準備安裝SnapCenter 完此伺服器

SnapCenter Software 4.9

NetApp
March 20, 2024

目錄

準備安裝SnapCenter 完此伺服器

網域與工作群組需求

可以在網域或工作群組中的系統上安裝此伺服器SnapCenter 。在工作群組和網域的情況下、用於安裝的使用者應該擁有機器的管理權限。

若要在SnapCenter Windows主機上安裝Sfor Server和SnapCenter Sof the plug-ins、您應該使用下列其中一項：

- * Active Directory網域*

  您必須使用具有本機系統管理員權限的網域使用者。網域使用者必須是Windows主機上本機系統管理員群組的成員。

- 工作群組

  您必須使用具有本機系統管理員權限的本機帳戶。

雖然支援網域信任、多網域樹系和跨網域信任、但不支援跨樹系網域。Microsoft的Active Directory網域及信任相關文件包含更多資訊。

安裝SnapCenter 完支援服務器後、您不應變更SnapCenter 支援該主機的網域。如果您從SnapCenter 安裝了支援服務器的網域中移除此伺服器主機SnapCenter 、然後嘗試解除安裝SnapCenter 支援服務器、則解除安裝作業會失敗。

空間與規模需求

安裝SnapCenter 完此伺服器之前、您應該先熟悉空間和規模需求。您也應該套用可用的系統和安全性更新。

項目	需求
作業系統	Microsoft Windows 僅支援英文、德文、日文及簡體中文版的作業系統。 如需支援版本的最新資訊、請參閱 "NetApp 互通性對照表工具"。
最小CPU數	4核心
最低RAM	8 GB MySQL伺服器緩衝資源池使用總RAM的20%。

項目	需求
不需佔用SnapCenter 太多硬碟空間、即可容納整個伺服器軟體和記錄	4 GB 如果SnapCenter 您在SnapCenter 安裝了S什麼 伺服器的同一個磁碟機上有這個版本的資訊庫、建議您使用10 GB的容量。
不需SnapCenter 佔用太多硬碟空間	6 GB 附註：如果SnapCenter 您在SnapCenter 安裝了該系統資訊庫的同一個磁碟機中安裝了該伺服器、則建議您使用10 GB的容量。
必要的軟體套件	• Microsoft .NET Framework 4.7.2 或更新版本 • Windows管理架構（WMF4.0或更新版本） • PowerShell 4.0或更新版本 如需 .NET 特定疑難排解資訊、請參閱 "對於沒有網際網路連線的舊版系統、 SnapCenter 升級或安裝失敗"。

SAN 主機需求

如果SnapCenter 您的支援主機是FC/iSCSI環境的一部分、您可能需要在系統上安裝額外的軟體、才能存取ONTAP 該儲存設備。

不包括主機公用程式或DSM。SnapCenter如果SnapCenter 您的支援對象是SAN環境的一部分、您可能需要安裝及設定下列軟體：

- 主機公用程式

  主機公用程式支援FC和iSCSI、可讓您在Windows伺服器上使用MPIO。 如需相關資訊、請參閱 "主機公用程式文件"。

- 適用於Windows MPIO的Microsoft DSM

  此軟體可搭配Windows MPIO驅動程式使用、以管理NetApp與Windows主機電腦之間的多個路徑。

  高可用度組態需要DSM。

  如果您使用ONTAP 的是功能不實的DSM、則應移轉至Microsoft DSM。如需詳細資訊、請參閱 "如何從ONTAP 功能需求DSM移轉至Microsoft DSM"。

支援的儲存系統與應用程式

您應該知道支援的儲存系統、應用程式和資料庫。

- 支援不支援更新版本的支援功能、可保護您的資料。SnapCenter ONTAP
- 支援Amazon FSX for NetApp功能、保護資料不受來自於更新版的支援。SnapCenter ONTAP SnapCenter

  如果您使用Amazon FSX for NetApp ONTAP Sfor NetApp的話、請確保SnapCenter 將支援此功能的支援伺服器主機外掛程式升級至4.5 P1或更新版本、以執行資料保護作業。

  如需Amazon FSX for NetApp ONTAP 功能的相關資訊、請參閱 "Amazon FSX for NetApp ONTAP 的支援文件"。

- 支援不同應用程式和資料庫的保護。SnapCenter

  如需支援的應用程式和資料庫詳細資訊、請參閱 "NetApp 互通性對照表工具"。

- SnapCenter 4.9 P1 及更新版本支援在 VMware Cloud on Amazon Web Services （ AWS ）軟體定義資料中心（ SDDC ）環境中保護 Oracle 和 Microsoft SQL 工作負載。

  如需詳細資訊、請參閱 "在 AWS SDDC 環境中使用 VMware Cloud 中的 NetApp SnapCenter 來保護 Oracle 、 MS SQL 工作負載"。

支援的瀏覽器

可在多個瀏覽器上使用此軟體。SnapCenter

- Chrome

  如果您使用的是v66、可能無法啟動SnapCenter vsGUI。

- Internet Explorer

  如果您使用的是IE 10或更早版本、則無法正確載入此程式。SnapCenter您應該升級至IE 11。

  - 僅支援預設層級的安全性。

    變更Internet Explorer安全性設定會導致瀏覽器顯示出現重大問題。

  - 必須停用Internet Explorer相容性檢視。

- Microsoft Edge

如需支援版本的最新資訊、請參閱 "NetApp 互通性對照表工具"。

連線與連接埠需求

在安裝SnapCenter 完還原伺服器和應用程式或資料庫外掛程式之前、您應確保符合連線和連接埠的要求。

- 應用程式無法共用連接埠。

  每個連接埠都必須專供適當的應用程式使用。

- 對於可自訂的連接埠、如果您不想使用預設連接埠、可以在安裝期間選取自訂連接埠。

  您可以使用「修改主機」精靈、在安裝後變更外掛程式連接埠。

- 對於固定連接埠、您應該接受預設的連接埠號碼。
- 防火牆
  - 防火牆、Proxy或其他網路裝置不應干擾連線。
  - 如果您在安裝SnapCenter 時指定自訂連接埠、則應在外掛主機上新增防火牆規則、以供SnapCenter 該連接埠用於「支援程式載入器」。

下表列出不同的連接埠及其預設值。

連接埠類型	預設連接埠
連接埠SnapCenter	8146 （ HTTPS ）、雙向、可自訂、如同 URL https://server:8146_ 中所列 用於SnapCenter 在客戶端（SnapCenter 不知使用者）和SnapCenter 伺服器之間進行通訊。也可用於從外掛程式主機到SnapCenter 該伺服器的通訊。 若要自訂連接埠、請參閱 "使用安裝精靈安裝 SnapCenter 伺服器。"
WSSMCore通訊連接埠SnapCenter	8145（HTTPS）、雙向、可自訂 連接埠用於SnapCenter 在Sfor the Sfor Server 和SnapCenter 安裝了該插件的主機之間進行通訊。 若要自訂連接埠、請參閱 "使用安裝精靈安裝 SnapCenter 伺服器。"
MySQL連接埠	3306（HTTPS）、雙向 連接埠用於SnapCenter 在不同時執行的情況下、與MySQL儲存庫資料庫進行通訊。 您可以建立安全的連線、從SnapCenter 「伺服器」到MySQL伺服器。 "深入瞭解" 若要自訂連接埠、請參閱 "使用安裝精靈安裝 SnapCenter 伺服器。"

連接埠類型	預設連接埠
Windows外掛程式主機	135、445（TCP） 除了連接埠135和445之外、Microsoft指定的動態連接埠範圍也應該開啟。遠端安裝作業使用Windows Management Instrumentation（WMI）服務、此服務會動態搜尋此連接埠範圍。 如需支援的動態連接埠範圍資訊、請參閱 "Windows的服務總覽和網路連接埠需求" 連接埠可用於SnapCenter 在安裝外掛程式的伺服器與主機之間進行通訊。若要將外掛程式套件二進位檔推送至Windows外掛程式主機、連接埠只能在外掛程式主機上開啟、而且可以在安裝後關閉。
Linux或AIX外掛程式主機	22（SSH） 連接埠用於SnapCenter 在安裝外掛程式的伺服器與主機之間進行通訊。這些連接埠是SnapCenter 由效能資料所使用、可將外掛套件二進位檔複製到Linux或AIX外掛程式主機、並應開啟或排除在防火牆或iptables之外。
適用於Windows的程式集外掛套件、適用於Linux的程式集外掛套件或適用於AIX的程式集外掛套件SnapCenter SnapCenter SnapCenter	8145（HTTPS）、雙向、可自訂 連接埠用於SMCore與安裝外掛程式套件的主機之間的通訊。 SVM管理LIF與SnapCenter SVM管理伺服器之間的通訊路徑也必須開放。 若要自訂連接埠、請參閱 "新增主機並安裝SnapCenter適用於Microsoft Windows的解決方案" 或 "新增主機並安裝適用於 Linux 或 AIX 的 SnapCenter 外掛程式套件。"
Oracle資料庫的支援外掛程式SnapCenter	27216、可自訂 Oracle的外掛程式會使用預設的JDBC連接埠來連線至Oracle資料庫。 若要自訂連接埠、請參閱 "新增主機並安裝適用於 Linux 或 AIX 的 SnapCenter 外掛程式套件。"

連接埠類型	預設連接埠
客製SnapCenter 化的外掛程式	9090（HTTPS）、已修正 這是僅用於自訂外掛程式主機的內部連接埠、不需要防火牆例外。 透過連接埠8145、即可在伺服SnapCenter 器與自訂外掛程式之間進行通訊。
叢集或SVM通訊連接埠ONTAP	443（HTTPS）、biddirectional80（HTTP）、雙向 此連接埠由SAL（Storage Abstraction Layer、Storage Abstraction Layer）使用、用於執行SnapCenter 支援服務器和SVM的主機之間的通訊。此連接埠目前也用於SnapCenter Windows外掛程式主機上的SAL、用於SnapCenter 在支援該外掛程式的主機和SVM之間進行通訊。
SAP HANA資料庫適用的插件vCode Spell Checkerport SnapCenter	3執行個體編號13或3執行個體編號15、HTTP或HTTPS、雙向且可自訂 對於多租戶資料庫容器（MDC）單一租戶、連接埠編號以13結尾；對於非MDC、連接埠編號以15結尾。 例如、32013是連接埠編號、例如20、31015是連接埠編號、例如10。 若要自訂連接埠、請參閱 "新增主機並在遠端主機上安裝外掛程式套件。"
網域控制器通訊連接埠	請參閱Microsoft文件以識別應在網域控制器防火牆中開啟的連接埠、以便驗證正常運作。 您必須開啟網域控制器上的Microsoft必要連接埠、SnapCenter 才能讓支援服務器、外掛程式主機或其他Windows用戶端驗證使用者。

若要修改連接埠詳細資料、請參閱 "修改外掛程式主機"。

不需要授權SnapCenter

支援多個授權、以保護應用程式、資料庫、檔案系統和虛擬機器的資料。SnapCenter安裝的不完整授權類型SnapCenter 取決於您的儲存環境和您想要使用的功能。

授權	必要時
以標準控制器為基礎SnapCenter	FAS 、 AFF 、 All SAN Array （ASA）所需的 不含不含控制器型授權的優質套裝組合。SnapCenter 如果您擁有SnapManager 此產品的不支援功能、您也可以取得SnapCenter 「不支援即用」的授權。如果您想要試用 FAS 、 AFF 或 ASA 儲存設備來安裝 SnapCenter 、請聯絡銷售代表以取得優質產品組合評估授權。 此外、也提供資料保護套裝組合的一部分。SnapCenter如果您已購買A400或更新版本、則應購買資料保護套裝組合。
以容量為基礎的標準SnapCenter	需要搭配使用ONTAP Select Cloud Volumes ONTAP 如果Cloud Volumes ONTAP 您是一個不知道或ONTAP Select 不知道的客戶、您必須根據SnapCenter 由支援的資料、購買每TB容量型授權。根據預設SnapCenter 、不含內建90天100 TB SnapCenter 的功能型試用授權。如需其他詳細資料、請聯絡銷售代表。
SnapMirror或SnapVault	ONTAP 如果在功能區啟用複寫、則需要SnapMirror或SnapVault 不含任何資訊的授權SnapCenter 。
SnapRestore	還原及驗證備份所需的。 在主要儲存系統上 • 需要在SnapVault 目的地系統上執行遠端驗證、以及從備份還原。 • SnapMirror目的地系統需要執行遠端驗證。
FlexClone	複製資料庫和驗證作業所需的。 在一線和二線儲存系統上 • 需要在SnapVault 目的地系統上、從次要資料庫備份建立複本。 • SnapMirror目的地系統需要從次要SnapMirror備份建立複本。

授權	必要時
通訊協定	• LUN的iSCSI或FC授權 • 適用於SMB共用的CIFS授權 • NFS類型VMDK的NFS授權 • 適用於VMFS類型VMDK的iSCSI或FC授權 SnapMirror目的地系統需要在來源磁碟區無法使用時提供資料。
不含標準授權（選用）SnapCenter	次要目的地 我們建議您將SnapCenter 不需要的「不二用」授權新增至次要目的地。如果SnapCenter 在次要目的地上未啟用「支援支援功能」、SnapCenter 則在執行容錯移轉作業之後、您將無法使用「支援功能」在次要目的地上備份資源。不過、次要目的地需要FlexClone授權才能執行複製與驗證作業。

不再提供「進階」和「不適用的NAS檔案服務」授權。SnapCenter SnapCenter

您應該安裝一SnapCenter 或多個版本的不二授權。如需如何新增授權的資訊、請參閱 "新增SnapCenter 以控制器為基礎的功能" 或 "新增SnapCenter 以功能為基礎的「功能型標準」授權"。

單一信箱恢復（SMBR）授權

如果您使用SnapCenter Exchange的還原外掛程式來管理Microsoft Exchange Server資料庫和單一信箱恢復（SMBR）、則您需要額外的SMBR授權、而此授權必須根據使用者信箱另行購買。

NetApp ® 單一信箱恢復已於 2023 年 5 月 12 日結束可用度（ EOA ）。如需詳細資訊、請參閱 "CPS-00507"。NetApp 將持續支援已於 2020 年 6 月 24 日推出的行銷零件編號、以支援購買信箱容量、維護和支援的客戶。

NetApp 單一信箱恢復是 Ontrack 提供的合作夥伴產品。Ontrack PowerControl 提供的功能與 NetApp 單一信箱恢復功能類似。客戶可從 Ontrack （透過 licensingteam@ontrack.com ）取得新的 Ontrack PowerControl 軟體授權、以及 Ontrack PowerControl 的維護與支援續約、以便在 2023 年 5 月 12 日結束後進行精細信箱恢復。

認證方法

認證資料會根據應用程式或環境使用不同的驗證方法。認證資料會驗證使用者、讓他們能夠執行SnapCenter 功能不中斷的作業。您應該建立一組認證來安裝外掛程式、並建立另一組用於資料保護作業的認證。

Windows驗證

Windows驗證方法會根據Active Directory進行驗證。對於Windows驗證、Active Directory是設定在SnapCenter非功能性的環境中。無需額外組態即可驗證。SnapCenter您需要Windows認證來執行新增主機、安裝外掛程式套件及排程工作等工作。

不受信任的網域驗證

支援使用不受信任網域的使用者和群組來建立Windows認證。SnapCenter若要驗證成功、您應該使用SnapCenter NetApp註冊不受信任的網域。

本機工作群組驗證

支援與本機工作群組使用者和群組一起建立Windows認證。SnapCenter本機工作群組使用者和群組的Windows驗證不會在Windows認證建立時進行、而是延後至執行主機登錄和其他主機作業為止。

SQL Server驗證

SQL驗證方法會針對SQL Server執行個體進行驗證。這表示SQL Server執行個體必須在SnapCenter 支援中發現。因此、在新增SQL認證之前、您必須先新增主機、安裝外掛程式套件、以及重新整理資源。您需要SQL Server驗證才能執行作業、例如在SQL Server上排程或探索資源。

Linux驗證

Linux驗證方法會針對Linux主機進行驗證。您需要在新增Linux主機並從SnapCenter 支援程式介面從遠端安裝適用於Linux的支援程式套件的初始步驟中進行Linux驗證SnapCenter 。

AIX 驗證

AIX驗證方法會針對AIX主機進行驗證。在新增AIX主機並從SnapCenter 支援程式GUI遠端安裝適用於AIX的支援程式套件的初始步驟中、您需要AIX驗證SnapCenter 。

Oracle資料庫驗證

Oracle資料庫驗證方法會根據Oracle資料庫進行驗證。如果在資料庫主機上停用作業系統（OS）驗證、您需要Oracle資料庫驗證才能在Oracle資料庫上執行作業。因此、在新增Oracle資料庫認證之前、您應該先在Oracle資料庫中建立具有Sysdba權限的Oracle使用者。

Oracle ASM驗證

Oracle ASM驗證方法會針對Oracle自動儲存管理（ASM）執行個體進行驗證。如果您需要存取Oracle ASM執行個體、而且資料庫主機上的作業系統（OS）驗證已停用、則需要Oracle ASM驗證。因此、在新增Oracle ASM認證之前、您應該先在ASM執行個體中建立具有Sysasm權限的Oracle使用者。

RMAN目錄驗證

RMAN目錄驗證方法會根據Oracle Recovery Manager（RMAN）目錄資料庫進行驗證。如果您已設定外部目錄機制並將資料庫登錄至目錄資料庫、則需要新增RMAN目錄驗證。

儲存連線與認證

在執行資料保護作業之前、您應該先設定儲存連線、並新增SnapCenter 功能、以供使用。SnapCenter

- 儲存連線

  儲存連線可讓SnapCenter Sfor Sfor Server和SnapCenter Sfor插座存取ONTAP 功能豐富的功能。設定這些連線時、也需要設定AutoSupport 功能性的功能性和事件管理系統（EMS）。

- 認證

  - 網域管理員或系統管理員群組的任何成員

    在您要安裝SnapCenter 此插件的系統上、指定網域管理員或任何系統管理員群組成員。「使用者名稱」欄位的有效格式為：

    - *netbios*\使用者名稱
    - 網域FQDN \使用者名稱_
    - *username@UPN*

  - 本機管理員（僅適用於工作群組）

    對於屬於工作群組的系統、請在安裝SnapCenter 此插件的系統上指定內建的本機管理員。如果使用者帳戶擁有較高的權限、或主機系統上的使用者存取控制功能已停用、您可以指定屬於本機系統管理員群組的本機使用者帳戶。

  「使用者名稱」欄位的有效格式為：*username*

  - 個別資源群組的認證資料

    如果您為個別資源群組設定認證、但使用者名稱沒有完整的管理權限、則必須至少將資源群組和備份權限指派給使用者名稱。

多因素驗證（**MFA**）

管理多因素驗證（ **MFA** ）

您可以在 Active Directory Federation Service （ AD FS ）伺服器和 SnapCenter 伺服器中管理多因素驗證（ MFA ）功能。

啟用多因素驗證（ **MFA** ）

您可以使用 PowerShell 命令為 SnapCenter 伺服器啟用 MFA 功能。

關於這項工作

- 在相同的AD FS中設定其他應用程式時、支援SSO型登入。SnapCenter在某些AD FS組態中、SnapCenter由於安全原因、可能需要使用者驗證、視AD FS工作階段持續性而定。

- 執行即可取得可搭配 Cmdlet 使用之參數的相關資訊及其說明 `Get-Help command_name`。或者、您也可以參閱 "《軟件指令程式參考指南》SnapCenter"。

開始之前

- Windows Active Directory Federation Service（AD FS）應在各自的網域中啟動並執行。
- 您應該擁有 AD FS 支援的多因素驗證服務、例如 Azure MFA 、 Cisco Duo 等。
- 無論時區為何、均應使用相同的資訊區和AD FS伺服器時間戳記。SnapCenter
- 取得SnapCenter 並設定驗證伺服器的授權CA憑證。

  CA憑證為必填、原因如下：

  - 確保 ADFS-F5 通訊不會中斷、因為自我簽署的憑證在節點層級是唯一的。
  - 確保在獨立式或高可用度組態的升級、修復或災難恢復（DR）期間、不會重新建立自我簽署的憑證、因此可避免重新設定MFA。
  - 確保IP FQDN解析度。

    如需CA憑證的相關資訊、請參閱 "產生CA認證CSR檔案"。

步驟

1. 連線至Active Directory Federation Services（AD FS）主機。
2. 從下載AD FS聯盟中繼資料檔案 "https://<host fqfq>/ 聯邦中繼資料 /2007/06/Federation中繼 資料 .xml" 。
3. 將下載的檔案複製到SnapCenter 支援MFA功能的伺服器。
4. 透過PowerShell以「管理員」使用者身分登入SnapCenter 到「伺服器」SnapCenter 。
5. 使用PowerShell工作階段SnapCenter 、使用_New-SmMultifactorAuthenticationMetadata -path_ Cmdlet來產生FismFA中繼資料檔案。

   path參數指定將MFA中繼資料檔案儲存到SnapCenter Sof the Server主機的路徑。

6. 將產生的檔案複製到AD FS主機、以設定SnapCenter 將SURE做為用戶端實體。
7. 使用為 SnapCenter 伺服器啟用 MFA `Set-SmMultiFactorAuthentication` Cmdlet。
8. （選用）使用檢查 MFA 組態狀態和設定 `Get-SmMultiFactorAuthentication` Cmdlet。
9. 前往Microsoft管理主控台（MMC）並執行下列步驟：
   a. 按一下*檔案*>*新增/移除Snapin *。
   b. 在「新增或移除嵌入式管理單元」視窗中、選取「憑證」、然後按一下「新增」。
   c. 在「憑證」嵌入式管理單元視窗中、選取「電腦帳戶」選項、然後按一下「完成」。
   d. 按一下*主控台根目錄*>*憑證–本機電腦*>*個人*>*憑證*。
   e. 在繫結SnapCenter 至SUn供 參考的CA憑證上按一下滑鼠右鍵、然後選取*所有工作*>*管理私密金鑰*。
   f. 在權限精靈上執行下列步驟：
      i. 按一下「 * 新增 * 」。
      ii. 按一下 * 位置 * 、然後選取相關主機（階層架構頂端）。

iii. 在*位置*快顯視窗中按一下*確定*。

iv. 在物件名稱欄位中、輸入「IIS_IUSRS」、然後按一下*檢查名稱*、再按一下*確定*。

如果檢查成功、請按一下「確定」。

10. 在AD FS主機中、開啟AD FS管理精靈、然後執行下列步驟：
    a. 右鍵點選*信賴廠商信任*>*新增信賴廠商信任*>*開始*。
    b. 選取第二個選項、然後瀏覽SnapCenter 「Some MFA中繼資料」檔案、然後按一下「* Next*（下一步）」。
    c. 指定顯示名稱、然後按一下*「下一步*」。
    d. 視需要選擇存取控制原則、然後按一下 * 下一步 * 。
    e. 在下一個索引標籤中選取預設值。
    f. 單擊*完成*。

    目前以依賴方的形式呈現提供的顯示名稱。SnapCenter

11. 選取名稱並執行下列步驟：
    a. 按一下*編輯請款發放政策*。
    b. 單擊* Add Rule（添加規則），然後單擊 Next*（下一步*）。
    c. 指定宣告規則的名稱。
    d. 選擇* Active Directory *作為屬性儲存區。
    e. 選取「使用者-主要名稱」屬性、並選取傳出的報銷類型為*名稱- ID*。
    f. 單擊*完成*。
12. 在ADFS伺服器上執行下列PowerShell命令。

```
Set-AdfsRelyingPartyTrust -TargetName '<Display name of relying party >'
-SigningCertificateRevocationCheck None

Set-AdfsRelyingPartyTrust -TargetName '<Display name of relying party >'
-EncryptionCertificateRevocationCheck None
```

13. 請執行下列步驟、確認中繼資料已成功匯入。
    a. 在依賴方信任上按一下滑鼠右鍵、然後選取*內容*。
    b. 確認已填入端點、識別項和簽名欄位。
14. 關閉所有瀏覽器索引標籤、然後重新開啟瀏覽器、以清除現有或作用中的工作階段 Cookie 、然後再次登入。

也可使用REST API來啟用「支援MFA」功能。SnapCenter

如需疑難排解資訊、請參閱 "在多個索引標籤中同時嘗試登入會顯示 MFA 錯誤"。

更新**AD FS MFA**中繼資料

只要AD FS伺服器有任何修改、例如升級、CA憑證續約、DR等、您就應該更新SnapCenter 位於支援區的AD FS MFA中繼資料。

步驟

1. 從下載AD FS聯盟中繼資料檔案 "https://<host Fqd>>/資料中繼資料/2007/06/FedationMetadata。XML」
2. 將下載的檔案複製SnapCenter 到「伺服器」以更新MFA組態。
3. 執行下列Cmdlet來更新SnapCenter Sf1中的AD FS中繼資料：

   ```
   Set-SmMultiFactorAuthentication -Path <location of ADFS MFA metadata xml file>
   ```

4. 關閉所有瀏覽器索引標籤、然後重新開啟瀏覽器、以清除現有或作用中的工作階段 Cookie 、然後再次登入。

更新**SnapCenter** 功能不支援**MFA**中繼資料

每當有任何修改ADFS伺服器（例如修復、CA憑證續約、DR等）時、您就應該更新SnapCenter AD FS中的功能完善的MFA中繼資料。

步驟

1. 在AD FS主機中、開啟AD FS管理精靈、然後執行下列步驟：
   a. 按一下*信賴廠商信任*。
   b. 在建立SnapCenter 的依賴方信任上按一下滑鼠右鍵、然後按一下「刪除」。

      隨即顯示使用者定義的信賴關係人信任名稱。

   c. 啟用多因素驗證（MFA）。

      請參閱 "啟用多因素驗證"。

2. 關閉所有瀏覽器索引標籤、然後重新開啟瀏覽器、以清除現有或作用中的工作階段 Cookie 、然後再次登入。

停用多因素驗證（**MFA**）

步驟

1. 停用 MFA 、並清除使用啟用 MFA 時所建立的組態檔案 `Set-SmMultiFactorAuthentication` Cmdlet。
2. 關閉所有瀏覽器索引標籤、然後重新開啟瀏覽器、以清除現有或作用中的工作階段 Cookie 、然後再次登入。

使用 **REST API** 、 **PowerShell** 和 **sccli** 來管理多因素驗證（ **MFA** ）

瀏覽器、 REST API 、 PowerShell 和 sccli 支援 MFA 登入。MFA 可透過 AD FS 身分識別管理員提供支援。您可以從 GUI 、 REST API 、 PowerShell 和 sccli 啟用 MFA 、停用 MFA 、以及設定 MFA 。

將 **AD FS** 設定為 **OAUTH/OIDC**

- 使用 Windows GUI 精靈 * 設定 AD FS
  1. 瀏覽至 * 伺服器管理員儀表板 * > * 工具 * > * ADFS 管理 * 。
  2. 瀏覽至 **ADFS** > * 應用程式群組 * 。
     a. 在 * 應用程式群組 * 上按一下滑鼠右鍵。
     b. 選取 * 新增應用程式群組 * 、然後輸入 * 應用程式名稱 * 。
     c. 選取 * 伺服器應用程式 * 。
     d. 單擊 * 下一步 * 。
  3. 複本 * 用戶端識別碼 * 。

     這是用戶端 ID 。 …在重新導向 URL 中新增回撥 URL （ SnapCenter 伺服器 URL ）。 …單擊 * 下一步 * 。
  4. 選取 * 產生共用密碼 * 。

     複製機密值。這是用戶端的秘密。 …單擊 * 下一步 * 。
  5. 在 * 摘要 * 頁面上、按一下 * 下一步 * 。
     a. 在 * 完整 * 頁面上、按一下 * 關閉 * 。
  6. 右鍵單擊新添加的 * 應用程序組 * ，然後選擇 * 屬性 * 。
  7. 從應用程式內容中選取 * 新增應用程式 * 。
  8. 按一下 * 新增應用程式 * 。

     選取「網路 API 」、然後按一下「 * 下一步 * 」。
  9. 在「設定 Web API 」頁面上、在「識別碼」區段中、輸入上一步所建立的 SnapCenter 伺服器 URL 和用戶端識別碼。
     a. 按一下「 * 新增 * 」。
     b. 單擊 * 下一步 * 。
  10. 在 * 選擇存取控制原則 * 頁面上、根據您的需求選擇控制原則（例如、允許所有人並要求 MFA ）、然後按一下 * 下一步 * 。
  11. 在「 * 設定應用程式權限 * 」頁面上、依預設會選取 OpenID 作為範圍、按一下 * 下一步 * 。
  12. 在 * 摘要 * 頁面上、按一下 * 下一步 * 。

      在 * 完整 * 頁面上、按一下 * 關閉 * 。
  13. 在 * 範例應用程式內容 * 頁面上、按一下 * 確定 * 。
  14. 由授權伺服器（ AD FS ）發出的 JWT 權杖、並打算由資源使用。

      此權杖的「 aud 」或「 Audience 」宣告必須符合資源或 Web API 的識別碼。
  15. 編輯選取的 WebAPI 、並檢查回撥 URL （ SnapCenter 伺服器 URL ）和用戶端識別碼是否正確新增。

設定 OpenID Connect 以提供宣告的使用者名稱。

16. 開啟位於伺服器管理員右上角 * 工具 * 功能表下的 * AD FS 管理 * 工具。
    a. 從左側側欄中選擇 * 應用程式群組 * 資料夾。
    b. 選取 Web API 、然後按一下 * 編輯 * 。
    c. 前往「發行轉換規則」標籤
17. 按一下*新增規則*。
    a. 在請款規則範本下拉式清單中、選取 * 將 LDAP 屬性傳送為請款 * 。
    b. 單擊 * 下一步 * 。
18. 輸入 * 請款規則 * 名稱。
    a. 在屬性儲存區下拉式清單中選取 * Active Directory* 。
    b. 在 **LDAP Attribute** 下拉列表中選擇 **User-Princie-Name** ，在 o*utGo Claim Type* 下拉列表中選擇 **UPN** 。
    c. 單擊*完成*。

使用 **PowerShell** 命令建立應用程式群組

您可以使用 PowerShell 命令建立應用程式群組、 Web API 、並新增範圍和宣告。這些命令以自動指令碼格式提供。如需詳細資訊、請參閱 <link to KB article> 。

1. 使用下列組合在 AD FS 中建立新的應用程式群組。

```
New-AdfsApplicationGroup -Name $ClientRoleIdentifier
-ApplicationGroupIdentifier $ClientRoleIdentifier
```

`ClientRoleIdentifier` 應用程式群組的名稱

`redirectURL` 授權後重新導向的有效 URL

2. 建立 AD FS 伺服器應用程式並產生用戶端機密。

```
Add-AdfsServerApplication -Name "$ClientRoleIdentifier - Server app"
-ApplicationGroupIdentifier $ClientRoleIdentifier -RedirectUri $redirectURL
-Identifier $identifier -GenerateClientSecret
```

3. 建立 ADFS Web API 應用程式、並設定其應使用的原則名稱。

```
$identifier = (New-Guid).Guid

Add-AdfsWebApiApplication -ApplicationGroupIdentifier $ClientRoleIdentifier
-Name "App Web API"

-Identifier $identifier -AccessControlPolicyName "Permit everyone"
```

4. 從下列命令的輸出中取得用戶端 ID 和用戶端機密、因為只會顯示一次。

```
"client_id = $identifier"
```

```
"client_secret: "$($ADFSApp.ClientSecret)
```

5. 將 allats補助 和 OpenID 權限授予 AD FS 應用程式。

```
Grant-AdfsApplicationPermission -ClientRoleIdentifier $identifier
-ServerRoleIdentifier $identifier -ScopeNames @('openid')

$transformrule = @"

@RuleTemplate = "LdapClaims"

@RuleName = "AD User properties and Groups"

c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname",
Issuer ==

"AD AUTHORITY"]

⇒ issue(store = "Active Directory", types =
("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"), query =
";userPrincipalName;{0}", param = c.Value);

"@
```

6. 寫出轉換規則檔案。

```
$transformrule |Out-File -FilePath .\issueancetransformrules.tmp -force
-Encoding ascii $relativePath = Get-Item .\issueancetransformrules.tmp
```

7. 命名 Web API 應用程式、並使用外部檔案定義其「發行轉換規則」。

```
Set-AdfsWebApiApplication -Name "$ClientRoleIdentifier - Web API"
-TargetIdentifier

$identifier -Identifier $identifier,$redirectURL -IssuanceTransformRulesFile

$relativePath
```

更新存取權杖到期時間

您可以使用 PowerShell 命令更新存取權杖到期時間。

關於此工作

- 存取權杖只能用於使用者、用戶端和資源的特定組合。存取權杖無法撤銷、且在過期前有效。
- 依預設、存取權杖的到期時間為 60 分鐘。 這段最短的到期時間已足夠且已調整。您必須提供足夠的價值、以避免任何持續進行的業務關鍵工作。

步驟

若要更新應用程式群組 WebApi 的存取權杖到期時間、請在 AD FS 伺服器中使用下列命令。

+ `Set-AdfsWebApiApplication -TokenLifetime 3600 -TargetName "<Web API>"`

從 **AD FS** 取得承載權杖

您應該在任何 REST 用戶端（例如 Postman ）中填入下列參數、並提示您填寫使用者認證。此外、您應該輸入第二因素驗證（您擁有的東西和您的東西）來取得承載權杖。

+ 承載權杖的有效性可從 AD FS 伺服器根據應用程式進行設定、預設的有效期為 60 分鐘。

欄位	價值
授與類型	授權代碼
回撥 URL	如果您沒有回撥 URL 、請輸入應用程式的基礎 URL 。
驗證 URL	[ADFS- 網域名稱]/ADFS/OAuth2/Authorize
存取權杖 URL	[ADFS- 網域名稱]/ADFS/OAuth2/token
用戶端ID	輸入 AD FS 用戶端 ID
用戶端機密	輸入 AD FS 用戶端機密
範圍	OpenID
用戶端驗證	以基本驗證標頭傳送
資源	在 **Advance Options** 標籤中、新增與 Callback URL 值相同的資源欄位、此值在 JWT Token 中會顯示為「 aud 」值。

使用 **PowerShell** 、 **sccli** 和 **REST API** 在 **SnapCenter** 伺服器中設定 **MFA**

您可以使用 PowerShell 、 sccli 和 REST API 在 SnapCenter 伺服器中設定 MFA 。

SnapCenter MFA CLI 驗證

在 PowerShell 和 sccli 中、現有的 Cmdlet （ Open-SmConnection ）會以另一個稱為「 AccessToken 」的欄位來延伸、以使用承載權杖來驗證使用者。

```
Open-SmConnection -Credential <PSCredential> [-SMSbaseUrl <String>] [-Port
<String>] [-RoleName <String>] [ -AccessToken <string>]
```

執行上述 Cmdlet 之後 , 會建立工作階段 , 讓個別使用者進一步執行 SnapCenter Cmdlet 。

SnapCenter MFA REST API 驗證

在 REST API 用戶端（例如 Postman 或 swagger ）中使用 _Authorization=B承載 <access token> 格式的承載權杖、並在標頭中提及使用者 RoleName 、以取得 SnapCenter 的成功回應。

MFA REST API 工作流程

當 MFA 設定為 AD FS 時、您應該使用存取（承載）權杖進行驗證、以便透過任何 REST API 存取 SnapCenter 應用程式。

關於此工作

- 您可以使用任何 REST 用戶端、例如 Postman 、 Swagger UI 或 Fireplane 。
- 取得存取權杖、並使用它來驗證後續要求（ SnapCenter REST API ）以執行任何作業。

步驟

- 透過 AD FS MFA * 驗證
  1. 設定 REST 用戶端呼叫 AD FS 端點以取得存取權杖。

     當您按下按鈕以取得應用程式的存取權杖時、系統會將您重新導向至 AD FS SSO 頁面、您必須在其中提供 AD 認證並驗證 MFA 。 1. 在 AD FS SSO 頁面的「使用者名稱」文字方塊中、輸入您的使用者名稱或電子郵件。

     使用者名稱必須格式化為 user@domain 或 domain\user 。
  2. 在密碼文字方塊中、輸入您的密碼。
  3. 按一下*登入*。
  4. 在 * 登入選項 * 區段中、選取驗證選項並進行驗證（視您的組態而定）。
     - 推播：核准傳送至手機的推播通知。
     - QR 代碼：使用驗證點行動應用程式掃描 QR 代碼、然後輸入應用程式中顯示的驗證代碼
     - 一次性密碼：輸入 Token 的一次性密碼。
  5. 驗證成功後、會開啟一個快顯視窗、其中包含存取權、 ID 和重新整理 Token 。

     複製存取權杖、並在 SnapCenter REST API 中使用它來執行作業。
  6. 在 REST API 中、您應該在標頭區段中傳遞存取權杖和角色名稱。
  7. SnapCenter 會從 AD FS 驗證此存取權杖。

     如果它是有效的權杖、 SnapCenter 會將其解碼、並取得使用者名稱。
  8. SnapCenter 會使用使用者名稱和角色名稱來驗證使用者執行 API 。

     如果驗證成功、 SnapCenter 會傳回結果、否則會顯示錯誤訊息。

啟用或停用 **REST API** 、 **CLI** 和 **GUI** 的 **SnapCenter MFA** 功能

- 圖形使用者介面 *

步驟

1. 以 SnapCenter 管理員身分登入 SnapCenter Server 。
2. 按一下 * 設定 * > * 全域設定 * > * 多重資料驗證（ MFA ）設定 *
3. 選取介面（ GUI/RST API/CLI ）以啟用或停用 MFA 登入。

◦ PowerShell 介面 *

步驟

1. 執行 PowerShell 或 CLI 命令、以啟用 MFA for GUI 、 REST API 、 PowerShell 和 sccli 。

```
Set-SmMultiFactorAuthentication -IsGuiMFAEnabled -IsRestApiMFAEnabled
-IsCliMFAEnabled -Path
```

path 參數會指定 AD FS MFA 中繼資料 XML 檔案的位置。

啟用 MFA 以使用指定的 AD FS 中繼資料檔案路徑來設定 SnapCenter GUI 、 REST API 、 PowerShell 和 sccli 。

2. 使用檢查 MFA 組態狀態和設定 `Get-SmMultiFactorAuthentication` Cmdlet。

*sccli 介面 *

步驟

1. `# sccli Set-SmMultiFactorAuthentication -IsGuiMFAEnabled true -IsRESTAPIMFAEnabled true -IsCliMFAEnabled true -Path "C:\ADFS_metadata\abc.xml"`
2. `# sccli Get-SmMultiFactorAuthentication`

◦ REST API*

3. 執行下列 POST API 以啟用 MFA for GUI 、 REST API 、 PowerShell 和 sccli 。

參數	價值
要求的 URL	/API/4.9/settings/multitactorauthentication
HTTP方法	貼文
要求主體	｛ "IsGuiMFAEnabled" ：錯誤、 "IsRestApiMFAEnabled" ：對、 "IsClicMFAEnabled" ：錯、 "ADFSConfigFilePath" ： "C:\\ADFS_中繼 資料 \\abc.xml " ｝

回應本文	{ "MFAConfiguration" ： { "IsGuiMFAEnabled" ： 錯誤、 "ADFSConfigFilePath" ： "C:\\ADFS_中繼資料 \\abc.xml 、 "SCConfigFilePath" ： null 、 "IsRestApiMFAEnabled" ：對、 "IsClicMFAEnabled" ：錯、 "ADFSHostName" ： "win-adfs-sc49.winscedom2.com } }

4. 使用下列 API 檢查 MFA 組態狀態和設定。

參數	價值
要求的 URL	/API/4.9/settings/multitactorauthentication
HTTP方法	取得
回應本文	{ "MFAConfiguration" ： { "IsGuiMFAEnabled" ： 錯誤、 "ADFSConfigFilePath" ： "C:\\ADFS_中繼資料 \\abc.xml 、 "SCConfigFilePath" ： null 、 "IsRestApiMFAEnabled" ：對、 "IsClicMFAEnabled" ：錯、 "ADFSHostName" ： "win-adfs-sc49.winscedom2.com } }

版權資訊

商標資訊