管理您的帳戶
Astra Control Center

NetApp
March 12, 2024

目錄

管理您的帳戶

管理本機使用者和角色

您可以使用Astra Control UI來新增、移除及編輯Astra Control Center安裝的使用者。您可以使用Astra Control UI或 "Astra Control API" 管理使用者：

您也可以使用LDAP為選取的使用者執行驗證。

使用**LDAP**

LDAP是存取分散式目錄資訊的業界標準傳輸協定、也是企業驗證的熱門選擇。您可以將Astra Control Center連線至LDAP伺服器、為選取的Astra Control使用者執行驗證。在高層級上、組態包括將Astra與LDAP整合、以及定義與LDAP定義對應的Astra Control使用者和群組。您可以使用Astra Control API或Web UI來設定LDAP驗證、以及LDAP使用者和群組。如需詳細資訊、請參閱下列文件：

- "使用Astra Control API來管理遠端驗證和使用者"
- "使用Astra Control UI來管理遠端使用者和群組"
- "使用Astra Control UI來管理遠端驗證"

新增使用者

帳戶擁有者和系統管理員可以新增更多使用者至Astra Control Center安裝。

步驟

1. 在*管理您的帳戶*導覽區域中、選取*帳戶*。
2. 選取*使用者*索引標籤。
3. 選取*新增使用者*。
4. 輸入使用者的名稱、電子郵件地址和暫用密碼。

   使用者必須在第一次登入時變更密碼。

5. 選取具有適當系統權限的使用者角色。

   每個角色都提供下列權限：

   - *檢視器*可以檢視資源。
   - *成員*具有檢視者角色權限、可管理應用程式與叢集、取消管理應用程式、以及刪除快照與備份。
   - 「管理」具有「成員角色」權限、可新增及移除擁有者以外的任何其他使用者。
   - *擁有者*具有管理員角色權限、可新增及移除任何使用者帳戶。

6. 若要新增限制給具有成員或檢視者角色的使用者、請啟用*限制角色限制*核取方塊。

   如需新增限制的詳細資訊、請參閱 "管理本機使用者和角色"。

7. 選取*「Add*」。

管理密碼

您可以在Astra Control Center中管理使用者帳戶的密碼。

變更您的密碼

您可以隨時變更使用者帳戶的密碼。

步驟

1. 選取畫面右上角的使用者圖示。
2. 選擇*設定檔*。
3. 從「動作」欄的「選項」功能表中選取「變更密碼」。
4. 輸入符合密碼需求的密碼。
5. 再次輸入密碼進行確認。
6. 選擇*變更密碼*。

重設其他使用者的密碼

如果您的帳戶具有「管理員」或「擁有者」角色權限、您可以重設其他使用者帳戶和您自己的密碼。當您重設密碼時、您會設定使用者登入時必須變更的暫用密碼。

步驟

1. 在*管理您的帳戶*導覽區域中、選取*帳戶*。
2. 選取「動作」下拉式清單。
3. 選擇*重設密碼*。
4. 輸入符合密碼需求的暫用密碼。
5. 再次輸入密碼進行確認。

   下次使用者登入時、系統會提示使用者變更密碼。

6. 選擇*重設密碼*。

移除使用者

擁有擁有者或管理員角色的使用者可以隨時從帳戶中移除其他使用者。

步驟

1. 在*管理您的帳戶*導覽區域中、選取*帳戶*。
2. 在「使用者」索引標籤中、選取您要移除之每個使用者列中的核取方塊。
3. 從「動作」欄的「選項」功能表中、選取「移除使用者」。
4. 出現提示時、請輸入「移除」一詞、然後選取「是、移除使用者*」、確認刪除。

結果

Astra Control Center會將使用者從帳戶中移除。

管理角色

您可以新增命名空間限制、並將使用者角色限制在這些限制中、藉此管理角色。這可讓您控制組織內資源的存取。您可以使用Astra Control UI或 "Astra Control API" 以管理角色。

將命名空間限制新增至角色

管理員或擁有者使用者可以將命名空間限制新增至「成員」或「檢視者」角色。

步驟

1. 在*管理您的帳戶*導覽區域中、選取*帳戶*。
2. 選取*使用者*索引標籤。
3. 在「動作」欄中、選取具有「成員」或「檢視者」角色的使用者功能表按鈕。
4. 選擇*編輯角色*。
5. 啟用「限制角色*」核取方塊。

   此核取方塊僅適用於「成員」或「檢視者」角色。您可以從*角色*下拉式清單中選取不同的角色。

6. 選取*新增限制*。

   您可以依命名空間或命名空間標籤檢視可用限制清單。

7. 在*限制類型*下拉式清單中、視命名空間的設定方式而定、選取* Kubernetes命名空間*或* Kubernetes命名空間標籤*。
8. 從清單中選取一或多個命名空間或標籤、以構成限制、限制角色只能使用這些命名空間。
9. 選擇* Confirm（確認）*。

   「編輯角色」頁面會顯示您為此角色選擇的限制清單。

10. 選擇* Confirm（確認）*。

    在「帳戶」頁面上、您可以在「角色」欄中檢視任何成員或檢視者角色的限制條件。

> 如果您啟用角色的限制、並選取* Confirm（確認）*而不新增任何限制、則該角色會被視為具有完整限制（該角色無法存取指派給命名空間的任何資源）。

從角色移除命名空間限制

管理員或擁有者使用者可以從角色移除命名空間限制。

步驟

1. 在*管理您的帳戶*導覽區域中、選取*帳戶*。
2. 選取*使用者*索引標籤。
3. 在「動作」欄中、選取具有作用中限制之「成員」或「檢視者」角色的使用者功能表按鈕。
4. 選擇*編輯角色*。

「編輯角色」對話方塊會顯示角色的作用中限制。

5. 選取您需要移除之限制右側的* X*。
6. 選擇* Confirm（確認）*。

以取得更多資訊

- "使用者角色和命名空間"

管理遠端驗證

LDAP是存取分散式目錄資訊的業界標準傳輸協定、也是企業驗證的熱門選擇。您可以將Astra Control Center連線至LDAP伺服器、為選取的Astra Control使用者執行驗證。

在高層級上、組態包括將Astra與LDAP整合、以及定義與LDAP定義對應的Astra Control使用者和群組。您可以使用Astra Control API或Web UI來設定LDAP驗證、以及LDAP使用者和群組。

> Astra Control Center 會使用啟用遠端驗證時所設定的使用者登入屬性來搜尋和追蹤遠端使用者。此欄位中必須存在電子郵件地址（「郵件」）或使用者主體名稱（「 userPrincipalName 」）的屬性、您想要在 Astra Control Center 中顯示的任何遠端使用者都必須存在。此屬性在 Astra Control Center 中作為驗證的使用者名稱、並在搜尋遠端使用者時使用。

新增**LDAPS**驗證的憑證

新增LDAP伺服器的私有TLS憑證、以便Astra Control Center在您使用LDAPS連線時、能夠與LDAP伺服器進行驗證。您只需要執行一次、或是安裝的憑證過期時。

步驟

1. 前往*帳戶*。
2. 選取*憑證*索引標籤。
3. 選取*「Add*」。
4. 上傳 `.pem` 將檔案內容從剪貼簿中歸檔或貼上。
5. 選取「信任」核取方塊。
6. 選取*新增憑證*。

啟用遠端驗證

您可以啟用LDAP驗證、並設定Astra Control與遠端LDAP伺服器之間的連線。

開始之前

如果您打算使用LDAPS、請確定LDAP伺服器的私有TLS憑證已安裝在Astra控制中心、以便Astra控制中心能夠與LDAP伺服器進行驗證。請參閱 新增LDAPS驗證的憑證 以取得相關指示。

步驟

1. 前往*帳戶>連線*。

2. 在*遠端驗證*窗格中、選取組態功能表。
3. 選擇*連接*。
4. 輸入伺服器IP位址、連接埠及偏好的連線傳輸協定（LDAP或LDAPS）。

> 最佳實務做法是在連接LDAP伺服器時使用LDAPS。您必須先在Astra Control Center中安裝LDAP伺服器的私有TLS憑證、才能連線至LDAPS。

5. 以電子郵件格式輸入服務帳戶認證（administrator@example.com）。Astra Control會在連線至LDAP伺服器時使用這些認證資料。
6. 在 * 使用者比對 * 區段中、執行下列步驟：
   a. 輸入從 LDAP 伺服器擷取使用者資訊時要使用的基礎 DN 和適當的使用者搜尋篩選器。
   b. （選用）如果您的目錄使用使用者登入屬性 `userPrincipalName` 而非 `mail`、輸入 `userPrincipalName` 在 * 使用者登入屬性 * 欄位的正確屬性中。
7. 在「群組比對」區段中、輸入群組搜尋基礎DN和適當的自訂群組搜尋篩選器。

> 請務必使用正確的基礎辨別名稱（DN）和適當的搜尋篩選器來搜尋*使用者比對*和*群組比對*。基礎DN會告知Astra Control在目錄樹狀結構的哪個層級開始搜尋、而搜尋篩選器則會限制Astra Control從目錄樹狀結構中搜尋的部分。

8. 選擇*提交*。

結果

「遠端驗證」窗格狀態會移至*「擱置中」、並在建立與**LDAP**伺服器的連線時移至「已連線」*。

停用遠端驗證

您可以暫時停用與LDAP伺服器的作用中連線。

> 停用LDAP伺服器連線時、會儲存所有設定、並保留從該LDAP伺服器新增至Astra Control的所有遠端使用者和群組。您可以隨時重新連線至此LDAP伺服器。

步驟

1. 前往*帳戶>連線*。
2. 在*遠端驗證*窗格中、選取組態功能表。
3. 選擇*停用*。

結果

「遠端驗證」窗格狀態會移至「停用」。所有遠端驗證設定、遠端使用者和遠端群組都會保留下來、您可以隨時重新啟用連線。

編輯遠端驗證設定

如果您已停用LDAP伺服器的連線、或*遠端驗證*窗格處於「連線錯誤」狀態、您可以編輯組態設定。

當「遠端驗證」窗格處於「已停用」狀態時、您無法編輯LDAP伺服器URL或IP位址。您需要 [中斷遠端驗證] 第一。

步驟

1. 前往*帳戶>連線*。
2. 在*遠端驗證*窗格中、選取組態功能表。
3. 選擇*編輯*。
4. 進行必要的變更、然後選取*編輯*。

中斷遠端驗證

您可以中斷與LDAP伺服器的連線、並從Astra Control移除組態設定。

如果您是 LDAP 使用者且中斷連線、工作階段將立即結束當您中斷與LDAP伺服器的連線時、該LDAP伺服器的所有組態設定都會從Astra Control中移除、以及從該LDAP伺服器新增的任何遠端使用者和群組。

步驟

1. 前往*帳戶>連線*。
2. 在*遠端驗證*窗格中、選取組態功能表。
3. 選擇*中斷連線*。

結果

「遠端驗證」窗格狀態會移至「中斷連線」。遠端驗證設定、遠端使用者和遠端群組都會從Astra Control中移除。

管理遠端使用者和群組

如果您已在Astra Control系統上啟用LDAP驗證、您可以搜尋LDAP使用者和群組、並將其納入系統的核准使用者中。

新增遠端使用者

帳戶擁有者和管理員可以將遠端使用者新增至Astra Control。Astra Control Center 最多支援 10 、 000 名 LDAP 遠端使用者。

Astra Control Center 會使用啟用遠端驗證時所設定的使用者登入屬性來搜尋和追蹤遠端使用者。此欄位中必須存在電子郵件地址（「郵件」）或使用者主體名稱（「 userPrincipalName 」）的屬性、您想要在 Astra Control Center 中顯示的任何遠端使用者都必須存在。此屬性在 Astra Control Center 中作為驗證的使用者名稱、並在搜尋遠端使用者時使用。

如果系統上已存在具有相同電子郵件地址的本機使用者（根據「 mail 」或「 user principal name 」屬性）、則無法新增遠端使用者。若要將使用者新增為遠端使用者、請先從系統中刪除本機使用者。

步驟

1. 前往*帳戶*區域。
2. 選取*使用者與群組*索引標籤。
3. 在頁面最右側、選取*遠端使用者*。
4. 選取*「Add*」。
5. 或者、您也可以在*依電子郵件篩選*欄位中輸入使用者的電子郵件地址、以搜尋LDAP使用者。
6. 從清單中選取一或多個使用者。
7. 指派角色給使用者。

   如果您指派不同的角色給使用者和使用者群組、則權限越高的角色優先。

8. 您也可以將一或多個命名空間限制指派給此使用者、然後選取*限制角色至限制*以強制執行限制。您可以選取*新增限制*來新增命名空間限制。

   當使用者透過LDAP群組成員資格指派多個角色時、最具權限角色的限制是唯一會生效的限制。例如、如果具有本機檢視器角色的使用者加入三個繫結至「成員」角色的群組、則「成員」角色的限制總和會生效、而且會忽略「檢視器」角色的任何限制。

9. 選取*「Add*」。

結果

新使用者會出現在遠端使用者清單中。在此清單中、您可以看到使用者的作用中限制、也可以從*動作*功能表管理使用者。

新增遠端群組

若要一次新增許多遠端使用者、帳戶擁有者和管理員可以將遠端群組新增至Astra Control。當您新增遠端群組時、該群組中的所有遠端使用者都可以登入 Astra Control 、並繼承與該群組相同的角色。

Astra Control Center 最多支援 5 、 000 個 LDAP 遠端群組。

步驟

1. 前往*帳戶*區域。
2. 選取*使用者與群組*索引標籤。
3. 在頁面最右側、選取*遠端群組*。
4. 選取*「Add*」。

   在此視窗中、您可以看到Astra Control從目錄擷取的LDAP群組一般名稱和辨別名稱清單。

5. 或者、您也可以在*依一般名稱篩選*欄位中輸入群組的一般名稱、以搜尋LDAP群組。
6. 從清單中選取一或多個群組。
7. 指派角色給群組。

您選取的角色會指派給此群組中的所有使用者。如果您指派不同的角色給使用者和使用者群組、則權限越高的角色優先。

8. 您也可以將一或多個命名空間限制指派給此群組、然後選取*限制角色限制*以強制執行限制。您可以選取*新增限制*來新增命名空間限制。

當使用者透過LDAP群組成員資格指派多個角色時、最具權限角色的限制是唯一會生效的限制。例如、如果具有本機檢視器角色的使用者加入三個繫結至「成員」角色的群組、則「成員」角色的限制總和會生效、而且會忽略「檢視器」角色的任何限制。

9. 選取*「Add*」。

結果

新群組會出現在遠端群組清單中。此群組中的遠端使用者不會出現在遠端使用者清單中、直到每個遠端使用者登入為止。在此清單中、您可以查看群組的詳細資料、也可以從*「動作」*功能表管理群組。

檢視及管理通知

Astra會在行動完成或失敗時通知您。例如、如果成功完成應用程式的備份、您會看到通知。

您可以從介面右上角管理這些通知：

步驟

1. 選取右上角的未讀取通知數。
2. 檢閱通知、然後選取*標示為已讀取*或*顯示所有通知*。

   如果您選取*顯示所有通知*、則會載入「通知」頁面。

3. 在*通知*頁面上、檢視通知、選取您要標示為已讀的通知、選取*行動*、然後選取*標示為已讀*。

新增及移除認證資料

隨時從ONTAP 您的帳戶新增及移除本地私有雲端供應商的認證資料、例如用OpenShift管理的Kubernetes叢集、或Unmanaged Kubernetes叢集。Astra Control Center會使用這些認證資料來探索叢集和叢集上的應用程式、並代表您配置資源。

請注意、Astra Control Center中的所有使用者都共用相同的認證資料集。

新增認證資料

您可以在管理叢集時、將認證新增至Astra Control Center。若要透過新增叢集來新增認證、請參閱 "新增Kubernetes叢集"。

如果您建立自己的 kubeconfig 檔案、則應該只定義其中的 * 一 * 內容元素。請參閱 "Kubernetes 文件" 以取得建立 kubeconfig 檔案的相關資訊。

移除認證資料

隨時從帳戶移除認證資料。您只能在之後移除認證 "取消管理所有相關的叢集"。

您新增至Astra Control Center的第一組認證資料一律使用中、因為Astra Control Center使用認證資料來驗證備份儲存區。最好不要移除這些認證資料。

步驟

1. 選擇*帳戶*。
2. 選取*認證*索引標籤。
3. 在*狀態*欄中選取您要移除之認證的「選項」功能表。
4. 選擇*移除*。
5. 輸入「移除」一詞以確認刪除、然後選取*是、移除認證*。

結果

Astra Control Center會從帳戶移除認證資料。

監控帳戶活動

您可以檢視Astra Control帳戶中活動的詳細資料。例如、當邀請新使用者、新增叢集或擷取快照時。您也可以將帳戶活動匯出至CSV檔案。

如果您從Astra Control管理Kubernetes叢集、且Astra Control已連線Cloud Insights 至原地、Astra Control會將事件記錄傳送至Cloud Insights 原地。日誌資訊（包括Pod部署和PVc附件的相關資訊）會顯示在Astra Control活動記錄中。使用此資訊來識別您所管理的Kubernetes叢集上的任何問題。

檢視**Astra Control**中的所有帳戶活動

1. 選擇*活動*。
2. 使用篩選器縮小活動清單範圍、或使用搜尋方塊找到您想要的確切內容。
3. 選取*匯出至CSV*、將您的帳戶活動下載至CSV檔案。

檢視特定應用程式的帳戶活動

1. 選取*應用程式*、然後選取應用程式名稱。
2. 選擇*活動*。

檢視叢集的帳戶活動

1. 選取*叢集*、然後選取叢集名稱。
2. 選擇*活動*。

採取行動以解決需要注意的事件

1. 選擇*活動*。
2. 選取需要注意的事件。
3. 選取*「採取行動」*下拉式選項。

   您可在此清單中檢視可能採取的修正行動、檢視與問題相關的文件、並取得協助解決問題的支援。

更新現有授權

您可以將試用版授權轉換為完整授權、也可以使用新授權來更新現有的試用版或完整授權。如果您沒有完整授權、請與NetApp銷售聯絡人聯絡、以取得完整授權與序號。您可以使用Astra Control Center UI或 "Astra Control API" 以更新現有授權。

步驟

1. 登入 "NetApp 支援網站"。
2. 存取Astra Control Center下載頁面、輸入序號、然後下載完整的NetApp授權檔案（NLF）。
3. 登入Astra Control Center UI。
4. 從左側導覽中、選取*帳戶*>*授權*。
5. 在「帳戶>*授權*」頁面中、選取現有授權的狀態下拉式功能表、然後選取「取代」。
6. 瀏覽至您下載的授權檔案。
7. 選取*「Add*」。

「帳戶>*授權*」頁面會顯示授權資訊、到期日、授權序號、帳戶ID及使用的CPU單位。

以取得更多資訊

- "Astra Control Center授權"

版權資訊

商標資訊