VSC工作所需的權限

VSC, VASA Provider, and SRA 9.7

NetApp
March 21, 2024

目錄

VSC工作所需的權限

不同的VMware vSphere虛擬儲存主控台工作需要不同的權限組合、這些權限分別是（VSC）和原生vCenter Server權限。

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"

VSC需要VMware vSphere的產品層級權限

若要存取VMware vSphere GUI的虛擬儲存主控台、您必須在正確的vSphere物件層級指派產品層級的VSC特定檢視權限。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	工作分派層級
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。

VSC、VASA Provider和SRA虛擬應用裝置的角色型存取控制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的虛擬儲存主控台中ONTAP、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。

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VSC for VMware vSphere時的推薦ONTAP 功能

您可以設定數ONTAP 個建議的VMware vCenter功能、以搭配VMware vSphere的虛擬儲存主控台和角色型存取控制（RBAC）。這些角色包含ONTAP 執行（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：

- 9.7或更新版本

  "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）

  "適用於VSC、VASA Provider和Storage Replication Adapter 7.0的RBAC使用者建立工具、適用於VMware vSphere"

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。

如何為ONTAP VMware vSphere的VSC設定以角色為基礎的存取控制

如果您想要在VMware vSphere（VSC）的虛擬儲存主控台上使用角色型存取控制、則必須在ONTAP 儲存系統上設定以角色為基礎的存取控制（RBAC）。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可以存取叢集層級或層級的儲存系統。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。如果您是直接新增詳細資料來新增儲存系統、您必須注意「vsadmin」使用者並沒有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。

若要建立新使用者、並將叢集或連線至VSC、VASA Provider及SRA、您應該執行下列步驟：

- 建立叢集管理員或系統管理員角色

> 您可以使用下列其中一項來建立這些角色：
>
> - 系統管理程式9.7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）
>
> "適用於VSC、VASA Provider和Storage Replication Adapter 7.0的RBAC使用者建立工具、適用於VMware vSphere"

- 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層級的SAN或NAS角色。這可讓使用者執行SRM作業。

> 如果您想要使用ONTAP 指令功能手動設定角色和權限、請參閱知識庫文章。

- "VSC、VASA和SRA 7.0 ONTAP 版《RBAC組態》"
- "彙總SVM層級的VSC和SRA所有命令"

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。如果您已新增直接儲存IP、VSC就不會執行初始驗證。VSC會在工作流程稍後檢查並強制執行權限。

設定使用者角色和權限

您可以使用虛擬應用裝置隨附的Json檔案、為VSC、VASA Provider、SRA和ONTAP SRA供System Manager使用、來設定管理儲存系統的新使用者角色。

開始之前

- 您應該ONTAP 已經使用「https://{virtual_appliance_IP}:9083/vsc/config/VSC_ONTAP_User_Privileges.zip`」、從VSC、VASA Provider和SRA的虛擬應用裝置下載了「SRAT權限」檔案。
- 您應該已設定ONTAP 好「更新系統管理程式」。
- 您應該已以系統管理員權限登入儲存系統。

步驟

1. 解壓縮下載的「https://{virtual_appliance_IP}:9083/vsc/config/VSC_ONTAP_User_Privileges.zip`」檔案。
2. 存取ONTAP 《系統管理程式》。
3. 按一下功能表：叢集[設定>使用者與角色]。
4. 按一下*新增使用者*。
5. 在「新增使用者」對話方塊中、選取*虛擬化產品*。
6. 按一下「瀏覽」以選取並上傳ONTAP 「恢復能力Json」檔案。

   產品欄位會自動填入。

7. 從「產品功能」下拉式功能表中選取所需的功能。

   「角色」欄位會根據所選的產品功能自動填入。

8. 輸入所需的使用者名稱和密碼。
9. 選取使用者所需的權限（探索、建立儲存設備、修改儲存設備、銷毀儲存設備）、然後按一下*新增*。

結果

新的角色和使用者隨即新增、您可以在已設定的角色下查看詳細權限。