



勒索軟體保護文件 Ransomware Protection

NetApp
May 03, 2022

目錄

勒索軟體保護文件	1
勒索軟體保護的新功能	2
2022年3月15日	2
2022年2月9日	2
開始使用	3
深入瞭解勒索軟體保護	3
使用勒索軟體保護	5
管理資料來源的網路安全建議	5
知識與支援	11
註冊以取得支援	11
取得協助	12
法律聲明	14
版權	14
商標	14
專利	14
隱私權政策	14
開放原始碼	14

勒索軟體保護文件

勒索軟體保護的新功能

瞭解勒索軟體保護的新功能。

2022年3月15日

新的面板可追蹤業務關鍵資料的權限狀態

新的「業務關鍵資料權限分析」面板會顯示資料的權限狀態、這對您的業務而言至關重要。如此一來、您就能快速評估保護業務關鍵資料的能力。 ["如需詳細資料、請前往此處"](#)。

「開放權限」區域現在包括**OneDrive**和**SharePoint**帳戶

勒索軟體保護儀表板中的「開放權限」區域現在包含OneDrive帳戶和SharePoint帳戶中掃描檔案的權限。

2022年2月9日

全新勒索軟體保護服務

全新的勒索軟體保護服務可讓您檢視網路安全相關資訊、並評估資料對網路攻擊的恢復能力。它也提供警示與修正清單、讓您的資料更安全。

["深入瞭解這項新服務"](#)。

開始使用

深入瞭解勒索軟體保護

勒索軟體攻擊可能會耗費一定的時間、資源和商譽。勒索軟體保護服務可讓您檢視網路安全的相關資訊、並評估資料對網路攻擊的恢復能力。它也提供警示與修正清單、讓您的資料更安全。

["瞭解勒索軟體保護的使用案例"](#)。



勒索軟體保護服務目前是試用版產品。

功能

勒索軟體保護目前提供多項功能、可協助您保護網路儲存設備。未來將會新增其他功能。目前功能可識別下列時機：

- 您工作環境中的磁碟區無法透過使用建立備份至雲端來保護 ["雲端備份"](#)。
- 您工作環境中的資料和資料來源並未使用進行掃描 ["雲端資料感測"](#) 找出法規遵循與隱私權方面的考量、並找出最佳化商機。
- 在工作環境或資料來源中、加密檔案的百分比出現異常增加。

這可能是勒索軟體攻擊在您的網路上開始的指標。

- 敏感資料位於檔案中、而在工作環境或資料來源中、存取權限等級太高。
- 使用者已新增至Active Directory網域管理員群組。

["請參閱勒索軟體保護儀表板、瞭解如何檢視這些潛在問題。"](#)

使用Cloud Volumes ONTAP VMware系統時、您可以直接從工作環境部署一些額外的勒索軟體保護功能。 ["瞭解如何新增額外的勒索軟體保護功能"](#)。

支援的工作環境和資料來源

["雲端資料感測"](#) 是使用勒索軟體保護服務的先決條件。在安裝並啟動Data Sense之後、您可以使用勒索軟體保護功能來瞭解資料對於下列類型的工作環境和資料來源的網路攻擊有多強彈性：

工作環境：

- （部署於AWS、Azure或GCP）Cloud Volumes ONTAP
- 內部部署 ONTAP 的叢集
- Azure NetApp Files
- Amazon FSX for ONTAP Sx
- Amazon S3

資料來源：

- 非NetApp檔案共用
- 物件儲存（使用S3傳輸協定）
- 資料庫
- OneDrive 帳戶
- SharePoint帳戶

勒索軟體保護功能也會監控您的全域Active Directory組態（若有） ["在Cloud Data意義上設定此功能"](#)。

勒索軟體保護的運作方式

在高層級的勒索軟體保護、運作方式如下：

1. 勒索軟體保護會從Cloud Data Sense、Cloud Backup及其他Cloud Manager資源收集資訊、以填入勒索軟體保護儀表板。
2. 您可以使用勒索軟體保護儀表板來取得系統保護程度的總覽。
3. 您可以使用所提供的報告工具來協助保護網路儲存設備。

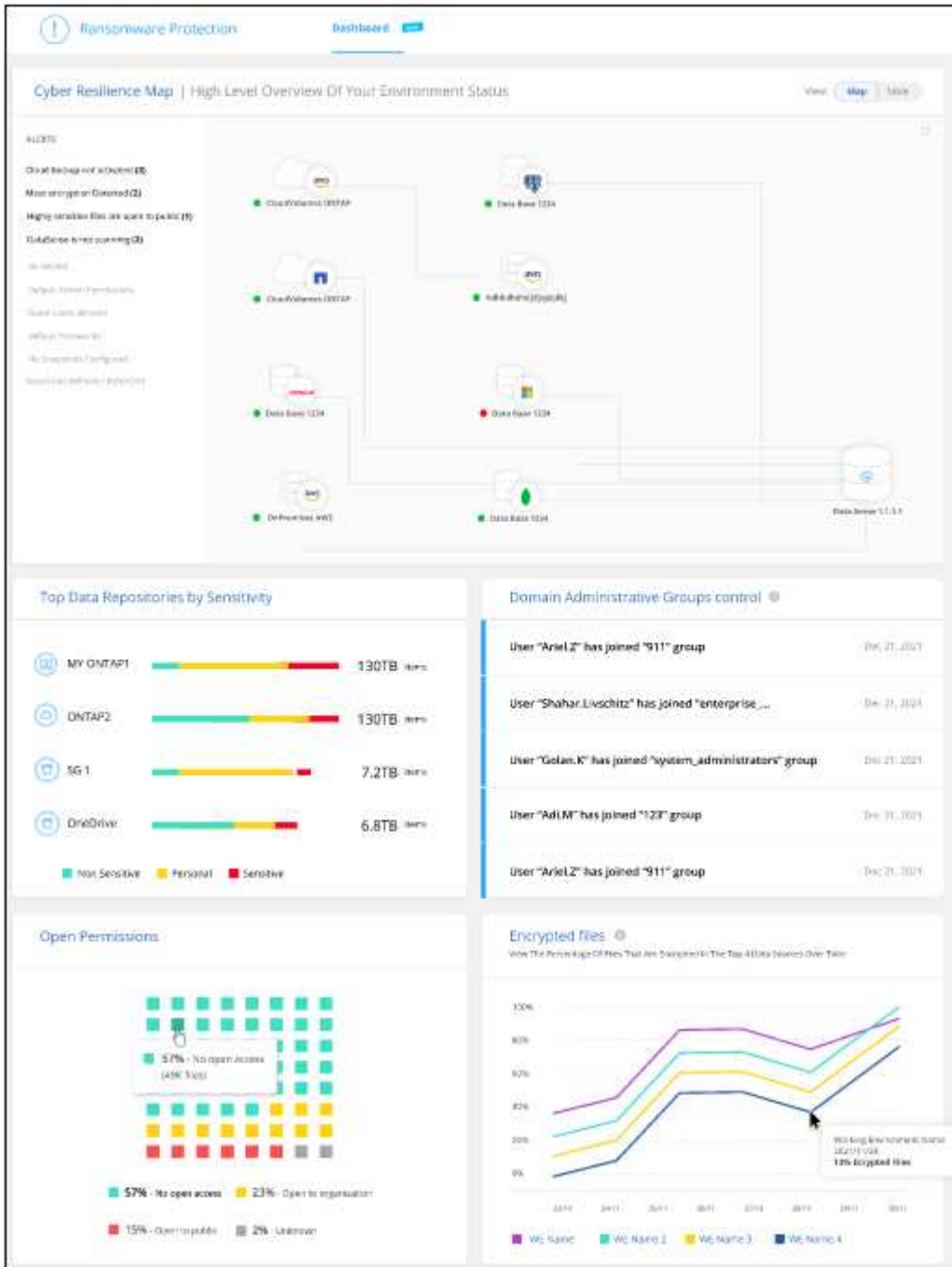
成本

試用版期間的勒索軟體保護服務不需另外付費。

使用勒索軟體保護

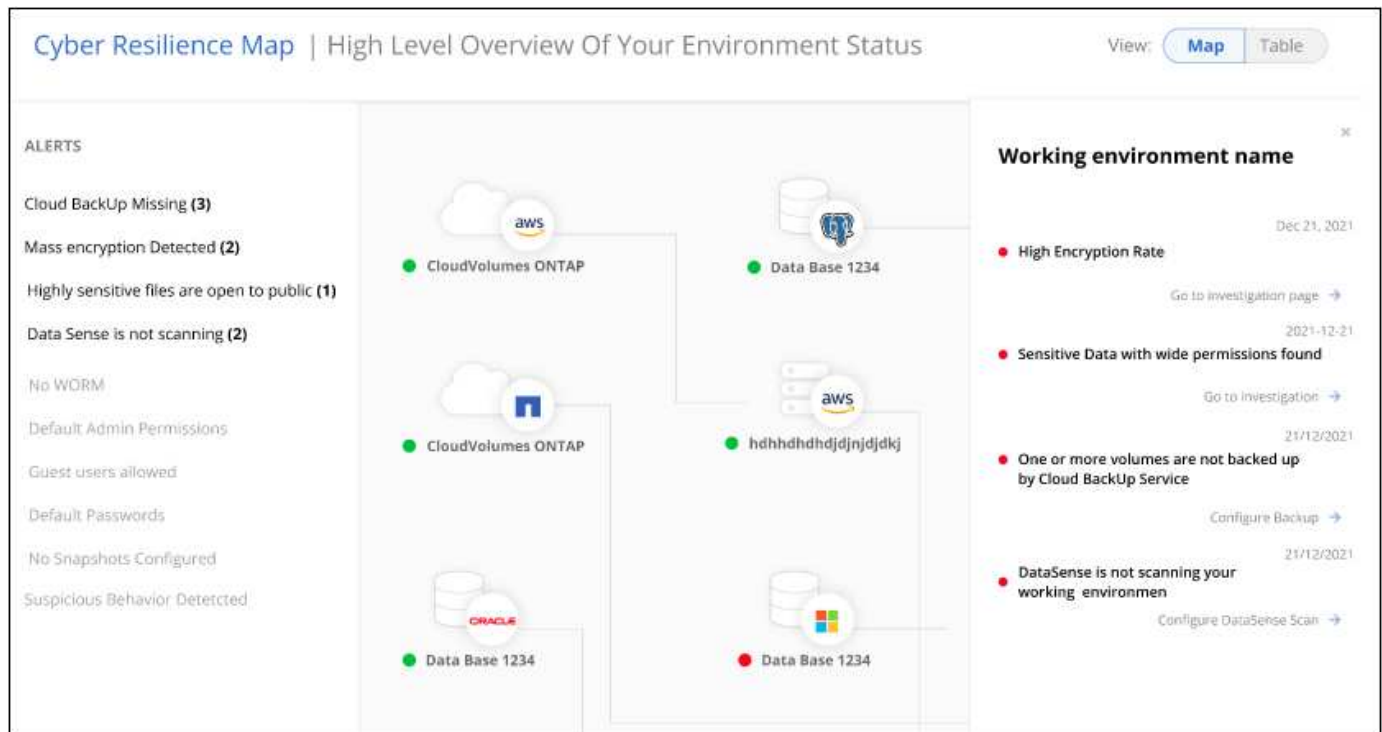
管理資料來源的網路安全建議

使用勒索軟體保護儀表板檢視所有工作環境和資料來源的網路恢復能力總覽。您可以深入瞭解每個區域、以瞭解更多詳細資料和可能的修正。



網路恢復地圖

網路還原地圖是儀表板的主要區域。它可讓您以視覺化的方式查看所有工作環境和資料來源、並能檢視相關的網路恢復能力資訊。



地圖由三個部分組成：

左側面板

顯示服務正在監控所有資料來源的警示清單。也會指出您環境中每個作用中警示的數目。有大量一種警示類型、可能是嘗試先解決這些警示的好理由。

中央面板

以圖形格式顯示所有資料來源、服務和Active Directory。健全的環境具有綠色指標、而具有警示的環境則有紅色指標。

右側面板

按一下具有紅色指標的資料來源之後、此面板會顯示該資料來源的警示、並提供解決警示的建議。警示會排序、以便先列出最新的警示。許多建議都會引導您選擇另一項Cloud Manager服務、以便解決此問題。

這些是目前追蹤的警示和建議的修正。

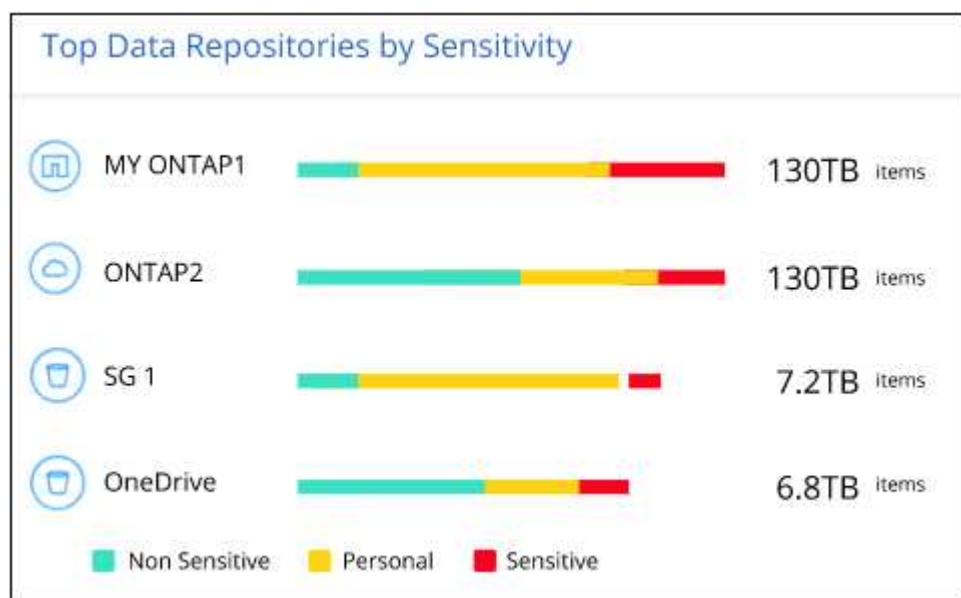
警示	說明	補救
偵測到高資料加密率	資料來源中加密檔案或毀損檔案的百分比發生異常增加。這表示在過去7天內、加密檔案的百分比增加超過20%。例如、如果50%的檔案已加密、則一天之後此數字會增加至60%、您會看到此警示。	按一下連結以啟動 " 資料感應調查頁面 "。您可以在其中選取特定_Working Environment_和_Category（加密和毀損）_的篩選器、以檢視所有加密和毀損檔案的清單。
找到具有廣泛權限的敏感資料	敏感資料位於檔案中、而資料來源的存取權限等級太高。	按一下連結以啟動 " 資料感應調查頁面 "。您可以在其中選取特定_Working Environment_、_Sensitivity Level（敏感個人）_和_Open權限_的篩選條件、以檢視發生此問題的檔案清單。

警示	說明	補救
一或多個磁碟區未使用Cloud Backup備份	工作環境中的部分磁碟區未受到使用保護 "雲端備份"。	按一下連結以啟動Cloud Backup、然後您可以識別工作環境中未備份的磁碟區、然後決定是否要在這些磁碟區上啟用備份。
Data Sense不會掃描資料來源中的一或多個儲存庫（磁碟區、儲存區等）	您的資料來源中有些資料並未使用進行掃描 "雲端資料感測" 找出法規遵循與隱私權方面的考量、並找出最佳化商機。	按一下連結以啟動「Data Sense（資料感測）」、並針對未掃描的項目啟用掃描與對應功能。

依資料敏感度排名第一的資料儲存庫

「_依敏感度等級_排名前四的資料儲存庫」面板最多會列出包含最敏感項目的前四個資料儲存庫（工作環境和資料來源）。每個工作環境的長條圖分為：

- 非敏感資料
- 個人資料
- 敏感的個人資料



您可以將游標停留在每個區段上、查看每個類別中的項目總數。

按一下每個區域、即可在「Data Sense Investigation」（資料感測調查）頁面中檢視篩選後的結果、以便進一步調查。

網域管理員群組控制項

「網域管理員群組」控制面板會顯示最近新增至網域系統管理員群組的使用者、以便您查看這些群組中是否允許所有使用者。您必須擁有 "整合全域Active Directory" 此面板可在Cloud Data感應中使用。

Domain Administrative Groups control ⓘ	
User "Ariel.Z" has joined "911" group	Dec 21, 2021
User "Shahar.Livschitz" has joined "enterprise_..."	Dec 21, 2021
User "Golan.K" has joined "system_administrators" group	Dec 21, 2021
User "Adi.M" has joined "123" group	Dec 21, 2021

預設的管理管理群組包括「系統管理員」、「網域管理員」、「企業系統管理員」、「企業金鑰管理員」及「金鑰管理員」。

依開啟權限類型列出的資料

「開啟權限」面板會顯示所有要掃描檔案的每種權限類型百分比。此圖表是以Data Sense提供、並顯示下列權限類型：

- 無開放存取權
- 開放給組織使用
- 開放給大眾使用
- 不明存取

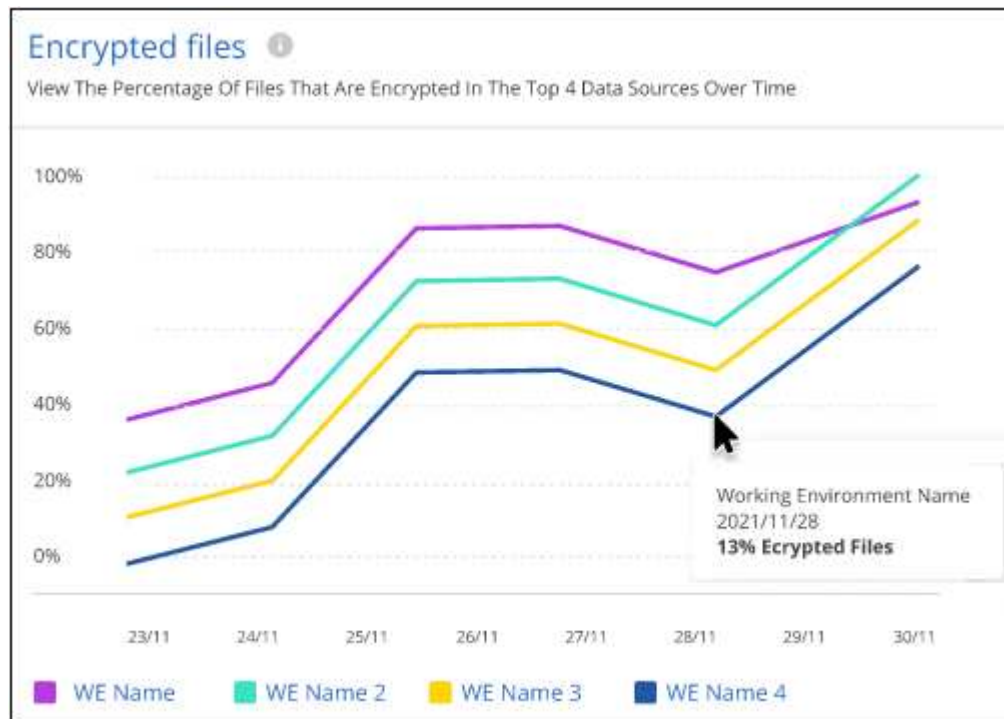


您可以將游標停在每個區段上、查看每個類別中的檔案百分比和總數。

按一下每個區域、即可在「Data Sense Investigation」（資料感測調查）頁面中檢視篩選後的結果、以便進一步調查。

以加密檔案列出的資料

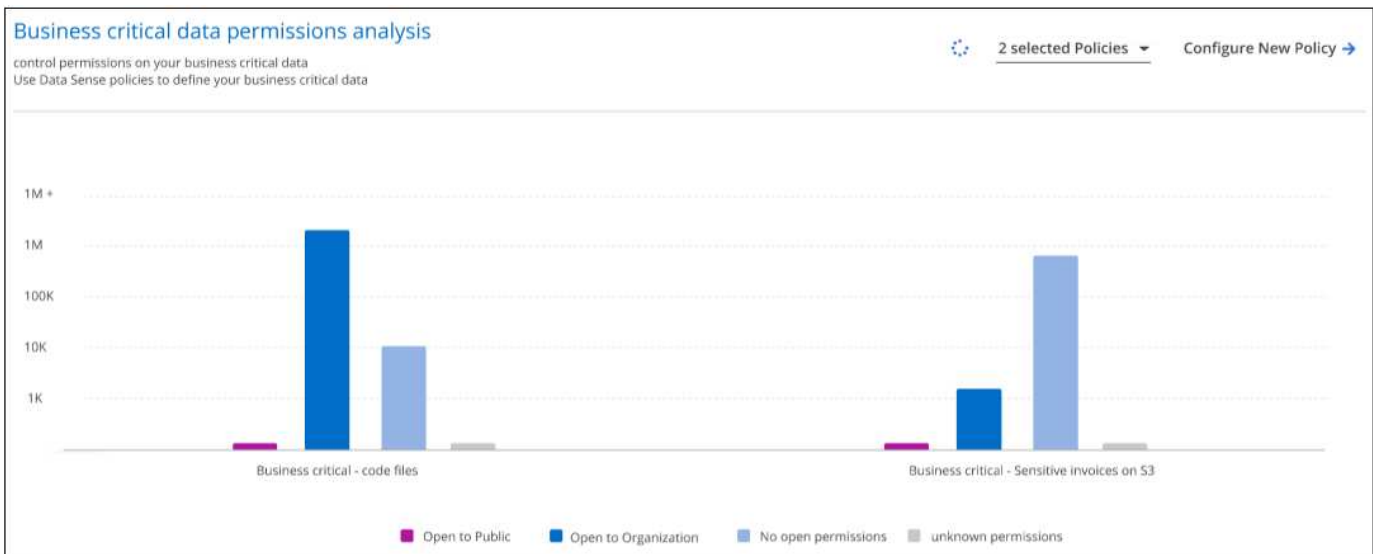
「加密檔案」面板會顯示前4大資料來源、其檔案經過一段時間加密的百分比最高。這些項目通常是受密碼保護的項目。它會比較過去7天的加密速率、以查看哪些資料來源的資料增加率超過20%。增加此金額可能表示勒索軟體已經攻擊您的系統。



按一下其中一個資料來源的一行、即可在「Data Sense Investigation」（資料感測調查）頁面中檢視篩選後的結果、以便進一步調查。

關鍵業務資料的權限狀態

「業務關鍵資料權限分析」面板會顯示資料的權限狀態、這對您的業務而言至關重要。如此一來、您就能快速評估保護業務關鍵資料的能力。



此面板一開始沒有資料、因為資料只會在您選取所建立的Data Sense *Policies*（資料感測_原則）來檢視最重要的商業資料之後填入。瞭解如何操作 "[使用Data Sense建立原則](#)"。

在此面板中新增最多2個原則之後、圖表會顯示符合原則條件之所有資料的權限分析。它會列出下列項目數量：

- 開放給大眾使用：Data Sense認為公開的項目
- 開放給組織權限：Data Sense認為對組織開放的項目
- 無開放式權限：Data有意義的項目、將其視為無開放式權限
- 未知權限：Data有意義視為未知權限的項目

將游標移到圖表中的每個長條上、即可檢視每個類別中的結果數目。按一下長條圖、就會顯示「Data Sense Investigation」（資料感測調查）頁面、以便進一步調查哪些項目具有開啟權限、以及您是否應該調整檔案權限。

知識與支援

註冊以取得支援

在您透過NetApp技術支援開啟支援案例之前、您必須先將NetApp支援網站帳戶新增至Cloud Manager、然後註冊以取得支援。

新增一個NSS帳戶

「支援儀表板」可讓您從單一位置新增及管理所有NetApp支援網站帳戶。

步驟

1. 如果您還沒有 NetApp 支援網站帳戶、"註冊一項"。
2. 在Cloud Manager主控台右上角、按一下「說明」圖示、然後選取*「支援」*。



3. 按一下「」 「nss管理」 > 「新增nssAccount」。
4. 出現提示時、按一下*繼續*以重新導向至Microsoft登入頁面。

NetApp使用Microsoft Azure Active Directory做為身分識別供應商、提供專為支援與授權所設計的驗證服務。

5. 在登入頁面上、提供您的NetApp支援網站註冊電子郵件地址和密碼、以執行驗證程序。

此動作可讓Cloud Manager使用您的NSS帳戶。

附註：帳戶必須是客戶層級的帳戶（非來賓帳戶或臨時帳戶）。

註冊您的帳戶以取得支援

支援註冊可從支援儀表板的Cloud Manager取得。

步驟

1. 在Cloud Manager主控台右上角、按一下「說明」圖示、然後選取*「支援」*。



2. 在* Resources（資源）選項卡中，單擊 Register for Support*（註冊以獲得支持*）。
3. 選取您要登錄的NSS認證、然後按一下「登錄」。

取得協助

NetApp以多種方式支援Cloud Manager及其雲端服務。我們全年無休提供豐富的免費自助支援選項、例如知識庫（KB）文章和社群論壇。您的支援註冊包括透過網路票證提供遠端技術支援。

自我支援

這些選項可供免費使用、一天24小時、一週7天：

- "知識庫"

請搜尋Cloud Manager知識庫、找出有助於疑難排解問題的文章。

- "社群"

加入Cloud Manager社群、追蹤後續討論或建立新討論。

- 文件

您目前正在檢視的Cloud Manager文件。

- mailto：ng-cloudmanager-feedback@netapp.com [意見反應電子郵件]

我們非常重視您的意見。提交意見反應、協助我們改善Cloud Manager。

NetApp支援

除了上述的自我支援選項、您也可以與NetApp支援工程師合作、在您啟動支援之後解決任何問題。

步驟

1. 在Cloud Manager中、按一下*「說明」>「支援」*。
2. 在「Technical Support（技術支援）」下選擇可用的選項之一：
 - a. 按一下*致電我們*以尋找NetApp技術支援的電話號碼。
 - b. 按一下「開啟問題」、選取其中一個選項、然後按一下「傳送」。

NetApp代表將審查您的案例、並盡快回覆您。

法律聲明

法律聲明提供版權聲明、商標、專利等存取權限。

版權

<http://www.netapp.com/us/legal/copyright.aspx>

商標

NetApp、NetApp 標誌及 NetApp 商標頁面上列出的標章均為 NetApp、Inc. 的商標。其他公司與產品名稱可能為其各自所有者的商標。

<http://www.netapp.com/us/legal/netapptmlist.aspx>

專利

如需最新的 NetApp 擁有專利清單、請參閱：

<https://www.netapp.com/us/media/patents-page.pdf>

隱私權政策

<https://www.netapp.com/us/legal/privacypolicy/index.aspx>

開放原始碼

通知檔案提供有關 NetApp 軟體所使用之協力廠商版權與授權的資訊。

- ["Cloud Manager 3.9 注意事項"](#)

Copyright Information

Copyright © 2022 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.