取。此命令可讓您只移除一項資源的認證、而非清除所有資源的所有使用者認證。

步驟

1. 若要刪除使用者的主機認證、請輸入下列命令：

   「msap認證刪除-host -name_host_name_-username_-username_」

刪除設定檔的使用者認證

您可以刪除設定檔的使用者認證、讓使用者無法再存取。

步驟

1. 若要刪除使用者的設定檔認證、請輸入下列命令：

   ‘* smsap認證刪除-profile -name *profile_name**’

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 保留隨時變更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。