



Ask Me AI 助理

Information Security for Workload Factory

NetApp

September 16, 2026

目錄

Ask Me AI 助理	1
NetApp Workload Factory 的 Ask Me 安全性架構	1
Ask Me 中的 RAG 架構	1
多層提示安全性	1
模型資料隔離和隱私	1
工具使用和代理安全性	2
NetApp Workload Factory 的 Ask Me 存取控制	2
驗證	2
憑證保護和機密處理	2
基礎架構安全性	2
NetApp Workload Factory 的 Ask Me 執行模式	2
工具執行安全措施	3
輸出控制	3
NetApp Workload Factory 的 Ask Me 隱私權與可用度	3
資料處理和隱私	3
可用性和隔離控制	3

Ask Me AI 助理

NetApp Workload Factory 的 Ask Me 安全性架構

Ask Me 是內建於 NetApp Workload Factory 的生成式 AI 助手。它為 Amazon FSx for NetApp ONTAP 和 Workload Factory 主題提供即時的對話式支援。回應均基於經過驗證的 NetApp 文件，且 Ask Me 無法存取公共網際網路或使用客戶資料來訓練模型。多層安全性機制有助於區塊惡意查詢，將回應限制在支援的網域內，並防止使用者輸入覆寫系統指令。當 Ask Me 使用工具時，授權邊界、唯讀查詢強制執行、臨時沙箱和稽核記錄有助於約束和監控執行。

您可以隨時透過 Workload Factory 管理 設定選擇退出 Ask Me，這將停用您使用者帳戶的助理。["了解更多關於管理 GenAI 功能的資訊。"](#)

Ask Me 中的 RAG 架構

Ask Me 使用擷取增強生成（RAG）。

- 精心整理的知識庫：回覆基於經過驗證、已發佈的 NetApp 文件所組成的代管語料庫。
- 擷取評分與篩選：模型上下文中僅包含足夠相關的內容。
- 沒有網路存取：此模型無法取得、瀏覽或抓取外部內容。
- 來源標註：回覆包含所用來源文件的引用。

多層提示安全性

- 第 1 層：安全性分類器（LLM 作為評判者）封鎖惡意查詢（提示注入、權限提報、資料外洩、社交工程、原則違規）。

系統會記錄被封鎖的查詢，生成式模型永遠不會看到它們。

- 第 2 層：系統提示強化可防止使用者輸入覆寫系統指令。
- 第 3 層：網域範圍限制對 FSx ONTAP 和 Workload Factory 主題的回應。
- 第 4 層：工具使用治理在加固的沙箱中驗證參數並執行查詢；此模型不能執行任意操作。

模型資料隔離和隱私

- 沒有使用客戶資料進行模型訓練
- 要求層級隔離（無跨租戶資料外洩）
- 工作階段範圍的對話上下文，具有有限的歷史記錄
- 無持久模型記憶體容量
- 代管推論基礎架構

工具使用和代理安全性

- 授權範圍工具（強制執行使用者權限邊界）
- 嚴格的工具執行逾時
- 用於擷取資料的臨時性、工作階段範圍沙箱
- 使用允許清單強制執行唯讀查詢
- 工具呼叫稽核及敏感參數清理

NetApp Workload Factory 的 Ask Me 存取控制

在 NetApp Workload Factory 中，Ask Me 存取安全性的核心在於經過驗證的工作階段、使用者層級的責任歸屬，以及在執行階段作業期間受保護的機密處理。驗證控制會驗證每個工作階段，並將互動與特定使用者建立關聯。敏感憑證會在執行階段從代管的機密保存庫中擷取，並從記錄中刪除。該服務也套用基礎架構控制，包括非根目錄 Container 執行和受限的 CORS 允許清單。

驗證

- 使用加密驗證進行簽署 JWT 驗證（包括對象、發行者和演算法檢查，例如 RS256）
- 服務邊界處的中介軟體強制驗證
- 使用者身分範圍限定，以便將互動歸因於特定使用者

憑證保護和機密處理

- 安全保存庫儲存設備：服務使用的敏感憑證儲存在代管的機密保存庫中，並在執行階段擷取。應用程式程式碼、組態檔案或 Container 映像檔中均不儲存任何機密。
- 日誌清理：在寫入日誌之前，會將敏感值（認證、權杖、密碼、存取金鑰、憑證）從日誌中遮蔽。

基礎架構安全性

- 非根目錄 Container 執行
- CORS 僅限於受信任 NetApp 網域的明確允許清單

NetApp Workload Factory 的 Ask Me 執行模式

NetApp Workload Factory 為 Ask Me 提供多種執行模式，每種模式都有不同的安全性和隱私特性。當 Ask Me 使用工具整合時（例如查詢客戶本身的 Workload Factory 資源），工具的執行會透過分層防護來控制。啟用工具的執行會在經過驗證的使用者權限範圍內運作，並對每次操作的持續時間和範圍套用限制。擷取到的資料會保留在短暫的工作階段沙箱中，該沙箱會封鎖外部存取，並在工作階段結束時毀損。獨立的提示與程式碼控制會強制執行唯讀查詢，而稽核記錄會擷取工具活動，並清除敏感值。

工具執行安全措施

- 授權範圍工具在已驗證使用者的權限範圍內運作。
- 工具執行逾時限制了長時間運行的操作。
- 臨時資料沙箱將工具檢索的資料儲存在工作階段範圍內，阻止外部存取、檔案 I/O、網路呼叫和引擎層級的擴充載入，並在工作階段結束時毀損。
- 唯讀查詢強制執行透過嚴格的允許清單來驗證產生的查詢。
- 提示強制執行與程式碼強制執行的安全性會獨立套用。
- 工具呼叫稽核會記錄工具名稱、參數、時間戳記和結果狀態，並進行敏感值清理。

輸出控制

- Token 限制執行
- 用於分類/安全性關鍵操作的確定性輸出（溫度 0）
- 具有提前終止與清理的串流

NetApp Workload Factory 的 Ask Me 隱私權與可用度

在 NetApp Workload Factory 中，Ask Me 隱私控制可限制資料暴露，讓工作階段處理保持隔離的，並維護使用者互動的隱私邊界。您的輸入由代管 AI 服務處理，該服務不會使用這些資料來訓練或改進基礎模型。擷取到的操作資料在工作階段期間保留在短暫的記憶體儲存設備中，不會持久化或是共享的。跨多個雲端區域的多模型後援鍵可在主要模型受限或無法使用時支援可用度，同時相同的安全性控制適用於所有後援模型。

資料處理和隱私

- 提示中的使用者資料：由代管 AI 服務處理，該服務不會使用您的輸入來訓練或改進基礎模型。
- 知識庫內容：僅包含精選、已發佈的 NetApp 文件；不包含您的資料。
- 操作資料：僅當使用者查詢自己的資源時才會擷取；在工作階段期間保存在短暫的記憶體容量儲存設備中，不會持續保留或共享的。
- 稽核記錄：已記錄查詢中繼資料（匿名使用者 ID、時間戳記、持續時間），並清理敏感欄位。
- 回饋資料：單獨儲存並與查詢 ID 關聯，不與匿名使用者 ID 以外的個人識別資訊關聯。

可用性和隔離控制

Ask Me 採用跨多個雲端區域的多模型回退鍵。

如果主模型受到限制或無法使用，系統可以容錯移轉至替代模型。

所有模型均受到相同的安全性控制、系統提示強化與隔離保證所規範。

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。