



使用 **SNMP** 監控 StorageGRID software

NetApp
May 29, 2026

目錄

使用 SNMP 監控	1
使用 SNMP 監控	1
功能	1
SNMP 版本支持	1
限制	2
設定 SNMP 代理	2
指定基本配置	2
輸入社區字串	3
建立陷阱目的地	4
建立代理地址	6
建立 USM 用戶	7
更新 SNMP 代理	8
存取 MIB 文件	10
存取 MIB 文件	10
MIB 檔案內容	11
MIB 對象	11
通知類型 (陷阱)	12

使用 SNMP 監控

使用 SNMP 監控

如果要使用簡單網路管理協定 (SNMP) 監控StorageGRID，則必須設定StorageGRID隨附的 SNMP 代理程式。

- ["設定 SNMP 代理"](#)
- ["更新 SNMP 代理"](#)

功能

每個StorageGRID節點都執行一個提供 MIB 的 SNMP 代理程式或守護程式。StorageGRID MIB 包含警報的表和通知定義。MIB 還包含每個節點的平台和型號等系統描述資訊。每個StorageGRID節點也支援 MIB-II 物件的子集。



看["存取 MIB 文件"](#)如果您想在網格節點上下載 MIB 檔案。

最初，所有節點上的 SNMP 都是停用的。設定 SNMP 代理程式時，所有StorageGRID節點都會接收相同的設定。

StorageGRID SNMP 代理程式支援 SNMP 協定的所有三個版本。它為查詢提供唯讀 MIB 訪問，並且可以向管理系統發送兩種類型的事件驅動通知：

陷阱

陷阱是由 SNMP 代理程式發送的通知，不需要管理系統確認。陷阱用於通知管理系統StorageGRID內發生了某些事情，例如觸發了警報。

SNMP 的所有三個版本均支援陷阱。

通知

通知與陷阱類似，但需要管理系統的確認。如果 SNMP 代理程式在一定時間內未收到確認，它會重新發送通知，直到收到確認或達到最大重試值。

SNMPv2c 和 SNMPv3 支援通知。

在以下情況下會發送 Trap 和 Inform 通知：

- 任何嚴重程度等級都會觸發預設或自訂警報。若要抑制警報的 SNMP 通知，您必須["配置靜默"](#)以發出警報。警報通知由["首選發送者管理節點"](#)。

根據警報的嚴重性級別，每個警報都映射到三種陷阱類型之一：activeMinorAlert、activeMajorAlert 和 activeCriticalAlert。有關可觸發這些陷阱的警報列表，請參閱["警報參考"](#)。

SNMP 版本支持

該表提供了每個 SNMP 版本所支援內容的高級摘要。

	SNMPv1	SNMPv2c	SNMPv3
查詢 (GET 和 GETNEXT)	只讀 MIB 查詢	只讀 MIB 查詢	只讀 MIB 查詢
查詢身份驗證	社區字串	社區字串	基於用戶的安全模型 (USM) 用戶
通知 (誘捕和通報)	僅限陷阱	陷阱和通報	陷阱和通報
通知身份驗證	每個陷阱目標的預設陷阱社群 或自訂社群字串	每個陷阱目標的預設陷阱社群 或自訂社群字串	每個陷阱目的地的 USM 用戶

限制

- StorageGRID支援唯讀 MIB 存取。不支援讀寫存取。
- 網格中的所有節點都接收相同的配置。
- SNMPv3：StorageGRID不支援傳輸支援模式 (TSM)。
- SNMPv3：唯一支援的驗證協定是 SHA (HMAC-SHA-96)。
- SNMPv3：唯一支援的隱私權協定是 AES。

設定 SNMP 代理

您可以設定StorageGRID SNMP 代理程式以使用第三方 SNMP 管理系統進行唯讀 MIB 存取和通知。

開始之前

- 您已使用[支援的網頁瀏覽器](#)。
- 你有["Root存取權限"](#)。

關於此任務

StorageGRID SNMP 代理程式支援 SNMPv1、SNMPv2c 和 SNMPv3。您可以為一個或多個版本配置代理程式。對於 SNMPv3，僅支援使用者安全模型 (USM) 驗證。

網格中的所有節點都使用相同的 SNMP 配置。

指定基本配置

第一步，啟用StorageGRID SMNP 代理並提供基本資訊。

步驟

1. 選擇 設定 > 監控 > **SNMP** 代理程式。

出現 SNMP 代理頁面。

2. 若要在所有網格節點上啟用 SNMP 代理，請勾選「啟用 SNMP」複選框。
3. 在基本配置部分輸入以下資訊。

場地	描述
系統聯絡人	<p>選修的。StorageGRID系統的主要聯絡人，在 SNMP 訊息中以 sysContact 的形式傳回。</p> <p>系統聯絡人通常是一個電子郵件地址。此值適用於StorageGRID系統中的所有節點。*系統聯絡人*最多可包含 255 個字元。</p>
系統位置	<p>選修的。StorageGRID系統的位置，在 SNMP 訊息中以 sysLocation 的形式傳回。</p> <p>系統位置可以是任何有助於識別StorageGRID系統所在位置的資訊。例如，您可以使用設施的街道地址。此值適用於StorageGRID系統中的所有節點。*系統位置*最多可包含 255 個字元。</p>
啟用 SNMP 代理程式通知	<ul style="list-style-type: none">• 如果選擇此選項，StorageGRID SNMP 代理程式將發送陷阱和通知。• 如果未選擇，SNMP 代理程式支援唯讀 MIB 訪問，但不會發送任何 SNMP 通知。
啟用身份驗證陷阱	如果選擇此選項，StorageGRID SNMP 代理程式將在收到未正確驗證的協定訊息時傳送身份驗證陷阱。

輸入社區字串

如果您使用 SNMPv1 或 SNMPv2c，請完成社群字串部分。

當管理系統查詢StorageGRID MIB 時，它會傳送一個社群字串。如果社群字串與此處指定的某個值匹配，則 SNMP 代理程式會向管理系統發送回應。

步驟

1. 對於*唯讀社群*，可選擇輸入社群字串以允許在 IPv4 和 IPv6 代理位址上進行唯讀 MIB 存取。



為了確保StorageGRID系統的安全，請不要使用「public」作為社群字串。如果將此欄位留空，SNMP 代理程式將使用StorageGRID系統的網格 ID 作為社群字串。

每個社區字串最多可以有 32 個字符，且不能包含空格字符。

2. 選擇*新增另一個社區字串*來新增其他字串。

最多允許五個字串。

建立陷阱目的地

使用「其他配置」部分中的「陷阱目標」標籤來定義StorageGRID陷阱或通知通知的一個或多個目標。當您啟用SNMP代理程式並選擇 儲存 時，StorageGRID會在觸發警報時向每個定義的目的地發送通知。也會為支援的MIB-II實體（例如，ifDown 和 coldStart）發送標準通知。

步驟

1. 對於 預設陷阱社群 字段，可選擇輸入要用於 SNMPv1 或 SNMPv2 陷阱目標的預設社群字串。

根據需要，您可以在定義特定的陷阱目標時提供不同的（「自訂」）社群字串。

*預設陷阱社群*最多可以包含 32 個字符，且不能包含空格字符。

2. 若要新增陷阱目標，請選擇*創建*。
3. 選擇將用於此陷阱目標的 SNMP 版本。
4. 完成您所選版本的「建立陷阱目標」表單。

SNMPv1

如果您選擇 SNMPv1 作為版本，請填寫這些欄位。

場地	描述
類型	對 SNMPv1 來說必須是 Trap。
主持人	用於接收陷阱的 IPv4 或 IPv6 位址或完全限定網域名稱 (FQDN)。
港口	使用 162，這是 SNMP 陷阱的標準端口，除非您必須使用其他值。
協定	使用 UDP，它是標準 SNMP 陷阱協議，除非您需要使用 TCP。
社區字串	如果指定了，則使用預設陷阱社區，或為此陷阱目標輸入自訂社區字串。 自訂社區字串最多可以有 32 個字符，且不能包含空格。

SNMPv2c

如果您選擇 SNMPv2c 作為版本，請填寫這些欄位。

場地	描述
類型	目的地是否用於陷阱或通知。
主持人	用於接收陷阱的 IPv4 或 IPv6 位址或 FQDN。
港口	使用 162，這是 SNMP 陷阱的標準端口，除非您必須使用其他值。
協定	使用 UDP，它是標準 SNMP 陷阱協議，除非您需要使用 TCP。
社區字串	如果指定了，則使用預設陷阱社區，或為此陷阱目標輸入自訂社區字串。 自訂社區字串最多可以有 32 個字符，且不能包含空格。

SNMPv3

如果您選擇 SNMPv3 作為版本，請填寫這些欄位。

場地	描述
類型	目的地是否用於陷阱或通知。
主持人	用於接收陷阱的 IPv4 或 IPv6 位址或 FQDN。

場地	描述
港口	使用 162，這是 SNMP 陷阱的標準端口，除非您必須使用其他值。
協定	使用 UDP，它是標準 SNMP 陷阱協議，除非您需要使用 TCP。
USM 用戶	<p>將用於身份驗證的 USM 使用者。</p> <ul style="list-style-type: none"> • 如果您選擇了 Trap，則僅顯示沒有權威引擎 ID 的 USM 使用者。 • 如果您選擇了 *通知*，則僅顯示具有權威引擎 ID 的 USM 使用者。 • 如果沒有顯示使用者： <ul style="list-style-type: none"> i. 創建並保存陷阱目的地。 ii. 前往建立 USM 用戶並創建用戶。 iii. 返回「陷阱目標」標籤，從表格中選擇已儲存的目標，然後選擇「編輯」。 iv. 選擇用戶。

5. 選擇“創建”。

陷阱目標已建立並新增至表中。

建立代理地址

或者，使用其他配置部分中的代理程式位址標籤指定一個或多個「監聽位址」。這些是 SNMP 代理程式可以接收查詢的 StorageGRID 位址。

如果您未設定代理位址，則所有 StorageGRID 網路上的預設監聽位址為 UDP 連接埠 161。

步驟

1. 選擇“創建”。
2. 輸入以下資訊。

場地	描述
網際網路協定	<p>此位址是否使用 IPv4 或 IPv6。</p> <p>預設情況下，SNMP 使用 IPv4。</p>
傳輸協定	<p>此位址是否使用 UDP 或 TCP。</p> <p>預設情況下，SNMP 使用 UDP。</p>

場地	描述
StorageGRID網路	<p>代理將監聽哪個StorageGRID網路。</p> <ul style="list-style-type: none"> • 網格、管理和客戶端網路：SNMP 代理程式將監聽所有三個網路上的查詢。 • 網格網路 • 管理網路 • 客戶網路 <p>注意：如果您使用客戶端網路傳輸不安全的數據，並為客戶端網路建立代理位址，請注意 SNMP 流量也將不安全。</p>
港口	<p>可選，SNMP 代理應監聽的連接埠號碼。</p> <p>SNMP 代理程式的預設 UDP 連接埠是 161，但您可以輸入任何未使用的連接埠號碼。</p> <p>注意：當您儲存 SNMP 代理程式時，StorageGRID會自動在內部防火牆上開啟代理位址連接埠。您必須確保任何外部防火牆都允許存取這些連接埠。</p>

3. 選擇“創建”。

代理地址已建立並新增至表中。

建立 USM 用戶

如果您使用的是 SNMPv3，請使用其他設定部分中的 USM 使用者標籤來定義有權查詢 MIB 或接收陷阱和通知的 USM 使用者。



SNMPv3 *inform* 目的地必須具有具有引擎 ID 的使用者。SNMPv3 *trap* 目標不能擁有具有引擎 ID 的使用者。

如果您僅使用 SNMPv1 或 SNMPv2c，則這些步驟不適用。

步驟

1. 選擇“創建”。
2. 輸入以下資訊。

場地	描述
使用者名稱	<p>此 USM 使用者的唯一名稱。</p> <p>使用者名稱最多可以有 32 個字符，且不能包含空格字符。用戶建立後，用戶名不能更改。</p>

場地	描述
只讀 MIB 訪問	如果選擇，該使用者應該具有 MIB 的唯讀存取權限。
權威引擎 ID	<p>如果此使用者將在通知目的地中使用，則為該使用者的權威引擎 ID。</p> <p>輸入 10 到 64 個十六進位字元（5 到 32 個位元組），中間不帶空格。對於將在陷阱目的地中選擇以進行通知的 USM 用戶，此值是必需的。對於將在陷阱目標中選擇的 USM 用戶，不允許使用此值。</p> <p>注意：如果您選擇了*只讀 MIB 存取*，則不會顯示此字段，因為具有唯讀 MIB 存取權限的 USM 使用者不能擁有引擎 ID。</p>
安全等級	<p>USM 用戶的安全等級：</p> <ul style="list-style-type: none"> • authPriv：此使用者透過身分驗證和隱私（加密）進行通訊。您必須指定身份驗證協定和密碼以及隱私權協議和密碼。 • authNoPriv：此使用者透過身分驗證進行通信，但不進行隱私（無加密）。您必須指定身份驗證協定和密碼。
身份驗證協議	始終設定為 SHA，這是唯一支援的協定（HMAC-SHA-96）。
密碼	該用戶將用於身份驗證的密碼。
隱私協議	僅當您選擇 authPriv 並始終設定為 AES（這是唯一支援的隱私協定）時才顯示。
密碼	僅當您選擇 authPriv 時才顯示。該用戶將使用的密碼以保護隱私。

3. 選擇“創建”。

USM 使用者已建立並新增至表中。

4. 完成 SNMP 代理程式配置後，選擇*儲存*。

新的 SNMP 代理程式配置將生效。

更新 SNMP 代理

您可以停用 SNMP 通知、更新社群字串，或新增或刪除代理程式地址、USM 使用者和陷阱目的地。

開始之前

- 您已使用[支援的網頁瀏覽器](#)。
- 你有["Root存取權限"](#)。

關於此任務

看["設定 SNMP 代理"](#)有關 SNMP 代理頁面上每個欄位的詳細資訊。您必須選擇頁面底部的“儲存”才能提交在每個標籤上所做的任何變更。

步驟

1. 選擇 設定 > 監控 > **SNMP** 代理程式。

出現 SNMP 代理頁面。

2. 若要停用所有網格節點上的 SNMP 代理，請清除 啟用 **SNMP** 複選框，然後選擇 儲存。

如果重新啟用 SNMP 代理，則任何先前的 SNMP 設定都會保留。

3. 或者，更新基本配置部分中的資訊：

- a. 根據需要，更新*系統聯絡人*和*系統位置*。

- b. 或者，勾選或清除「啟用 SNMP 代理通知」複選框來控制StorageGRID SNMP 代理程式是否發送陷阱和通知通知。

清除此複選框後，SNMP 代理程式支援唯讀 MIB 訪問，但不發送 SNMP 通知。

- c. 或者，勾選或清除「啟用身份驗證陷阱」複選框，以控制StorageGRID SNMP 代理程式在收到未正確驗證的協定訊息時是否發送身份驗證陷阱。

4. 如果您使用 SNMPv1 或 SNMPv2c，則可以選擇在社群字串部分更新或新增 只讀社群。

5. 若要更新陷阱目標，請選擇「其他配置」部分中的「陷阱目標」標籤。

使用此選項卡可以定義StorageGRID陷阱或通知通知的一個或多個目標。當您啟用 SNMP 代理程式並選擇儲存時，StorageGRID會在觸發警報時向每個定義的目的地發送通知。也會為支援的 MIB-II 實體（例如，ifDown 和 coldStart）發送標準通知。

有關輸入內容的詳細信息，請參閱["創建陷阱目的地"](#)。

- 或者，更新或刪除預設陷阱社群。

如果刪除預設陷阱社區，則必須先確保任何現有的陷阱目標都使用自訂社區字串。

- 若要新增陷阱目標，請選擇*創建*。
- 若要編輯陷阱目標，請選擇單選按鈕，然後選擇*編輯*。
- 若要刪除陷阱目標，請選擇單選按鈕，然後選擇*刪除*。
- 若要提交您的更改，請選擇頁面底部的“儲存”。

6. 若要更新代理地址，請選擇其他配置部分中的代理地址標籤。

使用此選項卡可以指定一個或多個「監聽位址」。這些是 SNMP 代理程式可以接收查詢的StorageGRID位址。

有關輸入內容的詳細信息，請參閱["建立代理地址"](#)。

- 若要新增代理地址，請選擇*建立*。
- 若要編輯代理位址，請選擇單選按鈕，然後選擇*編輯*。

- 若要刪除代理地址，請選擇單選按鈕，然後選擇*刪除*。

- 若要提交您的更改，請選擇頁面底部的“儲存”。

7. 若要更新 USM 用戶，請選擇「其他配置」部分中的「USM 用戶」標籤。

使用此標籤定義有權查詢 MIB 或接收陷阱和通知的 USM 使用者。

有關輸入內容的詳細信息，請參閱["建立 USM 用戶"](#)。

- 若要新增 USM 用戶，請選擇 建立。

- 若要編輯 USM 用戶，請選擇單選按鈕，然後選擇 編輯。

現有 USM 用戶的用戶名無法更改。如果您需要更改用戶名，則必須刪除該用戶並建立新用戶。



如果您新增或刪除使用者的權威引擎 ID，且該使用者目前被選為目標，則必須編輯或刪除該目標。否則，儲存 SNMP 代理程式設定時會出現驗證錯誤。

- 若要刪除 USM 用戶，請選擇單選按鈕，然後選擇 刪除。



如果您刪除的使用者目前被選為陷阱目標，則必須編輯或刪除該目標。否則，儲存 SNMP 代理程式設定時會出現驗證錯誤。

- 若要提交您的更改，請選擇頁面底部的“儲存”。

8. 更新 SNMP 代理程式配置後，選擇*儲存*。

存取 MIB 文件

MIB 檔案包含有關網格中節點的託管資源和服務的屬性的定義和資訊。您可以存取定義 StorageGRID 的物件和通知的 MIB 檔案。這些文件對於監控您的電網很有用。

看["使用 SNMP 監控"](#)有關 SNMP 和 MIB 檔案的詳細資訊。

存取 MIB 文件

請依照以下步驟存取 MIB 檔案。

步驟

1. 選擇 設定 > 監控 > **SNMP** 代理程式。

2. 在 SNMP 代理頁面，選擇要下載的檔案：

- **NETAPP-STORAGEGRID-MIB.txt**：定義所有管理節點上可存取的警報表和通知（陷阱）。

- **ES-NETAPP-06-MIB.mib**：定義基於 E 系列的設備的物件和通知。

- **MIB_1_10.zip**：定義具有 BMC 介面的設備的物件和通知。



您也可以在任何StorageGRID節點上的下列位置存取 MIB 檔案：
/usr/share/snmp/mibs

3. 要從 MIB 檔案中提取StorageGRID OID：

a. 取得StorageGRID MIB 根的 OID：

```
root@user-adml:~ # snmptranslate -On -IR storagegrid
```

結果：.1.3.6.1.4.1.789.28669 (`28669` 始終是StorageGRID的 OID)

a. 在整個樹中尋找StorageGRID OID (使用 `paste` 連接線)：

```
root@user-adml:~ # snmptranslate -Tso | paste -d " " - - | grep 28669
```



這 `snmptranslate` 命令有許多選項可用於探索 MIB。此指令在任何StorageGRID節點上均可用。

MIB 檔案內容

所有物件均位於StorageGRID OID 下。

物件名稱	物件 ID (OID)	描述
		NetApp StorageGRID實體的 MIB 模組。

MIB對象

物件名稱	物件 ID (OID)	描述
activeAlertCount		activeAlertTable 中的活動警報數。
活動警報表		StorageGRID中的活動警報表。
活動警報ID		警報的 ID。僅在目前活動警報集中是唯一的。
activeAlertName		警報的名稱。
activeAlertInstance		產生警報的實體的名稱，通常是節點名稱。
activeAlertSeverity		警報的嚴重性。
活動警報開始時間		觸發警報的日期和時間。

通知類型 (陷阱)

所有通知都包含以下變數作為 varbinds :

- 活動警報ID
- activeAlertName
- activeAlertInstance
- activeAlertSeverity
- 活動警報開始時間

通知類型	物件 ID (OID)	描述
主動輕微警報		嚴重程度較低的警報
活躍重大警報		嚴重程度較高的警報
activeCriticalAlert		嚴重程度警報

版權資訊

Copyright © 2026 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。