



NetApp July 10, 2024

This PDF was generated from https://docs.netapp.com/zh-tw/ontap/authentication/dynamic-authorization-overview.html on July 10, 2024. Always check docs.netapp.com for the latest.

# 目錄

管	理動態授權	1
	動態授權總覽	1
	啟用或停用動態授權	1
	自訂動態授權	3

# 管理動態授權

# 動態授權總覽

從 ONTAP 9.15.1 開始、系統管理員可以設定並啟用動態授權、以提高遠端存取 ONTAP 的安全性、同時降低惡意攻擊者可能造成的潛在損害。有了 ONTAP 9.15.1 、動態授權提 供了一個初始架構、可將安全分數指派給使用者、如果他們的活動看起來可疑、則可透過 額外的授權檢查來挑戰他們、或是完全拒絕作業。系統管理員可以建立規則、指派信任分 數、以及限制命令、以決定何時允許或拒絕使用者的特定活動。系統管理員可以在整個叢 集範圍內啟用動態授權、或是為個別的儲存 VM 啟用授權。

## 動態授權的運作方式

動態授權使用信任評分系統、根據授權原則、將不同的信任等級指派給使用者。根據使用者的信任層級、可以允許或拒絕他們執行的活動、也可以提示使用者進行進一步驗證。

以嘗試刪除磁碟區的三個不同使用者為例。在他們嘗試執行作業時、會檢查每位使用者的風險等級:

- 第一位使用者在正常上班時間從信任的裝置登入、這使得她的風險等級偏低;無需額外驗證即可執行作業。
- 第二位使用者在下班時間從家中的受信任裝置登入、風險等級較低;在允許操作之前、系統會提示她進行額 外驗證。
- 第三位使用者在辦公時間以外的新位置從不受信任的裝置登入、因此風險等級較高、因此不允許進行此作業。
- 下一步
  - •"自訂動態授權"
  - "啟用或停用動態授權"

# 啟用或停用動態授權

從 ONTAP 9.15.1 開始、系統管理員可以在中設定及啟用動態授權 visibility 測試組態的模式、或在中 enforced 模式、可啟動透過 SSH 連線的 CLI 使用者組態。如果您不再需要動態授權、可以停用它。當您停用動態授權時、組態設定會保持可用狀態、如果您決定重新啟用、您可以稍後再使用。

如需的參數詳細資訊、請參閱 security dynamic-authorization modify 命令、請參閱 ONTAP 手冊頁。

#### 啟用動態授權以進行測試

您可以在可見度模式中啟用動態授權、藉此測試功能、並確保使用者不會被意外鎖定。在此模式中、信任分數會 針對每個受限活動進行檢查、但不會強制執行。但是、任何會被拒絕或受到其他驗證挑戰的活動都會記錄下來。 最佳實務做法是先在此模式中測試您想要的設定、然後再執行設定。



即使您尚未設定任何其他動態授權設定、也可以依照此步驟第一次啟用動態授權。請參閱 "自訂 動態授權" 針對設定其他動態授權設定的步驟、將其自訂至您的環境。

步驟

1. 設定全域設定並將功能狀態變更為、即可在可見度模式中啟用動態授權 visibility。如果您不使用 -vserver 參數、命令會在叢集層級執行。更新括弧 <> 中的值以符合您的環境。必須使用粗體參數:

```
security dynamic-authorization modify \
<strong>-state visibility</strong> \
-lower-challenge-boundary <percent> \
-upper-challenge-boundary <percent> \
-suppression-interval <interval> \
-vserver <storage_VM_name>
```

2. 使用檢查結果 show 顯示全域組態的命令:

security dynamic-authorization show

# 在強制模式中啟用動態授權

您可以在強制模式中啟用動態授權。一般而言、在使用可見度模式完成測試之後、您會使用此模式。在此模式 中、每個受限活動都會檢查信任分數、如果符合限制條件、則會強制執行活動限制。也會強制執行抑制間隔、以 防止在指定時間間隔內發生其他驗證挑戰。



此步驟假設您先前已在中設定並啟用動態授權 visibility 強烈建議使用模式。

步驟

1. 在中啟用動態授權 enforced 模式、將其狀態變更為 enforced。如果您不使用 -vserver 參數、命令會 在叢集層級執行。更新括弧 <> 中的值以符合您的環境。必須使用粗體參數:

```
security dynamic-authorization modify \
<strong>-state enforced</strong> \
-vserver <storage VM name>
```

2. 使用檢查結果 show 顯示全域組態的命令:

security dynamic-authorization show

## 停用動態授權

如果不再需要新增的驗證安全性、您可以停用動態授權。

#### 步驟

1. 將動態授權狀態變更為、以停用動態授權 disabled。如果您不使用 -vserver 參數、命令會在叢集層級 執行。更新括弧 <> 中的值以符合您的環境。必須使用粗體參數:

security dynamic-authorization modify \
<strong>-state disabled</strong> \
-vserver <storage VM name>

2. 使用檢查結果 show 顯示全域組態的命令:

security dynamic-authorization show

# 下一步

(選用)視您的環境而定、請參閱 "自訂動態授權" 設定其他動態授權設定。

# 自訂動態授權

身為管理員、您可以自訂動態授權組態的不同層面、以提高遠端系統管理員 SSH 連線至 ONTAP 叢集的安全性。

您可以根據安全需求自訂下列動態授權設定:

- [設定動態授權全域設定]
- [設定動態授權信任分數元件]
- [設定自訂信任分數提供者]
- •[設定受限命令]
- [設定動態授權群組]

設定動態授權全域設定

您可以設定動態授權的全域設定、包括要保護的儲存 VM 、驗證挑戰的抑制時間間隔、以及信任分數設定。

如需有關的參數和預設值的詳細資訊 security dynamic-authorization modify 命令、請參閱 ONTAP 手冊頁。

步驟

 設定動態授權的全域設定。如果您不使用 -vserver 參數、命令會在叢集層級執行。更新括弧 <> 中的值以 符合您的環境:

```
security dynamic-authorization modify \
-lower-challenge-boundary <percent> \
-upper-challenge-boundary <percent> \
-suppression-interval <interval> \
-vserver <storage_VM_name>
```

2. 檢視產生的組態:

security dynamic-authorization show

## 設定受限命令

啟用動態授權時、此功能會包含一組預設的限制命令。您可以修改此清單以符合您的需求。請參閱 "多重管理驗 證( MAV )文件" 以取得受限命令的預設清單資訊。

#### 新增受限制的命令

您可以將命令新增至受限於動態授權的命令清單。

如需有關的參數和預設值的詳細資訊 security dynamic-authorization rule create 命令、請參閱 ONTAP 手冊頁。

步驟

1. 新增命令。更新括弧 <> 中的值以符合您的環境。如果您不使用 -vserver 參數、命令會在叢集層級執行。 必須使用粗體參數:

```
security dynamic-authorization rule create \
-query <query> \
<strong>-operation <text></strong> \
-index <integer> \
-vserver <storage VM name>
```

2. 檢視所產生的限制命令清單:

security dynamic-authorization rule show

#### 移除受限制的命令

您可以從受限於動態授權的命令清單中移除命令。

如需有關的參數和預設值的詳細資訊 security dynamic-authorization rule delete 命令、請參閱 ONTAP 手冊頁。

步驟

1. 移除命令。更新括弧 <> 中的值以符合您的環境。如果您不使用 -vserver 參數、命令會在叢集層級執行。 必須使用粗體參數:

```
security dynamic-authorization rule delete \
<strong>-operation <text></strong> \
-vserver <storage VM name>
```

2. 檢視所產生的限制命令清單:

security dynamic-authorization rule show

### 設定動態授權群組

根據預設、動態授權會在您啟用後立即套用至所有使用者和群組。不過、您可以使用建立群組 security dynamic-authorization group create 因此動態授權僅適用於這些特定使用者。

新增動態授權群組

您可以新增動態授權群組。

如需有關的參數和預設值的詳細資訊 security dynamic-authorization group create 命令、請參閱 ONTAP 手冊頁。

步驟

建立群組。更新括弧 <> 中的值以符合您的環境。如果您不使用 -vserver 參數、命令會在叢集層級執行。
 必須使用粗體參數:

```
security dynamic-authorization group create \
<strong>-group-name <group-name></strong> \
-vserver <storage_VM_name> \
-exclude-users <user1,user2,user3...>
```

#### 2. 檢視產生的動態授權群組:

security dynamic-authorization group show

移除動態授權群組

您可以移除動態授權群組。

步驟

1. 删除群組。更新括弧 <> 中的值以符合您的環境。如果您不使用 -vserver 參數、命令會在叢集層級執行。

必須使用粗體參數:

security dynamic-authorization group delete \
<strong>-group-name <group-name></strong> \
-vserver <storage VM name>

2. 檢視產生的動態授權群組:

security dynamic-authorization group show

# 設定動態授權信任分數元件

您可以設定最大分數權重、以變更評分準則的優先順序、或移除風險評分的特定準則。



最佳做法是保留預設分數權重值、並在需要時才進行調整。

如需有關的參數和預設值的詳細資訊 security dynamic-authorization trust-score-component modify 命令、請參閱 ONTAP 手冊頁。

以下是您可以修改的元件、以及其預設分數和百分比權重:

準則	元件名稱	預設原始分數權重	預設百分比權重
信任的裝置	trusted-device	20.	50
使用者登入驗證記錄	authentication- history	20.	50

步驟

1. 修改信任分數元件。更新括弧 <> 中的值以符合您的環境。如果您不使用 -vserver 參數、命令會在叢集層 級執行。必須使用粗體參數:

```
security dynamic-authorization trust-score-component modify \
<strong>-component <component-name></strong> \
<strong>-weight <integer></strong> \
-vserver <storage_VM_name>
```

2. 檢視產生的信任分數元件設定:

security dynamic-authorization trust-score-component show

如果使用者因系統原則而遭拒存取、且能夠證明其身分識別、則系統管理員可以重設使用者的信任分數。

如需有關的參數和預設值的詳細資訊 security dynamic-authorization user-trust-score reset 命令、請參閱 ONTAP 手冊頁。

步驟

 新增命令。請參閱 [設定動態授權信任分數元件] 取得您可以重設的信任分數元件清單。更新括弧 <> 中的值 以符合您的環境。如果您不使用 -vserver 參數、命令會在叢集層級執行。必須使用粗體參數:

```
security dynamic-authorization user-trust-score reset \
<strong>-username <username></strong> \
<strong>-component <component-name></strong> \
-vserver <storage VM name>
```

顯示您的信任分數

使用者可以顯示自己的登入工作階段信任分數。

#### 步驟

1. 顯示您的信任分數:

security login whoami

您應該會看到類似下列的輸出:

```
User: admin
Role: admin
Trust Score: 50
```

## 設定自訂信任分數提供者

如果您已經收到外部信任分數提供者的評分方法、可以將自訂提供者新增至動態授權組態。

開始之前

- 自訂信任分數提供者必須傳回 JSON 回應。必須符合下列語法需求:
  - 。傳回信任分數的欄位必須是純量欄位、而非陣列的元素。
  - 。傳回信任分數的欄位可以是巢狀欄位、例如 trust score.value。
  - JSON 回應中必須有一個欄位可傳回數值信任分數。如果無法原生使用、您可以撰寫包裝函式指令碼來 傳回此值。
- •提供的值可以是信任分數或風險分數。差異在於信任分數以遞增順序排列、分數較高則代表較高的信任層

級、而風險分數則以遞減順序排列。例如、分數範圍為 0 至 100 的信任分數為 90 、表示分數非常值得 信賴、可能會導致「允許」而不需要其他挑戰、 雖然分數範圍為 0 到 100 的風險分數為 90 、表示風險高、 可能導致「拒絕」、而不會有額外的挑戰。

- 自訂信任分數提供者必須透過 ONTAP REST API 存取。
- 自訂信任分數提供者必須使用其中一個支援的參數進行設定。不支援需要不在支援參數清單中的組態的自訂 信任分數提供者。

如需有關的參數和預設值的詳細資訊 security dynamic-authorization trust-score-component create 命令、請參閱 ONTAP 手冊頁。

步驟

 新增自訂信任分數提供者。更新括弧 <> 中的值以符合您的環境。如果您不使用 -vserver 參數、命令會在 叢集層級執行。必須使用粗體參數:

```
security dynamic-authorization trust-score-component create \
-component <text> \
<strong>-provider-uri <text></strong> \
-score-field <text> \
-min-score <integer> \
<strong>-max-score <integer></strong> \
<strong>-weight <integer></strong> \
-secret-access-key "<key_text>" \
-provider-http-headers <list<header,header,header>> \
-vserver <storage_VM_name>
```

2. 檢視產生的信任分數提供者設定:

security dynamic-authorization trust-score-component show

#### 設定自訂信任分數提供者標記

您可以使用標記與外部信任分數提供者通訊。這可讓您將 URL 中的資訊傳送給信任分數提供者、而不會洩漏敏 感資訊。

如需有關的參數和預設值的詳細資訊 security dynamic-authorization trust-score-component create 命令、請參閱 ONTAP 手冊頁。

步驟

 啟用信任分數提供者標記。更新括弧 <> 中的值以符合您的環境。如果您不使用 -vserver 參數、命令會在 叢集層級執行。必須使用粗體參數:

```
security dynamic-authorization trust-score-component create \
<strong>-component <component_name></strong> \
-weight <initial_score_weight> \
-max-score <max_score_for_provider> \
<strong>-provider-uri <provider_URI></strong> \
-score-field <REST_API_score_field> \
<strong>-secret-access-key "<key text>"</strong>
```

例如:

security dynamic-authorization trust-score-component create -component comp1 -weight 20 -max-score 100 -provider-uri https://<url>/trustscores/users/<user>/<ip>/component1.html?api-key=<access-key> -score -field score -access-key "MIIBBjCBrAIBArqyTHFvYdWiOpLkLKHGjUYUNSwfzX"

#### 版權資訊

Copyright © 2024 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。