角色型存取控制

ONTAP tools for VMware vSphere 9.10

NetApp
January 18, 2024

目錄

角色型存取控制

概述以角色為基礎的ONTAP 存取控制功能

vCenter Server提供角色型存取控制（RBAC）、可讓您控制vSphere物件的存取。在VMware vSphere的VMware®工具中、vCenter Server RBAC可搭配使用以確定特定使用者可在特定儲存系統上的物件上執行哪些VSC工作。ONTAP ONTAP

若要成功完成工作、您必須擁有適當的vCenter Server RBAC權限。在工作期間、VSC會先檢查使用者的vCenter Server權限、然後再檢查使用者ONTAP 的VMware vCenter權限。

您可以在根物件（也稱為根資料夾）上設定vCenter Server權限。然後您可以限制不需要這些權限的子實體、藉此精簡安全性。

vCenter Server權限的元件

vCenter Server可辨識權限、而非權限。每個vCenter Server權限均由三個元件組成。

vCenter Server具有下列元件：

- 一或多個權限（角色）

  權限定義使用者可以執行的工作。

- vSphere物件

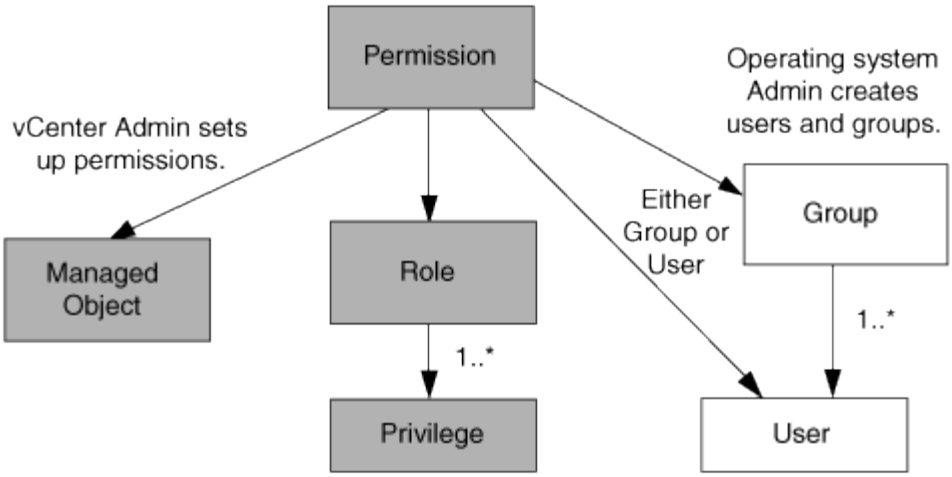
  物件是工作的目標。

- 使用者或群組

  使用者或群組會定義可以執行工作的人員。

如下圖所示、您必須擁有所有三個元素、才能取得權限。

> 在此圖中、灰色方塊表示vCenter Server中存在的元件、而白色方塊則表示vCenter Server執行所在作業系統中存在的元件。



權限

VMware vSphere的VMware vSphere的VMware VMware工具有兩種權限：ONTAP

- 原生vCenter Server權限

  這些權限隨附於vCenter Server。

- VSC專屬權限

  這些權限是針對特定VSC工作所定義。VSC獨一無二。

VSC工作需要VSC專屬權限和vCenter Server原生權限。這些權限構成使用者的「角色」。權限可以有多個權限。這些權限適用於登入vCenter Server的使用者。

> 為了簡化vCenter Server RBAC作業、VSC提供多種標準角色、其中包含執行VSC工作所需的所有VSC專屬和原生權限。

如果您變更權限內的權限、則與該權限相關的使用者應登出、然後登入以啟用更新的權限。

權限	角色	工作
NetApp ONTAP 解決方案工具主控台>檢視	• VSC管理員 • VSC配置 • VSC唯讀	所有VSC和VASA Provider特定工作都需要View權限。
NetApp虛擬儲存主控台>原則型管理>管理 或privilege.nvpfVSC.VASAGroup.com.netapp.nvpf.label >管理	VSC管理員	VSC和VASA Provider工作與儲存功能設定檔和臨界值設定相關。

vSphere物件

權限與vSphere物件相關聯、例如vCenter Server、ESXi主機、虛擬機器、資料存放區、資料中心、 和資料夾。

您可以將權限指派給任何vSphere物件。vCenter Server會根據指派給vSphere物件的權限、決定誰可以在該物件上執行哪些工作。對於VSC特定工作、權限僅會指派並驗證於根資料夾層級（vCenter Server）、而非任何其他實體。VAAI外掛程式作業除外、該作業會針對相關ESXi驗證權限。

使用者與群組

您可以使用Active Directory（或本機vCenter Server機器）來設定使用者和使用者群組。然後您可以使用vCenter Server權限來授予這些使用者或群組存取權、讓他們能夠執行特定的VSC工作。

> 這些vCenter Server權限適用於VSC vCenter使用者、而非VSC管理員。根據預設、VSC系統管理員擁有產品的完整存取權、不需要指派權限給他們。

使用者和群組並未指派角色給他們。他們可透過vCenter Server權限的一部分來存取角色。

指派和修改vCenter Server權限的重點

使用vCenter Server權限時、請謹記幾個重點。VMware vSphere工作的VMware選用功能是否成功、取決於您指派權限的位置、或使用者在修改權限後採取的行動。ONTAP

指派權限

如果您只想限制對vSphere物件和工作的存取、則只需要設定vCenter Server權限。否則、您可以以系統管理員的身分登入。此登入可讓您自動存取所有vSphere物件。

指派權限的位置決定使用者可以執行的VSC工作。

有時候、為了確保工作完成、您必須在較高層級（例如根物件）指派權限。當工作需要不適用於特定vSphere物件的權限（例如追蹤工作）、或是需要的權限套用至非vSphere物件（例如儲存系統）時、就會發生這種情況。

在這些情況下、您可以設定權限、讓子實體繼承權限。您也可以將其他權限指派給子實體。指派給子實體的權限一律會覆寫繼承自父實體的權限。這表示您可以將權限授予子實體、以限制指派給根物件並由子實體繼承的權限範圍。

> 除非貴公司的安全性原則需要更嚴格的權限、否則指派權限給根物件（也稱為根資料夾）是很好的做法。

權限與非vSphere物件

您建立的權限會套用至非vSphere物件。例如、儲存系統不是vSphere物件。如果某項權限適用於儲存系統、您必須將包含該權限的權限指派給VSC根物件、因為您無法將該權限指派給vSphere物件。

例如、任何包含VSC權限的權限、例如「新增/修改/跳過儲存系統」、都必須在根物件層級指派。

修改權限

您可以隨時修改一個權限。

如果您變更權限內的權限、則與該權限相關的使用者應登出、然後重新登入以啟用更新的權限。

標準角色隨ONTAP 附於整套的功能

為了簡化vCenter Server權限與角色型存取控制（RBAC）的使用、Virtual Storage Console（VSC）提供標準VSC角色、讓您能夠執行關鍵VSC工作。此外、也有唯讀角色可讓您檢視VSC資訊、但無法執行任何工作。

標準VSC角色具有必要的VSC專屬權限、以及使用者執行VSC工作所需的原生vCenter Server權限。此外、這些角色也會設定成擁有所有受支援版本vCenter Server所需的權限。

身為管理員、您可以視需要指派這些角色給使用者。

> 當您將VSC升級至最新版本時、系統會自動升級標準角色、以搭配新版VSC使用。

您可以按一下vSphere Client首頁上的*角色*來檢視VSC標準角色。

VSC提供的角色可讓您執行下列工作：

角色	說明
VSC管理員	提供執行所有VSC工作所需的所有原生vCenter Server權限和VSC專屬權限。
VSC唯讀	提供VSC的唯讀存取權。這些使用者無法執行任何存取控制的VSC動作。
VSC配置	提供配置儲存設備所需的所有原生vCenter Server權限和VSC專屬權限。您可以執行下列工作： • 建立新的資料存放區 • 銷毀資料存放區 • 檢視儲存功能設定檔的相關資訊

使用VSC標準角色的準則

當您使用VMware ONTAP vSphere角色的標準版基礎架構工具時、您應該遵循某些準則。

您不應直接修改標準角色。如果您這麼做、VSC會在您每次升級VSC時覆寫您的變更。每次升級VSC時、安裝程式都會更新標準角色定義。這樣做可確保您的VSC版本以及所有受支援版本的vCenter Server的角色都是最新的。

不過、您可以使用標準角色來建立專為您環境量身打造的角色。若要這麼做、您應該複製VSC標準角色、然後編輯複製的角色。藉由建立新角色、即使您重新啟動或升級VSC Windows服務、也能維持此角色。

您可以使用VSC標準角色的部分方法包括：

- 使用標準VSC角色執行所有VSC工作。

  在此案例中、標準角色提供使用者執行VSC工作所需的所有權限。

- 合併角色以擴充使用者可以執行的工作。

  如果標準VSC角色為您的環境提供過多精細度、您可以建立包含多個角色的較高層級群組來擴充角色。

  如果使用者需要執行其他需要額外原生vCenter Server權限的非VSC工作、您可以建立提供這些權限的角色、並將其新增至群組。

- 建立更精細的角色。

  如果貴公司要求您實作比標準VSC角色更具限制性的角色、您可以使用VSC角色來建立新角色。

  在這種情況下、您會複製必要的VSC角色、然後編輯複製的角色、使其僅擁有使用者所需的權限。

VSC工作所需的權限

VMware vSphere工作的不同功能需要不同的權限組合、這些權限是虛擬儲存主控台（VSC）和原生vCenter Server權限的專屬權限。ONTAP

如需VSC工作所需權限的相關資訊、請參閱NetApp知識庫文章1032542。

"如何為虛擬儲存主控台設定RBAC"

VMware vSphere的產品層級權限ONTAP 、由VMware vSphere的VMware工具提供

若要存取ONTAP VMware vSphere GUI的VMware vSphere工具、您必須在正確的vSphere物件層級指派產品層級VSC專屬檢視權限。如果您在沒有此權限的情況下登入、VSC會在您按一下NetApp圖示時顯示錯誤訊息、並防止您存取VSC。

下列資訊說明VSC產品層級檢視權限：

權限	說明	指派層級
檢視	您可以存取VSC GUI。此權限無法讓您在VSC內執行工作。若要執行任何VSC工作、您必須擁有正確的VSC專屬及原生vCenter Server權限、才能執行這些工作。	指派層級決定您可以看到的UI部分。在根物件（資料夾）上指派檢視權限、可讓您按一下NetApp圖示進入VSC。 您可以將「檢視」權限指派給另一個vSphere物件層級、但這樣做會限制您可以查看及使用的VSC功能表。 根物件是指派任何包含檢視權限的權限的建議位置。

適用於VMware的權限ONTAP

以角色為基礎的存取控制（RBAC）可讓您控制對特定儲存系統的存取、並控制使用者可在這些儲存系統上執行的動作。ONTAP在VMware vSphere的VMware®工具中ONTAP

、VMware vSphere的VMware RBAC可搭配vCenter Server RBAC來判斷特定使用者可在特定儲存系統的物件上執行哪些虛擬儲存主控台（VSC）工作。ONTAP

VSC會使用您在VSC中設定的認證（使用者名稱和密碼）來驗證每個儲存系統、並決定可在該儲存系統上執行哪些儲存作業。VSC會針對每個儲存系統使用一組認證資料。這些認證資料可決定在該儲存系統上執行哪些VSC工作；換句話說、認證資料適用於VSC、而非適用於個別VSC使用者。

支援RBAC僅適用於存取儲存系統及執行與儲存相關的VSC工作、例如資源配置虛擬機器。ONTAP如果ONTAP您沒有適用於特定儲存系統的適當RBAC權限、就無法在該儲存系統上裝載的vSphere物件上執行任何工作。您可以搭配ONTAP VSC專屬權限來使用RBAC、以控制使用者可以執行的VSC工作：

- 監控及設定儲存系統上的儲存或vCenter Server物件
- 資源配置位於儲存系統上的vSphere物件

利用具備VSC專屬權限的RBAC、可提供儲存管理員可管理的儲存導向安全層。ONTAP因此、您擁有比ONTAP單純使用VMware RBAC或僅使用vCenter Server RBAC支援更精細的存取控制。例如、有了vCenter Server RBAC、您可以允許vCenterUserB在NetApp儲存設備上配置資料存放區、同時防止vCenterUserA配置資料存放區。如果特定儲存系統的儲存系統認證不支援建立儲存設備、則vCenterUserB或vCenterUserA都無法在該儲存系統上配置資料存放區。

當您啟動VSC工作時、VSC會先驗證您是否擁有該工作的正確vCenter Server權限。如果vCenter Server權限不足以允許您執行工作、VSC就不需要檢查ONTAP 該儲存系統的「可靠性」權限、因為您未通過初始vCenter Server安全性檢查。因此、您無法存取儲存系統。

如果vCenter Server權限足夠、VSC會檢查ONTAP 與儲存系統認證（使用者名稱和密碼）相關聯的VMware RBAC權限（ONTAP 您的VMware角色）。 以判斷您是否擁有足夠的權限、可在該儲存系統上執行該VSC工作所需的儲存作業。如果ONTAP 您擁有正確的資訊功能、可以存取儲存系統並執行VSC工作。這個功能可決定您可以在儲存系統上執行的VSC工作。ONTAP

每個儲存系統都有ONTAP 一組相關的「樣」權限。

同時使用ONTAP VMware RBAC和vCenter Server RBAC可提供下列優點：

- 安全性

  管理員可控制哪些使用者可在精細的vCenter Server物件層級和儲存系統層級執行哪些工作。

- 稽核資訊

  在許多情況下、VSC會在儲存系統上提供稽核追蹤、讓您能夠將事件追蹤回執行儲存修改的vCenter Server使用者。

- 使用性

  您可以將所有的控制器認證資料保留在同一個位置。

使用VMware vSphere的VMware vSphere的VMware VMware VMware VMware VMware VMware VMware VMware VMware VMware VMware VMware VMware VMware VMware VMware ONTAP ONTAP

您可以設定數ONTAP 個建議的VMware vCenter功能、以搭配ONTAP VMware vSphere的VMware®工具和角色

型存取控制（RBAC）。這些角色包含ONTAP 執行虛擬儲存主控台（VSC）工作所執行之必要儲存作業所需的功能。

若要建立新的使用者角色、您必須以系統管理員身分登入執行ONTAP 效益分析的儲存系統。您可以ONTAP 使用下列其中一項來建立功能：

- 系統管理程式9.8P1或更新版本ONTAP

  "設定使用者角色和權限"

- RBAC使用者建立工具ONTAP （若使用ONTAP 的是32個以上版本）

每ONTAP 個功能都有一個相關的使用者名稱和密碼配對、構成該角色的認證資料。如果您未使用這些認證登入、則無法存取與該角色相關的儲存作業。

作為安全措施、VSC特定ONTAP 的功能性角色會依階層順序排列。這表示第一個角色是最嚴格的角色、只有與最基本的VSC儲存作業集相關的權限。下一個角色同時包含自己的權限、以及與先前角色相關的所有權限。對於支援的儲存作業、每個額外角色的限制都較少。

以下是ONTAP 使用VSC時建議使用的部分RBAC角色。建立這些角色之後、您可以將角色指派給必須執行儲存相關工作的使用者、例如資源配置虛擬機器。

1. 探索

   此角色可讓您新增儲存系統。

2. 建立儲存設備

   此角色可讓您建立儲存設備。此角色也包含與探索角色相關的所有權限。

3. 修改儲存設備

   此角色可讓您修改儲存設備。此角色也包含與探索角色和建立儲存角色相關的所有權限。

4. 摧毀儲存設備

   此角色可讓您銷毀儲存設備。此角色也包含與探索角色、建立儲存角色及修改儲存角色相關的所有權限。

如果您使用VASA Provider ONTAP 來執行功能、也應該設定原則型管理（PBM）角色。此角色可讓您使用儲存原則來管理儲存設備。這項職務要求您也必須設定「探索」角色。

如何針對ONTAP VMware vSphere的VMware vSphere、設定ONTAP 以角色為基礎的驗證工具存取控制

如果您想要在VMware vSphere上使用角色型存取控制搭配使用VMware vSphere的VMware工具、則必須在ONTAP 儲存系統上設定以角色為基礎的存取控制（RBAC）ONTAP 。您可以使用ONTAP 「介紹RBAC」功能、建立一個或多個存取權限有限的自訂使用者帳戶。

VSC和SRA可存取叢集層級或儲存虛擬機器（SVM）SVM層級的儲存系統。如果您是在叢集層級新增儲存系統、則必須提供管理使用者的認證、以提供所有必要的功能。如果您是直接新增SVM詳細資料來新增儲存系

統、您必須注意、「vsadmin」使用者並不具備執行特定工作所需的全部角色和功能。

VASA Provider只能在叢集層級存取儲存系統。如果特定儲存控制器需要VASA Provider、則即使您使用VSC或SRA、也必須在叢集層級將儲存系統新增至VSC。

若要建立新的使用者、並將叢集或SVM連線ONTAP 至VMware Tools、您應該執行下列步驟：

- 建立叢集管理員或SVM管理員角色

  您可以使用下列其中一項來建立這些角色：

  - 系統管理程式9.8P1或更新版本ONTAP

    "設定使用者角色和權限"

  - RBAC使用者建立工具ONTAP （若使用ONTAP 的是32個以上版本）

- 使用ONTAP NetApp建立已指派角色的使用者、並使用NetApp建立適當的應用程式集

  您需要這些儲存系統認證資料、才能設定VSC的儲存系統。您可以在VSC中輸入認證資料、為VSC設定儲存系統。每次使用這些認證登入儲存系統時、您都有權使用ONTAP 在建立認證時於各處設定的VSC功能。

- 將儲存系統新增至VSC、並提供您剛建立之使用者的認證資料

VSC角色

VSC將ONTAP 「不含功能的」權限分類為下列一組VSC角色：

- 探索

  可探索所有連線的儲存控制器

- 建立儲存設備

  可建立磁碟區和邏輯單元編號（LUN）

- 修改儲存設備

  實現儲存系統的大小調整和重複資料刪除

- 摧毀儲存設備

  可銷毀磁碟區和LUN

VASA供應商角色

您只能在叢集層級建立原則型管理。此角色可利用儲存功能設定檔、針對儲存設備進行原則型管理。

SRA角色

SRA將ONTAP 「不支援功能」權限分類為叢集層級或SVM層級的SAN或NAS角色。這可讓使用者執行SRM作

業。

當ONTAP 您將叢集新增至VSC時、VSC會執行初始權限驗證以驗證各項RBAC角色。如果您已新增直接SVM儲存IP、則VSC不會執行初始驗證。VSC會在工作流程稍後檢查並強制執行權限。