使用LDAP

ONTAP 9

NetApp
February 12, 2026

This PDF was generated from https://docs.netapp.com/zh-tw/ontap/nfs-admin/using-ldap-concept.html on February 12, 2026. Always check docs.netapp.com for the latest.

目錄

使用LDAP . . . 1
- 了解適用於 ONTAP NFS SVM 的 LDAP . . . 1
- 了解 ONTAP NFS SVM 的 LDAP 簽章和密封 . . . 2
- 了解適用於 ONTAP NFS SVM 的 LDAPS . . . 2
  - 術語 . . . 2
  - 如何使用LDAPS ONTAP . . . 3
- 為 ONTAP NFS SVM 啟用 LDAP RFC2307bis 支援 . . . 4
- 用於 LDAP 目錄搜尋的 ONTAP NFS 設定選項 . . . 5
  - 預設基礎和範圍搜尋值 . . . 5
  - 自訂基礎和範圍搜尋值 . . . 5
  - 多個自訂基礎DN值 . . . 6
  - 自訂 LDAP 搜尋篩選器 . . . 6
- 提高 ONTAP NFS SVM 的 LDAP 目錄網路群組按主機搜尋的效能 . . . 6
- 使用 LDAP 快速綁定對 ONTAP NFS SVM 進行 nsswitch 驗證 . . . 8
- 顯示 ONTAP NFS SVM 的 LDAP 統計資訊 . . . 9

使用LDAP

了解適用於 ONTAP NFS SVM 的 LDAP

LDAP（輕量型目錄存取傳輸協定）伺服器可讓您集中維護使用者資訊。如果您將使用者資料庫儲存在環境中的LDAP伺服器上、您可以設定儲存系統、以便在現有的LDAP資料庫中查詢使用者資訊。

- 在設定LDAP ONTAP 以供使用之前、您應確認您的站台部署符合LDAP伺服器和用戶端組態的最佳實務做法。尤其必須符合下列條件：
  - LDAP伺服器的網域名稱必須符合LDAP用戶端上的項目。
  - LDAP伺服器支援的LDAP使用者密碼雜湊類型必須包含ONTAP 下列項目：
    - 加密（所有類型）和SHA-1（SHa、SSHA）。
    - 從ONTAP 《Sf9.8》、《SHA-2雜湊》（SHA-256、SSH-384、SHA-512、SSHA-256、 也支援SSHA-384和SSHA-512）。
  - 如果LDAP伺服器需要工作階段安全性措施、您必須在LDAP用戶端中進行設定。

    下列工作階段安全性選項可供使用：
    - LDAP簽署（提供資料完整性檢查）及LDAP簽署與密封（提供資料完整性檢查與加密）
    - 啟動TLS
    - LDAPS（LDAP over TLS或SSL）
  - 若要啟用已簽署和密封的LDAP查詢、必須設定下列服務：
    - LDAP伺服器必須支援GSPI（Kerberos）SASL機制。
    - LDAP伺服器必須在DNS伺服器上設定DNS A/AAAA記錄和PTr記錄。
    - Kerberos伺服器必須在DNS伺服器上存在SRV.記錄。
  - 若要啟用Start TLS或LDAPS、應考慮下列事項。
    - 使用Start TLS而非LDAPS是NetApp最佳實務做法。
    - 如果使用 LDAPS，則必須在ONTAP 9.5 及更高版本中為 TLS 或 SSL 啟用 LDAP 伺服器。 ONTAP 9.4 - 9.0 不支援 SSL。
    - 必須已在網域中設定憑證伺服器。
  - 若要啟用LDAP參照追蹤（ONTAP 在更新版本的版本中）、必須滿足下列條件：
    - 這兩個網域都應設定下列其中一個信任關係：
      - 雙向
      - 單向、主要信任參照網域
      - 父-子
    - DNS必須設定為解析所有參照的伺服器名稱。
    - 網域密碼應相同、以在何時進行驗證 `--bind-as-cifs-server` 設為 true 。

LDAP參照追蹤不支援下列組態。

- 所有ONTAP 版本：
- 管理SVM上的LDAP用戶端
- 適用於更新版本的支援功能（9.9.1及更新版本均支援）ONTAP ：
- LDAP 簽署與密封（ `-session-security` 選項）
- 加密 TLS 連線（ `-use-start-tls` 選項）
- 透過 LDAPS 連接埠 636 （ `-use-ldaps-for-ad-ldap` 選項）

- 從 ONTAP 9.11.1 開始，您可以使用"使用 LDAP 快速綁定對 ONTAP NFS SVM 進行 nsswitch 驗證。"
- 在SVM上設定LDAP用戶端時、您必須輸入LDAP架構。

  在大多數情況下、預設ONTAP 的架構之一將是適當的。不過、如果您環境中的LDAP架構與這些架構不同、則必須先建立新的LDAP用戶端架構ONTAP 以供使用、才能建立LDAP用戶端。請洽詢您的LDAP管理員、瞭解您環境的需求。

- 不支援使用LDAP進行主機名稱解析。

如需其他資訊、請參閱 "NetApp技術報告4835：如何在ONTAP 功能方面設定LDAP"。

了解 ONTAP NFS SVM 的 LDAP 簽章和密封

從ONTAP 功能支援功能支援功能支援功能支援功能、從功能支援功能支援功能升級至功能性管理功能。您必須在儲存虛擬機器（ SVM ）上設定 NFS 伺服器安全性設定、使其對應於 LDAP 伺服器上的設定。

簽署可確認LDAP有效負載資料使用秘密金鑰技術的完整性。「密封」會加密LDAP有效負載資料、以避免以純文字傳輸敏感資訊。「*LDAP*安全性層級」選項會指出LDAP流量是否需要簽署、簽署及密封、或兩者皆不需要。預設值為 `none`。測試

在 SVM 上啟用 SMB 流量的 LDAP 簽署與密封功能 `-session-security-for-ad-ldap` 選項 `vserver cifs security modify` 命令。

了解適用於 ONTAP NFS SVM 的 LDAPS

您必須瞭ONTAP 解有關如何保護LDAP通訊的某些詞彙與概念。支援使用start TLS或LDAPS、在Active Directory整合式LDAP伺服器或UNIX型LDAP伺服器之間設定驗證工作階段。ONTAP

術語

您應該瞭ONTAP 解某些詞彙、瞭解如何使用LDAPS來保護LDAP通訊安全。

- * LDAP *

（輕量型目錄存取傳輸協定）一種用於存取和管理資訊目錄的傳輸協定。LDAP是用來儲存使用者、群組和網路群組等物件的資訊目錄。LDAP也提供目錄服務、可管理這些物件並滿足LDAP用戶端的LDAP要求。

- * SSL *

  （安全通訊端層）一種通訊協定、專為透過網際網路安全傳送資訊而開發。ONTAP 9 及更新版本支援 SSL 、但已不再採用 TLS 。

- * TLS *

  （傳輸層安全性）一種根據舊版SSL規格追蹤傳輸協定的IETF標準。這是SSL的後續版本。ONTAP 9.5 及更新版本支援 TLS 。

- * LDAPS（LDAP over SSL或TLS）*

  一種傳輸協定、使用TLS或SSL來保護LDAP用戶端與LDAP伺服器之間的通訊安全。術語 *LDAP over SSL* 和 *LDAP over TLS* 有時會互換使用。ONTAP 9.5 及更新版本支援 LDAPS 。

  - 在ONTAP 9.8-9.5 中，LDAPS 只能在連接埠 636 上啟用。為此，請使用 `-use-ldaps-for-ad-ldap`參數 `vserver cifs security modify`命令。
  - 從ONTAP 推出《支援支援支援支援服務的支援服務：支援服務器支援服務」、從功能支援服務的支援服務開始、您可以在任何連接埠上啟用LDAPS、但連接埠636仍為預設若要這麼做，請將參數設定 `-ldaps-enabled`為 `true`，並指定所需的 `-port`參數。如"指令參考資料ONTAP"需詳細 `vserver services name-service ldap client create`資訊，請參閱。

  使用Start TLS而非LDAPS是NetApp最佳實務做法。

- 啟動**TLS**

  （也稱為_start_tls_、_startTLs_和_StartTLS）一種機制、可透過TLS傳輸協定提供安全的通訊。

  支援使用STARTTLS來保護LDAP通訊安全、並使用預設的LDAP連接埠（389）與LDAP伺服器通訊。ONTAPLDAP伺服器必須設定為允許透過LDAP連接埠389進行連線、否則SVM與LDAP伺服器之間的LDAP TLS連線將會失敗。

如何使用**LDAPS ONTAP**

支援TLS伺服器驗證、可讓SVM LDAP用戶端在連結作業期間確認LDAP伺服器的身分。ONTAP啟用TLS的LDAP用戶端可使用公開金鑰密碼編譯的標準技術、檢查伺服器的憑證和公開ID是否有效、以及是否已由用戶端信任CA清單中所列的憑證授權單位（CA）核發。

LDAP支援使用TLS加密通訊的ARTTLS。StartTLS會以純文字連線形式透過標準LDAP連接埠（389）開始、然後將該連線升級為TLS。

支援下列項目：ONTAP

- LDAPS用於Active Directory整合式LDAP伺服器與SVM之間的SMB相關流量
- LDAP流量的LDAPS、用於名稱對應和其他UNIX資訊

  Active Directory整合式LDAP伺服器或UNIX型LDAP伺服器均可用來儲存LDAP名稱對應和其他UNIX資訊的資訊、例如使用者、群組和網路群組。

- 自我簽署的根CA憑證

  使用Active Directory整合式LDAP時、會在網域中安裝Windows Server憑證服務時產生自我簽署的根憑證。使用UNIX LDAP伺服器進行LDAP名稱對應時、會使用適合該LDAP應用程式的方法、產生並儲存自我簽署的根憑證。

根據預設、LDAPS會停用。

為 ONTAP NFS SVM 啟用 LDAP RFC2307bis 支援

如果您想要使用LDAP並需要額外的功能來使用巢狀群組成員資格、您可以設定ONTAP 支援功能以啟用LDAP RFC2307bis。

開始之前

您必須已建立要使用的預設LDAP用戶端架構之一的複本。

關於這項工作

在LDAP用戶端架構中、群組物件使用memberUid屬性。此屬性可包含多個值、並列出屬於該群組的使用者名稱。在啟用RFC2307bis的LDAP用戶端架構中、群組物件會使用uniqueMember屬性。此屬性可包含LDAP目錄中其他物件的完整辨別名稱（DN）。這可讓您使用巢狀群組、因為群組可以有其他群組作為成員。

使用者不應是256個以上群組的成員、包括巢狀群組。不考慮超過256個群組限制的任何群組。ONTAP

根據預設、會停用RFC2307bis支援。

當ONTAP 使用MS -AD-BIS架構建立LDAP用戶端時、即可在功能上自動啟用RFC2307bis支援。

如需其他資訊、請參閱 "NetApp技術報告4835：如何在ONTAP 功能方面設定LDAP"。

步驟

1. 將權限層級設為進階：

   ```
   set -privilege advanced
   ```

2. 修改複製的RFC2307 LDAP用戶端架構、以啟用RFC2307bis支援：

   ```
   vserver services name-service ldap client schema modify -vserver vserver_name
   -schema schema-name -enable-rfc2307bis true
   ```

3. 修改架構以符合LDAP伺服器支援的物件類別：

   ```
   vserver services name-service ldap client schema modify -vserver vserver-name
   -schema schema_name -group-of-unique-names-object-class object_class
   ```

4. 修改架構以符合LDAP伺服器支援的屬性名稱：

   ```
   vserver services name-service ldap client schema modify -vserver vserver-name
   -schema schema_name -unique-member-attribute attribute_name
   ```

5. 返回管理權限層級：

```
set -privilege admin
```

用於 LDAP 目錄搜尋的 ONTAP NFS 設定選項

您可以設定ONTAP 支援使用者、群組和netgroup資訊等方式、將LDAP用戶端設定為以最適合您環境的方式連線至LDAP伺服器、藉此最佳化LDAP目錄搜尋。您需要瞭解預設的LDAP基礎和範圍搜尋值何時足夠、以及指定自訂值何時更合適的參數。

使用者、群組和netgroup資訊的LDAP用戶端搜尋選項、有助於避免LDAP查詢失敗、進而避免用戶端無法存取儲存系統。它們也有助於確保搜尋作業盡可能有效率、以避免用戶端效能問題。

預設基礎和範圍搜尋值

LDAP基礎是LDAP用戶端用來執行LDAP查詢的預設基礎DN。所有搜尋、包括使用者、群組和網路群組搜尋、都是使用基礎DN來完成。當您的LDAP目錄相對較小、且所有相關項目都位於相同的DN中時、此選項是適當的。

如果未指定自訂基礎 DN 、則預設值為 `root`。這表示每個查詢都會搜尋整個目錄。雖然如此一來、LDAP查詢的成功機會就會最大化、但效率卻會降低、而且大型LDAP目錄的效能也會大幅降低。

LDAP基礎範圍是LDAP用戶端用來執行LDAP查詢的預設搜尋範圍。所有搜尋、包括使用者、群組和netgroup搜尋、都是使用基礎範圍來完成。它決定LDAP查詢只搜尋命名項目、DN下一層的項目、或DN下的整個子樹狀結構。

如果未指定自訂基礎範圍、則預設為 `subtree`。這表示每個查詢都會搜尋DN下方的整個子樹狀結構。雖然如此一來、LDAP查詢的成功機會就會最大化、但效率卻會降低、而且大型LDAP目錄的效能也會大幅降低。

自訂基礎和範圍搜尋值

您也可以為使用者、群組和netgroup搜尋指定個別的基礎和範圍值。以這種方式限制搜尋基礎和查詢範圍、可大幅提升效能、因為它會將搜尋範圍限制在LDAP目錄的較小子部分。

如果指定自訂基礎和範圍值、則會覆寫一般預設搜尋基礎和範圍、以供使用者、群組和netgroup搜尋。可在進階權限層級使用指定自訂基礎和範圍值的參數。

LDAP用戶端參數…	指定自訂…
`-base-dn`	所有 LDAP 搜尋的基準 DN。如果需要，可以輸入多個值（例如，如果在 ONTAP 9.5 及更高版本中啟用了 LDAP 引用追蹤）。
`-base-scope`	所有 LDAP 搜尋的基本範圍。
`-user-dn`	所有 LDAP 使用者搜尋的基本 DN。此參數也適用於使用者名稱映射搜尋。
`-user-scope`	所有 LDAP 使用者搜尋的基本範圍。此參數也適用於使用者名稱映射搜尋。

`-group-dn`	所有 LDAP 群組搜尋的基本 DN。
`-group-scope`	所有 LDAP 群組搜尋的基本範圍。
`-netgroup-dn`	所有 LDAP 網路群組搜尋的基本 DN。
`-netgroup-scope`	所有 LDAP 網路組搜尋的基本範圍。

多個自訂基礎**DN**值

如果您的LDAP目錄結構較為複雜、您可能需要指定多個基礎DNS、以搜尋LDAP目錄的多個部分以取得特定資訊。您可以為使用者、群組和netgroup DN參數指定多個DNS、方法是以分號（；）分隔這些DNS、並以雙引號（"）括住整個DN搜尋清單。如果DN包含分號、您必須在DN中的分號前面新增轉義字元（\）。

請注意、此範圍適用於為對應參數指定的整個DNS清單。例如、如果您為使用者範圍指定三個不同使用者DNS和子樹狀結構的清單、則LDAP使用者會搜尋三個指定DNS中的每個子樹狀結構。

從ONTAP 功能介紹9.5開始、您也可以指定LDAP _Referring Chasing _、以便ONTAP 在主要LDAP伺服器未傳回LDAP參照回應時、讓該支援功能可將查詢要求參照到其他LDAP伺服器。用戶端會使用該參照資料、從參照資料中所述的伺服器擷取目標物件。若要搜尋參照LDAP伺服器中的物件、可將參照物件的基礎DN新增至基礎DN、做為LDAP用戶端組態的一部分。不過、只有在啟用參照追蹤（使用 `-referral-enabled true` 選項）。

自訂 **LDAP** 搜尋篩選器

您可以使用 LDAP 組態選項參數來建立自訂搜尋篩選器。此 `-group-membership-filter`參數指定從 LDAP 伺服器查詢群組成員資格時所使用的搜尋篩選器。

有效篩選的範例包括：

```
(cn=*99), (cn=1*), (|(cn=*22)(cn=*33))
```

深入瞭解 "如何在 ONTAP 中設定 LDAP"。

提高 **ONTAP NFS SVM** 的 **LDAP** 目錄網路群組按主機搜尋的效能

如果您的LDAP環境已設定為允許依主機進行網路群組搜尋、您可以設定ONTAP 支援使用此功能的支援、並依主機執行網路群組搜尋。如此可大幅加快網路群組搜尋速度、並減少網路群組搜尋期間的延遲所導致的NFS用戶端存取問題。

開始之前

您的 LDAP 目錄必須包含 `netgroup.byhost` 地圖。

您的DNS伺服器應同時包含NFS用戶端的轉送（A）和反轉（PTr）查詢記錄。

當您在netGroups中指定IPv6位址時、必須一律縮短並壓縮RFC 5952中指定的每個位址。

關於這項工作

NIS 伺服器會將網路群組資訊儲存在三個不同的對應中、稱為 `netgroup`、 `netgroup.byuser`和 `netgroup.byhost`。的用途 `netgroup.byuser` 和 `netgroup.byhost` 地圖是為了加速網路群組搜尋。支援在NIS伺服器上執行各主機的網路群組搜尋、以縮短掛載回應時間。ONTAP

根據預設、 LDAP 目錄沒有這樣的 `netgroup.byhost` 對應 NIS 伺服器。不過、在協力廠商工具的協助下、可以匯入 NIS `netgroup.byhost` 映射到 LDAP 目錄以啓用逐主機快速 netgroup 搜索。如果您已將 LDAP 環境設定為允許逐主機網路群組搜尋、則可以使用來設定 ONTAP LDAP 用戶端 `netgroup.byhost` 對應名稱、 DN 和搜尋範圍、可更快速地逐主機搜尋 netgroup-by host 。

當ONTAP NFS用戶端要求存取匯出時、若能更快接收各主機的網路群組搜尋結果、則可讓支援者更快處理匯出規則。如此可降低網路群組搜尋延遲問題導致存取延遲的機率。

步驟

1. 取得確切完整的 NIS 辨別名稱 `netgroup.byhost` 將您匯入 LDAP 目錄的對應。

   對應DN可能會因您用於匯入的協力廠商工具而異。若要獲得最佳效能、您應該指定確切的對應DN。

2. 將權限層級設為進階： `set -privilege advanced`
3. 在儲存虛擬機器（ SVM ）的 LDAP 用戶端組態中、啟用逐主機網路群組搜尋： `vserver services name-service ldap client modify -vserver vserver_name -client-config config_name -is-netgroup-byhost-enabled true -netgroup-byhost-dn netgroup-by-host_map_distinguished_name -netgroup-byhost-scope netgroup-by-host_search_scope`

   `-is-netgroup-byhost-enabled` {`true` `false`} 啓用或禁用逐主機對 LDAP 目錄的 netgroup 搜索。預設值為 `false`。

   `-netgroup-byhost-dn` `netgroup-by-host_map_distinguished_name` 指定的辨別名稱 `netgroup.byhost` 在 LDAP 目錄中對應。它會覆寫基礎DN、以便依主機搜尋網路群組。如果您未指定此參數、ONTAP 則使用基礎DN。

   `-netgroup-byhost-scope` {`base`|`onelevel` `subtree`} 指定 netgroup-by host 搜尋的搜尋範圍。如果您未指定此參數、則預設值為 `subtree`。

   如果 LDAP 用戶端組態尚不存在、您可以在使用建立新的 LDAP 用戶端組態時、指定這些參數來啟用逐主機網路群組搜尋 `vserver services name-service ldap client create` 命令。

   > 這 `-ldap-servers`字段替換 `-servers`字段。您可以使用 `-ldap-servers`欄位指定 LDAP 伺服器的主機名稱或 IP 位址。

4. 返回管理權限層級： `set -privilege admin`

範例

下列命令會修改名為「 `LDAP_corp` 」的現有 LDAP 用戶端組態、以使用啟用逐主機網路群組搜尋 `netgroup.byhost` 名爲 "`nisMapName="netgroup.byhost" 、 DC=corp 、 DC=example 、 DC=com 的地圖和默認搜索範圍 `subtree`：

```
cluster1::*> vserver services name-service ldap client modify -vserver vs1
-client-config ldap_corp -is-netgroup-byhost-enabled true -netgroup-byhost
-dn nisMapName="netgroup.byhost",dc=corp,dc=example,dc=com
```

完成後

。 `netgroup.byhost` 和 `netgroup` 目錄中的地圖必須隨時保持同步、以避免用戶端存取問題。

相關資訊

"IETF RFC 5952：IPv6位址文字呈現的建議"

使用 LDAP 快速綁定對 ONTAP NFS SVM 進行 nsswitch 驗證

從SURF9.11.1開始ONTAP 、您可以利用LDAP _fast bind_Functionality（也稱為_並行 連結）、以更快、更簡單的用戶端驗證要求。若要使用此功能、LDAP伺服器必須支援快速連結功能。

關於這項工作

如果沒有快速連結、ONTAP 則使用LDAP Simple Bind來驗證LDAP伺服器的管理使用者。利用這種驗證方法、ONTAP 將使用者或群組名稱傳送至LDAP伺服器、接收儲存的雜湊密碼、並將伺服器雜湊代碼與本機使用者密碼產生的雜湊密碼進行比較。如果完全相同、ONTAP 則此功能會授予登入權限。

利用快速連結功能、ONTAP 透過安全連線、僅將使用者認證（使用者名稱和密碼）傳送至LDAP伺服器。然後LDAP伺服器會驗證這些認證資料、並指示ONTAP 資訊技術授予登入權限。

快速連結的優點之一是ONTAP 、不需要支援LDAP伺服器所支援的每一種新雜湊演算法、因為密碼雜湊是由LDAP伺服器執行。

"深入瞭解如何使用快速連結。"

您可以使用現有的LDAP用戶端組態進行LDAP快速連結。不過、強烈建議將LDAP用戶端設定為TLS或LDAPS、否則密碼會以純文字透過線路傳送。

若要在ONTAP 整個環境中啟用LDAP快速連結、您必須滿足下列需求：

- 必須在支援快速連結的LDAP伺服器上設定支援使用者的支援。ONTAP
- 必須在名稱服務交換器（nsswitch）資料庫中設定LDAP的支援功能。ONTAP
- 必須使用FAST Bind設定NS交換 器驗證的使用者和群組帳戶。ONTAP

步驟

1. 請向LDAP管理員確認LDAP伺服器支援LDAP快速連結。
2. 確保ONTAP LDAP伺服器上已設定了這個使用者認證資料。
3. 確認已針對LDAP快速連結正確設定管理或資料SVM。

    a. 若要確認LDAP FAST Bind伺服器已列在LDAP用戶端組態中、請輸入：

    ```
    vserver services name-service ldap client show
    ```

"瞭解LDAP用戶端組態。"

b. 以確認 `ldap` 是 nsswitch 設定的來源之一 `passwd` 資料庫、輸入：

```
vserver services name-service ns-switch show
```

"深入瞭解nsswitch組態。"

4. 確保管理使用者正在使用nsswitch進行驗證、且其帳戶中已啟用LDAP快速連結驗證。

   - 對於現有使用者、請輸入 `security login modify` 並驗證下列參數設定：

     `-authentication-method nsswitch`

     `-is-ldap-fastbind true`

   如"指令參考資料ONTAP"需詳細 `security login modify`資訊，請參閱。

   - 對於新的管理員使用者，請參閱"啟用 LDAP 或 NIS ONTAP 帳戶存取"。

顯示 ONTAP NFS SVM 的 LDAP 統計資訊

您可以顯示儲存系統上的儲存虛擬機器 (SVM) 的 LDAP 統計訊息，以監控效能和診斷問題。

開始之前

- 您必須在SVM上設定LDAP用戶端。
- 您必須已識別可從中檢視資料的LDAP物件。

步驟

1. 檢視計數器物件的效能資料：

   ```
   statistics show
   ```

範例

下列範例顯示計數器名稱為 **SMPL_1** 的範例統計資料： Avg_processor_busy 和 CPU_busy

```
cluster1::*> statistics start -object system -counter
avg_processor_busy|cpu_busy -sample-id smpl_1
Statistics collection is being started for Sample-id: smpl_1

cluster1::*> statistics stop -sample-id smpl_1
Statistics collection is being stopped for Sample-id: smpl_1

cluster1::*> statistics show -sample-id smpl_1
Object: system
Instance: cluster
Start-time: 8/2/2012 18:27:53
End-time: 8/2/2012 18:27:56
Cluster: cluster1
   Counter                                                     Value
   -------------------------------- --------------------------------
   avg_processor_busy                                             6%
   cpu_busy
```

相關資訊

- "統計數據顯示"
- "統計開始"
- "統計停止"

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。