RBAC安全性

ONTAP automation

NetApp
January 13, 2026

目錄

RBAC安全性

ONTAP REST API 的 RBAC 安全性總覽

包含強大且可擴充的角色型存取控制（RBAC）功能。ONTAP您可以為每個帳戶指派不同的角色、以控制使用者對透過REST API和CLI公開之資源的存取。這些角色定義不同ONTAP 層級的管理存取權限、以供各種不同的使用者使用。

ⓘ 藉助於《更新版本》（及後續版本）、可持續擴充及大幅增強其RBAC功能。ONTAP ONTAP如需詳細資訊、請參閱 "RBAC演進摘要" 和 "ONTAP REST API 的新功能" 。

職務ONTAP

角色是一組權限、可共同定義使用者可以採取的行動。每項權限都會識別特定的存取路徑及相關的存取層級。角色會指派給使用者帳戶、ONTAP 並在決定存取控制時套用到由功能不完整的角色。

角色類型

角色有兩種類型。他們是ONTAP 根據不同環境的需求而推出、並隨之量身打造。

ⓘ 使用每種角色時都有優點和缺點。請參閱 "比較角色類型" 以取得更多資訊。

類型	說明
休息	其餘角色是ONTAP 以32個9.6加入、一般適用於透過ONTAP REST API存取的使用者。建立REST角色會自動建立傳統的_mapping角色。
傳統	以上是ONTAP 支援支援支援支援支援支援支援的舊角色。這些產品是針對ONTAP 整個CLI環境而推出、並持續成為RBAC安全性的基礎。

範圍

每個角色都有定義及套用的範圍或內容。此範圍決定使用特定角色的位置和方式。

ⓘ 使用者帳戶也有類似的範圍、可決定使用者的定義和使用方式。ONTAP

範圍	說明
叢集	具有叢集範圍的角色是ONTAP 在整個叢集層級定義。它們與叢集層級的使用者帳戶相關聯。
SVM	具有SVM範圍的角色是針對特定資料SVM所定義。它們會指派給同一個SVM中的使用者帳戶。

角色定義的來源

有兩種方法ONTAP 可以定義「角色扮演」。

角色來源	說明
自訂	這個系統管理員可以建立自訂角色。ONTAP這些角色可根據特定環境和安全需求量身打造。
內建	雖然自訂角色可提供更高的靈活度、但叢集和SVM層級也有一組內建角色可供使用。這些角色是預先定義的、可用於許多常見的管理工作。

角色對應與ONTAP 資料處理

根據您使用的版本、所有或幾乎所有REST API呼叫都會對應到一或多個CLI命令。ONTAP當您建立REST角色時、也會建立傳統或舊角色。此*對應的*傳統角色是以對應的CLI命令為基礎、無法操作或變更。

不支援反轉角色對應。也就是、建立傳統角色並不會建立對應的REST角色。

RBAC演進摘要

所有的版本均包含ONTAP 傳統角色。其餘的角色稍後會介紹、並會依照下列說明進行演進。

部分9.6 ONTAP

REST API是ONTAP 以NetApp 9.6推出。其餘角色也隨附於此版本中。此外、當您建立REST角色時、也會建立對應的傳統角色。

零點9.7到9.10.1 ONTAP

從ONTAP 9.7到9.10.1的每個版本均包含REST API的增強功能。例如、每個版本都新增了其他REST端點。不過、這兩種角色類型的建立與管理仍是分開的。此外ONTAP 、針對快照REST端點「/API/storage / voles/｛vol.uuid｝/snapshots」（資源合格的端點）、還加入了REST RBAC支援。

零點9.11.1. ONTAP

此版本新增了使用REST API來設定及管理傳統角色的功能。此外還新增其他REST角色的存取層級。

在 ONTAP REST API 中使用角色和使用者

瞭解基本的RBAC功能之後、您就可以開始使用ONTAP 各種角色和使用者。

請參閱 "RBAC 工作流程" 如需如何建立及使用 ONTAP REST API 角色的範例。

管理存取

您可以ONTAP 透過REST API或命令列介面來建立及管理等功能。存取詳細資料如下所述。

REST API

在使用RBAC角色和使用者帳戶時、可以使用多個端點。表格中的前四個用於建立及管理角色。最後兩個用於建立及管理使用者帳戶。

您可以在ONTAP 線上存取此功能 "API 參考" 如需詳細資訊、包括如何使用API的範例、請參閱文件。

端點	說明
安全性/角色	此端點可讓您建立新的REST角色。從功能性的問題9.11.1開始ONTAP 、您也可以建立傳統角色。在這種情況ONTAP 下、由功能變數根據輸入參數來決定角色類型。您也可以擷取已定義角色的清單。
安全性/角色/｛Owner.UUID｝/｛name｝	您可以擷取或刪除特定叢集或SVM範圍內的角色。UUID值可識別定義角色的SVM（叢集或資料SVM）。名稱值是角色的名稱。
安全性/角色/｛Oner.UUID｝/｛name｝/權限	此端點可讓您設定特定角色的權限。內建的角色可以擷取、但無法更新。如ONTAP 需詳細資訊、請參閱適用於您的發行版的API參考文件。
安全性/角色/｛Owner.UUID｝/｛name｝/權限/[路徑]	您可以擷取、修改及刪除特定權限的存取層級和選用查詢值。如ONTAP需詳細資訊、請參閱適用於您的發行版的API參考文件。
安全/帳戶	此端點可讓您建立新的叢集或SVM範圍使用者帳戶。在帳戶運作之前、必須先加入或後續新增多種類型的資訊。您也可以擷取已定義的使用者帳戶清單。
安全性/帳戶/｛owner.UUID｝/｛name｝	您可以擷取、修改及刪除特定叢集或SVM範圍內的使用者帳戶。UUID值可識別定義使用者的SVM（叢集或資料SVM）。名稱值為帳戶名稱。

命令列介面

相關ONTAP 的CLI命令如下所述。所有命令均可透過系統管理員帳戶在叢集層級存取。

命令	說明
'安全登入'	此目錄包含建立及管理使用者登入所需的命令。
「安全登入REST角色」	此目錄包含建立及管理與使用者登入相關之REST角色所需的命令。
《安全登入角色》	此目錄包含建立及管理與使用者登入相關之傳統角色所需的命令。

角色定義

其餘角色和傳統角色是透過一組屬性來定義。

擁有者與範圍

角色可由ONTAP 叢集內的某個叢集或特定資料SVM擁有。擁有者也會隱含決定角色的範圍。

唯一名稱

每個角色在其範圍內都必須有唯一的名稱。叢集角色的名稱ONTAP 在叢集層級必須是唯一的、而SVM角色在特定SVM中必須是唯一的。

新REST角色的名稱在其餘角色和傳統角色之間必須是唯一的。這是因為建立REST角色也會產生具有相同名稱的新傳統_mapping角色。

一組權限

每個角色都包含一組或多個權限。每項權限都會識別特定的資源或命令、以及相關的存取層級。

權限

一個角色可以包含一或多個權限。每個權限定義都是一個群組、可建立特定資源或作業的存取層級。

資源路徑

資源路徑可識別為REST端點或CLI命令/命令目錄路徑。

REST端點

API端點會識別REST角色的目標資源。

CLI命令

CLI命令可識別傳統角色的目標。您也可以指定命令目錄、然後將所有下游命令都包含在ONTAP 列舉的CLI階層中。

存取層級

存取層級會定義角色對特定資源路徑或命令的存取類型。存取層級是透過一組預先定義的關鍵字來識別。採用了三種存取層級ONTAP 、搭配使用NetApp 9.6。它們既可用於傳統角色、也可用於REST角色。此外、還新增ONTAP 了三個使用者層級的更新版本、包括更新版本的版本。這些新的存取層級只能用於REST角色。

存取層級遵循CRUD模式。使用REST時、這是以主要HTTP方法（POST、GET、修補、刪除）為基礎。對應的CLI作業通常會對應至REST作業（建立、顯示、修改、刪除）。

存取層級	**REST**原元	新增	僅限**REST**角色
無	不適用	9.6	否
唯讀	取得	9.6	否
全部	取得、張貼、修補、刪除	9.6	否
read_create	取得、發佈	9.11.1.	是的
Read_modify	取得、修補	9.11.1.	是的
read_create_modify	取得、發佈、修補程式	9.11.1.	是的

選用查詢

建立傳統角色時、您可以選擇性地加入*查詢*值、以識別命令或命令目錄適用物件的子集。

內建角色摘要

您可以在叢集或SVM層級使用幾個ONTAP 隨附於功能性功能的預先定義角色。

叢集範圍內的角色

叢集範圍內有多個內建角色可供使用。

請參閱 "叢集管理員的預先定義角色" 以取得更多資訊。

角色	說明
管理	擁有此角色的系統管理員擁有不受限制的權限、可在ONTAP 這個系統中執行任何動作。他們可以設定所有叢集層級和SVM層級的資源。
AutoSupport	這是專為AutoSupport 此客戶量身打造的特殊職務。

角色	說明
備份	此特殊角色適用於需要備份系統的備份軟體。
SnapLock	這是專為SnapLock 此客戶量身打造的特殊職務。
唯讀	具有此角色的系統管理員可以檢視叢集層級的所有項目、但無法進行任何變更。
無	不提供管理功能。

SVM範圍內的角色

SVM範圍內有多個內建角色可供使用。* vsadmin*可讓您存取最通用且功能最強大的功能。另外還有幾個專為特定管理工作量身打造的角色、包括：

- vsadmin-volume
- vsadmin-Protocol
- vsadmin-Backup
- vsadmin-SnapLock
- vsadmin-readonly

請參閱 "SVM系統管理員的預先定義角色" 以取得更多資訊。

比較角色類型

在選擇* REST *角色或*傳統*角色之前、您應該瞭解兩者的差異。以下說明兩種角色類型的一些比較方法。

對於較進階或複雜的RBAC使用案例、通常應使用傳統角色。

使用者存取**ONTAP** 功能的方式

在建立角色之前、請務必瞭解使用者如何存取ONTAP 該系統。根據這種情況、您可以決定角色類型。

存取	建議類型
僅REST API	REST角色的設計可與REST API搭配使用。
REST API和CLI	您可以定義REST角色、也可以建立對應的傳統角色。
僅限CLI	您可以建立傳統角色。

存取路徑的精確性

為REST角色定義的存取路徑是以REST端點為基礎。傳統角色的存取路徑是以CLI命令或命令目錄為基礎。此外、您也可以加入選用的查詢參數及傳統角色、以根據命令參數值進一步限制存取。

版權資訊

商標資訊