安裝適用於 Microsoft Windows 的SnapCenter插件

SnapCenter software

NetApp
November 06, 2025

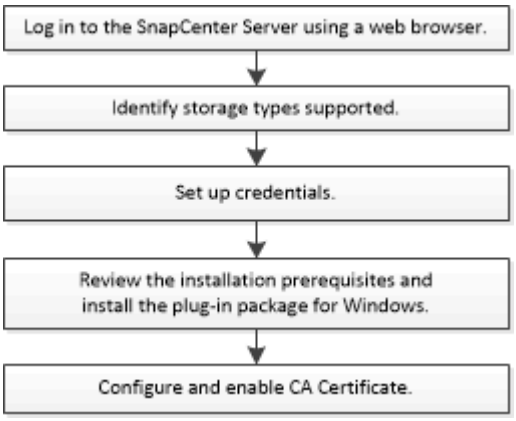
目錄

安裝適用於 Microsoft Windows 的SnapCenter插件 1
適用於 Microsoft Windows 的SnapCenter外掛程式的安裝工作流程 1
適用於 Microsoft Windows 的SnapCenter外掛程式的安裝需求 1
安裝適用於 Windows 的SnapCenter插件包的主機需求 1
設定 Windows 插件的憑證 2
在 Windows Server 2016 或更高版本上設定 gMSA 3
新增主機並安裝適用於 Microsoft Windows 的SnapCenter插件 5
使用 PowerShell cmdlet 在多個遠端主機上安裝適用於 Microsoft Windows 的SnapCenter插件 8
從命令列靜默安裝適用於 Microsoft Windows 的SnapCenter插件 8
監控SnapCenter插件包安裝狀態 10
設定CA憑證 10
產生CA憑證CSR文件 10
匯入 CA 憑證 11
取得 CA 憑證指紋 11
使用 Windows 主機插件服務設定 CA 憑證 12
為插件啟用 CA 憑證 13

安裝適用於 **Microsoft Windows** 的**SnapCenter**插件

適用於 **Microsoft Windows** 的**SnapCenter**外掛程式的安裝工作流程

如果要保護非資料庫文件的 Windows 文件，則必須安裝並設定適用於 Microsoft Windows 的SnapCenter外掛程式。



適用於 **Microsoft Windows** 的**SnapCenter**外掛程式的安裝需求

在安裝適用於 Windows 的插件之前，您應該了解某些安裝要求。

在開始使用適用於 Windows 的插件之前， SnapCenter管理員必須安裝和設定SnapCenter伺服器並執行先決條件任務。

- 您必須具有SnapCenter管理員權限才能安裝適用於 Windows 的插件。

  SnapCenter管理員角色必須具有管理員權限。

- 您必須已安裝並設定SnapCenter伺服器。
- 在 Windows 主機上安裝插件時，如果指定非內建的憑證或使用者屬於本機工作群組用戶，則必須在主機上停用 UAC。
- 如果您想要備份複製，則必須設定SnapMirror和SnapVault 。

安裝適用於 **Windows** 的**SnapCenter**插件包的主機需求

在安裝適用於 Windows 的SnapCenter插件包之前，您應該熟悉一些基本的主機系統空間需求和大小需求。

物品	要求
作業系統	微軟 Windows 有關受支援版本的最新信息，請參閱 "NetApp互通性表工具"。 如果您使用的是 Windows 叢集設置，您還應該安裝和設定 Windows 遠端管理 (WinRM)。
主機上SnapCenter插件的最小 RAM	1GB
主機上SnapCenter插件的最小安裝和日誌空間	5GB 您應該分配足夠的磁碟空間並監控日誌資料夾的儲存消耗。所需的日誌空間取決於要保護的實體的數量和資料保護操作的頻率。如果沒有足夠的磁碟空間，則不會為最近執行的操作建立日誌。
所需軟體包	• ASP.NET Core Runtime 8.0.12（以及所有後續 8.0.x 修補程式）託管包 • PowerShell 核心 7.4.2 有關受支援版本的最新信息，請參閱 "NetApp互通性表工具"。 有關 .NET 特定的故障排除信息，請參閱 "對於沒有網路連線的傳統系統， SnapCenter升級或安裝將會失敗。"

設定 Windows 插件的憑證

SnapCenter使用憑證對SnapCenter操作的使用者進行身份驗證。您應該建立用於安裝SnapCenter插件的憑證，以及用於在 Windows 檔案系統上執行資料保護作業的附加憑證。

您需要什麼

- 在安裝插件之前，您必須設定 Windows 憑證。
- 您必須在遠端主機上設定具有管理員權限（包括管理員權利）的憑證。
- 如果您為單一資源群組設定了憑證，且使用者沒有完全管理權限，則必須至少為該使用者指派資源群組和備份權限。

步驟

1. 在左側導覽窗格中，按一下「設定」。
2. 在「設定」頁面中，按一下「憑證」。

3. 點選“新建”。
4. 在「憑證」頁面中，執行下列操作：

對於這個領域...	這樣做...
憑證名稱	輸入憑證的名稱。
使用者名稱/密碼	輸入用於身份驗證的使用者名稱和密碼。 • 網域管理員或管理員群組的任何成員 指定要安裝SnapCenter插件的系統上的網域管理員或管理員群組的任何成員。用戶名字段的有效格式如下： ◦ `NetBIOS\UserName` ◦ `Domain FQDN\UserName` ◦ `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，請在要安裝SnapCenter插件的系統上指定內建的本機管理員。如果使用者帳戶具有提升的權限或主機系統上停用了使用者存取控制功能，則可以指定屬於本機管理員群組的本機使用者帳戶。用戶名字段的有效格式如下： `UserName` 請勿在密碼中使用雙引號（“）或反引號（`）。密碼中不應同時使用小於號 (<) 和驚嘆號 (!) 符號。例如，lessthan<!10、lessthan10<!、backtick`12。
密碼	輸入用於身份驗證的密碼。

5. 按一下“確定”。

   完成憑證設定後，您可能想要在「使用者和造訪」頁面上將憑證維護指派給使用者或使用者群組。

在 **Windows Server 2016** 或更高版本上設定 **gMSA**

Windows Server 2016 或更高版本可讓您建立群組託管服務帳戶 (gMSA)，該帳戶會從託管網域帳戶提供自動服務帳戶密碼管理。

開始之前

- 您應該擁有 Windows Server 2016 或更高版本的網域控制站。
- 您應該擁有一個 Windows Server 2016 或更高版本的主機，它是網域的成員。

步驟

1. 建立 KDS 根金鑰來為 gMSA 中的每個物件產生唯一的密碼。
2. 對於每個網域，從 Windows 網域控制站執行以下命令：Add-KDSRootKey -EffectiveImmediately
3. 建立並配置 gMSA：
   a. 建立用戶群組帳號，格式如下：

```
 domainName\accountName$
.. 將電腦物件新增至群組。
.. 使用您剛剛建立的使用者群組來建立 gMSA。
```

   例如，

```
 New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,…>
.. 跑步 `Get-ADServiceAccount`命令來驗證服務帳戶。
```

4. 在您的主機上設定 gMSA：
   a. 在要使用 gMSA 帳號的主機上啟用 Windows PowerShell 的 Active Directory 模組。

   為此，請從 PowerShell 執行以下命令：

```
PS C:\> Get-WindowsFeature AD-Domain-Services

Display Name                            Name                Install State
------------                            ----                -------------
[ ] Active Directory Domain Services    AD-Domain-Services  Available


PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Active Directory Domain Services,
Active ...
WARNING: Windows automatic updating is not enabled. To ensure that your
newly-installed role or feature is
automatically updated, turn on Windows Update.
```

   a. 重新啟動主機。
   b. 透過從 PowerShell 命令提示字元執行以下命令在主機上安裝 gMSA： `Install-AdServiceAccount`

`<gMSA>`

c. 透過執行以下命令驗證你的 gMSA 帳戶： `Test-AdServiceAccount <gMSA>`

5. 將管理權限指派給主機上配置的 gMSA。
6. 透過在SnapCenter伺服器中指定配置的 gMSA 帳戶來新增 Windows 主機。

   SnapCenter Server 將在主機上安裝選定的插件，並且指定的 gMSA 將在插件安裝期間用作服務登入帳戶。

新增主機並安裝適用於 Microsoft Windows 的SnapCenter插件

您可以使用SnapCenter新增主機頁面來新增 Windows 主機。適用於 Microsoft Windows 的SnapCenter外掛程式會自動安裝在指定主機上。這是安裝插件的推薦方法。您可以新增主機並為單一主機或叢集安裝插件。

開始之前

- 如果SnapCenter Server 主機的作業系統是 Windows 2019，而插件主機的作業系統是 Windows 2022，則應執行下列操作：
  - 升級到 Windows Server 2019（作業系統內部版本 17763.5936）或更高版本
  - 升級到 Windows Server 2022（作業系統內部版本 20348.2402）或更高版本
- 您必須是分配有插件安裝和卸載權限的角色的用戶，例如SnapCenter管理員角色。
- 在 Windows 主機上安裝插件時，如果指定非內建的憑證或使用者屬於本機工作群組用戶，則必須在主機上停用 UAC。
- 應將SnapCenter使用者新增至 Windows Server 的「作為服務登入」角色。
- 您應該確保訊息佇列服務處於運行狀態。
- 如果您使用群組託管服務帳戶 (gMSA)，則應使用管理權限設定 gMSA。

  "在 Windows Server 2016 或更高版本上為 Windows 檔案系統設定群組託管服務帳戶"

關於此任務

- 您不能將SnapCenter伺服器作為插件主機新增至另一個SnapCenter伺服器。
- Windows 外掛
  - 微軟 Windows
  - Microsoft Exchange 伺服器
  - 微軟 SQL 伺服器
  - SAP HANA
- 在集群上安裝插件

  如果在叢集（WSFC、Oracle RAC 或 Exchange DAG）上安裝插件，則它們將安裝在叢集的所有節點上。

- E系列儲存

  您無法在連接到 E 系列儲存的 Windows 主機上安裝適用於 Windows 的插件。

如果主機已經是工作群組的一部分並變更為另一個網域或反之亦然，則SnapCenter不支援將相同主機（插件主機）新增至SnapCenter。如果要新增相同的主機，則應從SnapCenter中刪除該主機，然後重新新增。

步驟

1. 在左側導覽窗格中，按一下「主機」。
2. 確保在頂部選擇了*託管主機*。
3. 按一下“新增”。
4. 在「主機」頁面中，執行下列操作：

對於這個領域...	這樣做...
主機類型	選擇 **Windows** 類型的主機。 SnapCenter Server 新增主機，然後安裝適用於 Windows 的插件（如果主機上尚未安裝）。
主機名稱	輸入主機的完全限定網域名稱 (FQDN) 或 IP 位址。 SnapCenter依賴 DNS 的正確配置。因此，最佳做法是輸入完全限定網域名稱 (FQDN)。 您可以輸入以下之一的 IP 位址或 FQDN： • 獨立主機 • Windows Server 故障轉移叢集 (WSFC) 如果您使用SnapCenter新增主機且它是子網域的一部分，則必須提供 FQDN。
證書	選擇您建立的憑證名稱或建立新的憑證。 該憑證必須具有遠端主機的管理權限。有關詳細信息，請參閱有關建立憑證的資訊。 將遊標放在您提供的憑證名稱上即可顯示有關憑證的詳細信息，包括使用者名稱、網域和主機類型。 驗證模式由您在新增主機精靈中指定的主機類型決定。

5. 在選擇要安裝的插件部分中，選擇要安裝的插件。

   對於新部署，沒有列出插件包。

6. （可選）按一下“更多選項”。

對於這個領域...	這樣做...
港口	保留預設連接埠號碼或指定連接埠號碼。 預設連接埠號碼為 8145。如果SnapCenter伺服器安裝在自訂連接埠上，則該連接埠號碼將顯示為預設連接埠。 如果您手動安裝了插件並指定了自訂端口，則必須指定相同的端口。否則，操作失敗。
安裝路徑	預設路徑為 C:\Program Files\ NetApp\ SnapCenter。 您可以選擇自訂路徑。對於適用於 Windows 的SnapCenter插件包，預設路徑為 C:\Program Files\ NetApp\ SnapCenter。但是，如果您願意，您可以自訂預設路徑。
新增叢集中的所有主機	選取此複選框可新增 WSFC 中的所有叢集節點。
跳過預安裝檢查	如果您已經手動安裝了插件並且不想驗證主機是否符合安裝插件的要求，請選取此核取方塊。
使用群組託管服務帳戶 (gMSA) 執行外掛程式服務	如果要使用群組託管服務帳戶 (gMSA) 來執行外掛程式服務，請選取此核取方塊。 以以下格式提供 gMSA 名稱：*domainName\accountName$*。 gMSA 將僅用作 Windows 服務的SnapCenter插件的登入服務帳戶。

7. 點選“提交”。

   如果您未選取「跳過預先檢查」複選框，則會驗證主機是否符合安裝插件的要求。系統會根據最低要求驗證磁碟空間、RAM、PowerShell 版本、.NET 版本和位置。如果不符合最低要求，則會顯示相應的錯誤或警告訊息。

   如果錯誤與磁碟空間或 RAM 有關，您可以更新位於 `C:\Program Files\NetApp\SnapCenter`WebApp 修改預設值。如果錯誤與其他參數有關，則必須修復該問題。

   在 HA 設定中，如果您要更新 web.config 文件，則必須在兩個節點上更新該文件。

8. 監控安裝進度。

使用 PowerShell cmdlet 在多個遠端主機上安裝適用於 Microsoft Windows 的SnapCenter插件

如果要同時在多個主機上安裝適用於 Microsoft Windows 的SnapCenter插件，可以使用 `Install-SmHostPackage`PowerShell 指令。

您必須以網域使用者身分登入SnapCenter ，並在要安裝插件的每個主機上擁有本機管理員權限。

步驟

1. 啟動 PowerShell。
2. 在SnapCenter伺服器主機上，使用 `Open-SmConnection`cmdlet，然後輸入您的憑證。
3. SnapCenter `Add-SmHost`cmdlet 和所需的參數。

   可以透過執行_Get-Help command_name_來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 "SnapCenter軟體 Cmdlet 參考指南"。

4. 使用 `Install-SmHostPackage`cmdlet 和所需的參數。

   您可以使用 `-skipprecheck`當您手動安裝了插件並且不想驗證主機是否符合安裝插件的要求時，可以選擇此選項。

從命令列靜默安裝適用於 Microsoft Windows 的SnapCenter插件

如果您無法從SnapCenter GUI 遠端安裝插件，則可以在 Windows 主機上本機安裝適用於 Microsoft Windows 的SnapCenter插件。您可以從 Windows 命令列以靜默模式無人值守執行適用於 Microsoft Windows 的SnapCenter外掛程式安裝程式。

開始之前

- 您必須安裝 ASP.NET Core Runtime 8.0.12（以及所有後續 8.0.x 修補程式）託管套件。
- 您必須安裝 PowerShell 7.4.2 或更高版本。
- 您必須是主機上的本機管理員。

步驟

1. 從安裝位置下載適用於 Microsoft Windows 的SnapCenter外掛程式。

   例如，預設安裝路徑為 C:\ProgramData\ NetApp\ SnapCenter\Package Repository。

   可以從安裝SnapCenter伺服器的主機存取此路徑。

2. 將安裝檔案複製到要安裝插件的主機上。
3. 從命令提示字元處，導覽至下載安裝檔案的目錄。
4. 輸入以下命令，用您的資料取代變數：

   ```
   "snapcenter_windows_host_plugin.exe"/silent / debuglog"" /log""
   ```

```
BI_SNAPCENTER_PORT= SUITE_INSTALLDIR="" BI_SERVICEACCOUNT= BI_SERVICEPWD=
ISFeatureInstall=SCW
```

例如：

```
`"C:\ProgramData\NetApp\SnapCenter\Package Repository
\snapcenter_windows_host_plugin.exe"/silent /debuglog"C:
\HPPW_SCW_Install.log" /log"C:\" BI_SNAPCENTER_PORT=8145
SUITE_INSTALLDIR="C: \Program Files\NetApp\SnapCenter"
BI_SERVICEACCOUNT=domain\administrator BI_SERVICEPWD=password
ISFeatureInstall=SCW`
```

安裝 Windows 插件期間傳遞的所有參數均區分大小寫。

輸入以下變數的值：

多變的	價值
/debuglog"<偵錯日誌路徑>	指定套件安裝程式日誌檔案的名稱和位置，如下例所示：Setup.exe /debuglog"C:\PathToLog\setupexe.log"。
BI_SNAPCENTER_連接埠	指定SnapCenter與 SMCore 通訊的連接埠。
套件安裝目錄	指定主機插件包安裝目錄。
BI_服務帳戶	為 Microsoft Windows Web 服務帳戶指定SnapCenter外掛程式。
BI_SERVICEPWD	指定 Microsoft Windows Web 服務帳戶的SnapCenter外掛程式的密碼。
ISFeature安裝	指定SnapCenter在遠端主機上部署的解決方案。

debuglog 參數包含SnapCenter日誌檔案的路徑。寫入此日誌檔案是取得故障排除資訊的首選方法，因為該檔案包含安裝對插件先決條件執行的檢查結果。

如有必要，您可以在SnapCenter for Windows 套件的日誌檔案中找到其他故障排除資訊。套件的日誌檔案列在 *%Temp%* 資料夾中（最早的在前），例如 *C:\temp*。

Windows 插件的安裝在主機上註冊該插件，而不是在SnapCenter伺服器上註冊。您可以透過使用SnapCenter GUI 或 PowerShell cmdlet 新增主機在SnapCenter伺服器上註冊插件。新增主機後，會自動發現插件。

監控SnapCenter插件包安裝狀態

您可以使用「作業」頁面監控SnapCenter插件包的安裝進度。您可能需要檢查安裝進度以確定安裝何時完成或是否有問題。

關於此任務

以下圖示出現在「作業」頁面上並指示操作的狀態：

- 進行中
- 成功完成
- 失敗的
- 已完成但有警告，或因警告而無法啟動
- 排隊

步驟

1. 在左側導覽窗格中，按一下「監控」。
2. 在「監控」頁面中，按一下「作業」。
3. 在 **Jobs** 頁面中，若要篩選清單以便僅列出外掛程式安裝操作，請執行下列操作：
   a. 按一下“過濾器”。
   b. 可選：指定開始日期和結束日期。
   c. 從類型下拉式選單中，選擇*插件安裝*。
   d. 從狀態下拉式選單中，選擇安裝狀態。
   e. 按一下“應用”。
4. 選擇安裝作業並點擊*詳細資料*以查看作業詳細資料。
5. 在「作業詳情」頁面中，按一下「檢視日誌」。

設定CA憑證

產生CA憑證CSR文件

您可以產生憑證簽署要求 (CSR) 並匯入可使用產生的 CSR 從憑證授權單位 (CA) 取得的憑證。該憑證將有一個與之關聯的私鑰。

CSR 是一段編碼文本，提供給授權憑證供應商以取得簽署的 CA 憑證。

CA 憑證 RSA 金鑰長度必須至少為 3072 位元。

有關生成 CSR 的信息，請參閱 "如何產生CA憑證CSR文件"。

如果您擁有您的網域（*.domain.company.com）或您的系統（machine1.domain.company.com）的 CA 證書，您可以跳過生成 CA 證書 CSR 檔案。您可以使用SnapCenter部署現有的 CA 憑證。

對於叢集配置，CA 憑證中應提及叢集名稱（虛擬叢集 FQDN）和對應的主機名稱。在取得憑證之前，可以透過填寫主題備用名稱 (SAN) 欄位來更新憑證。對於通配符憑證（*.domain.company.com），該憑證將隱式包含網域的所有主機名稱。

匯入 **CA** 憑證

您必須使用 Microsoft 管理主控台 (MMC) 將 CA 憑證匯入SnapCenter伺服器和 Windows 主機外掛程式。

步驟

1. 前往 Microsoft 管理主控台 (MMC)，然後按一下 檔案 > 新增/移除管理單元。
2. 在“新增或刪除管理單元”視窗中，選擇“證書”，然後按一下“新增”。
3. 在憑證管理單元視窗中，選擇「電腦帳戶」選項，然後按一下「完成」。
4. 按一下 控制台根 > 憑證 - 本機電腦 > 受信任的根憑證授權單位 > 憑證。
5. 右鍵單擊資料夾“受信任的根憑證授權單位”，然後選擇*所有任務*>*匯入*以啟動匯入精靈。
6. 完成嚮導，如下圖所示：

在此精靈視窗中...	執行以下操作...
導入私鑰	選擇選項*是*，匯入私鑰，然後按一下*下一步*。
導入文件格式	不做任何更改；按一下“下一步”。
安全	指定匯出憑證要使用的新密碼，然後按一下「下一步」。
完成憑證匯入精靈	查看摘要，然後按一下「完成」開始匯入。

匯入憑證時需攜帶私鑰（支援格式為：**.pfx**、.p12、*.p7b）。

7. 對「個人」資料夾重複步驟 5。

取得 **CA** 憑證指紋

憑證指紋是用於識別憑證的十六進位字串。指紋是使用指紋演算法根據憑證內容計算出來的。

步驟

1. 在 GUI 上執行以下操作：
   a. 雙擊該證書。

b. 在「證書」對話方塊中，按一下「詳細資料」標籤。

c. 捲動瀏覽欄位清單並按一下「指紋」。

d. 從框複製十六進位字元。

e. 刪除十六進制數之間的空格。

例如，如果指紋為：“a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b”，刪除空格後，將為：“a909502dd82ae41433e68383883”。

2. 從 PowerShell 執行以下操作：

a. 執行以下命令列出已安裝憑證的指紋並透過主題名稱識別最近安裝的憑證。

Get-ChildItem -Path 憑證:*LocalMachine\My*

b. 複製指紋。

使用 **Windows** 主機插件服務設定 **CA** 憑證

您應該使用 Windows 主機外掛程式服務來設定 CA 憑證以啟動已安裝的數位憑證。

在SnapCenter伺服器和所有已部署 CA 憑證的插件主機上執行下列步驟。

步驟

1. 透過執行以下命令刪除與 SMCore 預設連接埠 8145 的現有憑證綁定：

```
> netsh http delete sslcert ipport=0.0.0.0:_<SMCore Port>
```

例如：

```
 > netsh http delete sslcert ipport=0.0.0.0:8145
```

. 透過執行下列命令將新安裝的憑證與 `Windows` 主機插件服務綁定：

```
> $cert = "_<certificate thumbprint>_"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

例如：

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

為插件啟用 **CA** 憑證

您應該設定 CA 憑證並在SnapCenter伺服器和對應的插件主機中部署 CA 憑證。您應該為插件啟用 CA 憑證驗證。

開始之前

- 您可以使用執行_Set-SmCertificateSettings_ cmdlet 來啟用或停用 CA 憑證。
- 您可以使用_Get-SmCertificateSettings_顯示插件的憑證狀態。

可以透過執行_Get-Help command_name_來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 "SnapCenter軟體 Cmdlet 參考指南"。

步驟

1. 在左側導覽窗格中，按一下「主機」。
2. 在「主機」頁面中，按一下「託管主機」。
3. 選擇單一或多個插件主機。
4. 按一下“更多選項”。
5. 選擇*啟用憑證驗證*。

完成後

託管主機選項卡主機顯示一個掛鎖，掛鎖的顏色表示SnapCenter伺服器和插件主機之間的連線狀態。

- * * 表示 CA 憑證未啟用或未指派給插件主機。
- * * 表示 CA 憑證驗證成功。
- * * 表示無法驗證 CA 憑證。
- * * 表示無法檢索連線資訊。

當狀態為黃色或綠色時，表示資料保護操作已成功完成。

版權資訊

商標資訊