屬性型存取控制
ONTAP 9

NetApp
January 17, 2025

目錄

屬性型存取控制

使用 ONTAP 進行屬性型存取控制

您可以使用 ONTAP 來實作具有屬性和屬性型存取控制（ ABAC ）的增強 RBAC 。ONTAP 提供數種客戶可用來達成檔案層級 ABAC 的方法，包括使用 NFS 和 SMB/CIFS 的標記 NFS 4.2 和 XATTRS 。

屬性型存取控制（ ABAC ）是管理存取權限的精密方法，可考量使用者屬性，資源屬性和環境條件。國家標準與技術研究所（ NIST ）已建立 ABAC 標準，提供安全且一致的實作架構。

從 ONTAP 9 。 12.1 開始，您可以使用 NFSv4.2 安全性標籤和延伸屬性（ XATTRS ）來設定 ONTAP ，以便將其與角色型存取控制（ RBAC ）和屬性型存取控制（ ABAC ）身分識別整合。這項整合可讓 ONTAP 存取歸類為 NIST ABAC 相容資料管理解決方案的控制軟體，提供強大且進階的方法來管理複雜環境中的存取權限，包括原則強制執行點（ PEP ），原則決策點（ PDP ），以及考慮與使用者，資源和環境相關屬性的原則。

NetApp ONTAP 與延伸屬性（ XATTRS ）和屬性型存取控制（ ABAC ）軟體的整合符合 NIST 特別出版品 800-162 中所述的準則，確保符合 ABAC 實作的 NIST 標準。使用 NFS 4.2 安全標籤和 XATTRS ，可將使用者定義的屬性與檔案關聯，符合 NIST ABAC 標準在存取控制決策中考量資源屬性的要求。ABAC 軟體的 PEP 和 PDp 符合 NIST ABAC 標準，在存取控制程序中對這些元件的要求。能夠定義複雜的原則，以考量多種屬性和條件，符合 NIST ABAC 標準對原則型存取控制的要求。

相關資訊

- "使用 ONTAP 的 ABAC 方法"
- "NetApp ONTAP 中的 NFS ：最佳實務做法與實作指南"
- 徵求意見（ RFC ）
  - RFC 2203 ： RPCSEC_GSS 傳輸協定規格
  - RFC 3530 ：網路檔案系統（ NFS ）第 4 版傳輸協定

使用 ONTAP 的 ABAC 方法

ONTAP 提供各種方法供客戶用來達成檔案層級 ABAC ，包括使用 NFS 和 SMB/CIFS 的標示 NFSv4.2 和 XATTRS 。

標示為 NFSv4.2

從 ONTAP 9 · 9.1 開始，支援稱為 NFS 的 NFSv4.2 功能。

標記的 NFS 是一種使用 SELinux 標籤和強制存取控制（ MAC ）來管理精細檔案和資料夾存取的方法。這些 MAC 標籤會與檔案和資料夾一起儲存，並與 UNIX 權限和 NFSv4.x ACL 搭配使用。

支援標記的 NFS 表示 ONTAP 現在能夠辨識及瞭解 NFS 用戶端的 SELinux 標籤設定。RFC-7204 涵蓋標籤 NFS 。

標示為 NFSv4.2 的使用案例包括：

- 虛擬機器（ VM ）映像的 Mac 標籤
- 公共部門的資料安全性分類（秘密，機密和其他分類）
- 安全法規遵循
- 無磁碟Linux

啟用標記的 **NFSv4.2**

您可以使用下列進階權限選項來啟用或停用標記為 NFS ：

```
[-v4.2-seclabel {enabled|disabled}] - NFSV4.2 Security Label Support
(privilege: advanced)
```

此參數為選用參數，預設設定為 `disabled`。

標示為 **NFSv4.2** 的強制模式

從 ONTAP 9 · 9.1 開始， ONTAP 支援下列強制模式：

- * 有限伺服器模式 * ： ONTAP 無法強制執行標籤，但可以儲存及傳輸標籤。

  變更MAC標籤的能力也取決於用戶端強制執行。

- * 來賓模式 * ：如果用戶端未標示 NFS 感知（ v4.1 或更低版本），則 MAC 標籤不會傳輸。

ONTAP 目前不支援「完整模式」（儲存及強制執行 MAC 標籤）。

標有 **NFSv4.2** 的組態範例

以下組態範例示範使用 Red Hat Enterprise Linux 9.3 （ Plow ）版本的概念。

根據 John R. Smith 的認證建立的使用者 `jrsmith`擁有下列 Privileges 帳戶：

- 使用者名稱 = `jrsmith`
- Privileges = `uid=1112(jrsmith) gid=1112(jrsmith) groups=1112(jrsmith) context=user_u:user_r:user_t:s0`

有兩種角色：系統管理員帳戶是具有權限的使用者和使用者， `jrsmith`如下列 MLS Privileges 表所述：

使用者	角色	類型	層級
`admins`	`sysadm_r`	`sysadm_t`	`t:s0`
`jrsmith`	`user_r`	`user_t`	`t:s1 - t:s4`

在此範例環境中，使用者 `jrsmith`**可以存取層級為的** `s3`**檔案** `s0`。我們可以加強現有的安全性分類，如下所述，以確保系統管理員無法存取使用者專屬的資料。

- S0 = 權限管理使用者資料

- S0 = 未分類資料
- S1 = 機密
- S2 = 機密資料
- S3 = 重要機密資料

遵循貴組織的安全性原則

包含 **MCS** 的 **NFSv4.2** 安全性標籤範例

除了多層安全（ MLS ）之外，另一項稱為「多類別安全（ MCS ）」的功能可讓您定義專案等類別。

NFS 安全性標籤	價值
`entitySecurityMark`	`t:s01 = UNCLASSIFIED`

延伸屬性（ **XATTRS** ）

從 ONTAP 9 。 12.1 開始， ONTAP 支援 xatts 。 xatts 允許中繼資料與系統所提供的檔案和目錄相關聯，例如存取控制清單（ ACL ）或使用者定義的屬性。

若要實作 xattis ，您可以在 Linux 中使用 `setfattr`和 `getfattr`命令列公用程式來管理檔案系統物件的 xatts 。這些工具提供了一種強大的方法來管理檔案和目錄的其他中繼資料。雖然不當使用可能導致非預期行為或安全問題，但仍應謹慎使用。請務必參閱 `setfattr`和 `getfattr`手冊頁或其他可靠的文件，以取得詳細的使用說明。

在 ONTAP 檔案系統上啟用 xattis 時，使用者可以設定，修改及擷取檔案上的任意屬性。這些屬性可用來儲存標準檔案屬性集未擷取之檔案的其他資訊，例如存取控制資訊。

在 **ONTAP** 中使用 **xattis** 的要求

- Red Hat Enterprise Linux 8.4 或更新版本
- Ubuntu 22.04或更新版本
- 每個檔案最多可有 128 個 xatts
- xattr 金鑰限制為 255 個位元組
- 組合金鑰或值大小為每個 xattr 1,229 位元組
- 目錄和檔案可以有 xattis
- 若要設定和擷取 xatts ， `w`或必須為使用者和群組啟用寫入模式位元

xattis 的使用案例

使用者命名空間內會使用 xattis ，不會對 ONTAP 本身具有任何內在意義。而是由與檔案系統互動的用戶端應用程式來決定及管理其實際應用程式。

xattr 使用案例範例：

- 記錄負責建立檔案的應用程式名稱。
- 保留取得檔案的電子郵件訊息參考資料。

- 建立分類架構以組織檔案物件。
- 使用檔案原始下載來源的 URL 來標示檔案。

用於管理 **xattis** 的命令

- `setfattr`：設定檔案或目錄的延伸屬性：

  ```
  setfattr -n <attribute_name> -v <attribute_value> <file or directory name>
  ```

  命令範例：

  ```
  setfattr -n user.comment -v test example.txt
  ```

- `getfattr`：檢索特定擴展屬性的值或列出文件或目錄的所有擴展屬性：

  特定屬性：`getfattr -n <attribute_name> <file or directory name>`

  所有屬性：`getfattr <file or directory name>`

  命令範例：

  ```
  getfattr -n user.comment example.txt
  ```

xattr	價值
`user.digitalIdentifier`	`CN=John Smith jrsmith, OU=Finance, OU=U.S.ACME, O=US, C=US`
`user.countryOfAffiliations`	`USA`

使用 **ACE** 進行延伸屬性的使用者權限

存取控制項目（ ACE ）是存取控制清單（ ACL ）中的元件，可定義授予個別使用者或特定資源（例如檔案或目錄）使用者群組的存取權限。每個 ACE 都會指定允許或拒絕的存取類型，並與特定的安全性主體（使用者或群組身分識別）相關聯。

檔案類型	擷取 **xattr**	設定 **xattis**
檔案	R	A ， w ， T
目錄	R	T

說明 xattis 所需的權限：

- 擷取 xattr* ：使用者讀取檔案或目錄的延伸屬性所需的權限。「 R 」表示需要讀取權限。* 設定 xattribut* ：修改或設定延伸屬性所需的權限。「 A 」，「 w 」和「 T 」代表不同的權限範例，例如附加，寫入及與 xatts 相關的特定權限。* 檔案 * ：使用者需要附加，寫入及可能與 xatts 相關的特殊權限，才能設定延伸屬性。* 目錄 * ：設定延伸屬性需要特定的權限「 T 」。

支援 **xattis** 的 **SMB/CIFS** 通訊協定

ONTAP 對 SMB/CIFS 通訊協定的支援延伸至完整處理 xattart ，這是 Windows 環境中檔案中繼資料不可或缺的一部分。延伸屬性可讓使用者和應用程式儲存標準檔案屬性集以外的其他資訊，例如作者詳細資料，自訂安全性描述元或應用程式專屬資料。ONTAP 的 SMB/CIFS 實作可確保完全支援這些 xatts ，讓您能夠與 Windows 服務和應用程式無縫整合，這些服務和應用程式都仰賴此中繼資料來執行功能和原則。

當透過 ONTAP 管理的 SMB/CIFS 共用存取或傳輸檔案時，系統會保留 xatts 的完整性，確保所有中繼資料都會保留且保持一致。這對於維護安全性設定以及依賴 xattis 進行組態或作業的應用程式而言特別重要。ONTAP 在 SMB/CIFS 環境中對 xatts 的強大處理能力，可確保不同平台和環境之間的檔案共用安全可靠，為使用者提供無縫體驗，並確保資料治理原則得以維持。無論是為了協同作業，資料歸檔或法規遵循， ONTAP 對於 SMB/CIFS 共享區中的 xattits 的重視，都代表了它對於混合式作業系統環境中卓越資料管理和互通性的承諾。

ABAC 中的原則執行點（ **PEP** ）和原則決策點（ **PDP** ）

在以屬性為基礎的存取控制（ ABAC ）系統中，原則強制執行點（ PEP ）和原則決策點（ PDP ）扮演著重要角色。PEP 負責強制執行存取控制原則，而 PDP 則根據原則決定是否授予或拒絕存取。

在所提供的 Python 程式碼片段內容中，指令碼本身就是 PEP 。它通過打開文件並讀取其內容來授予對該文件的訪問權限，或通過提升來拒絕訪問來執行訪問控制決策 `PermissionError`。

另一方面， PDP 則是基礎 SELinux 系統的一部分。當指令碼嘗試以特定 SELinux 內容開啟檔案時， SELinux 系統會檢查其原則，以決定是否授予或拒絕存取。然後指令碼會強制執行此決定。

以下是此程式碼在 ABAC 環境中如何運作的逐步範例：

1. 此指令碼會使用功能將 SELinux 內容設定為 `jrsmith`內容相關內容 `selinux.setcon()`。這相當於 `jrsmith`嘗試存取檔案。
2. 指令碼會嘗試開啟檔案。這就是政治人物扮演的角色。
3. SELinux 系統會檢查其原則，查看是否 `jrsmith`允許（或更具體地說，具有 `SELinux` 內容的使用者 `jrsmith`）存取檔案。這是 PDP 的角色。
4. 如果允許存取檔案，則 `jrsmith` SELinux 系統會讓指令碼開啟檔案，指令碼會讀取及列印檔案內容。
5. 如果不允許存取檔案，則 `jrsmith` SELinux 系統會阻止指令碼開啟檔案，指令碼會提出 `PermissionError`。
6. 指令碼會還原原始的 SELinux 內容，以確保暫時內容變更不會影響其他作業。

使用 python 時，取得內容的程式碼如下所示，其中變數檔案路徑是要檢查的文件：

```
#Get the current context

context = selinux.getfilecon(file_path)[1]
```

ONTAP 複製與 **SnapMirror**

ONTAP 的複製和 SnapMirror 技術旨在提供高效可靠的資料複寫和複製功能，確保檔案資料的所有層面（包括擴充屬性（ xatts ））都會隨檔案一起保留和傳輸。 xattis 非常重要，因為它們會儲存與檔案相關的其他中繼資料，例如安全標籤，存取控制資訊和使用者定義的資料，這些資料是維護檔案內容和完整性所不可或缺的要素。

使用 ONTAP 的 FlexClone 技術複製磁碟區時，會建立磁碟區的完全可寫入複本。這項複製程序既即時又節省空間，而且包含所有檔案資料和中繼資料，可確保完整複寫 xattis 。同樣地， SnapMirror 也能確保資料鏡射到具有完全逼真度的次要系統。這包括 xattis ，對於仰賴此中繼資料才能正常運作的應用程式而言，這是非常重要的。

NetApp ONTAP 在複製和複寫作業中納入 xattis ，可確保完整的資料集及其所有特性，在主要和次要儲存系統中均可用且一致。對於需要一致的資料保護，快速恢復，以及遵守法規遵循與法規標準的組織而言，這種全方位的資料管理方法非常重要。它也能簡化不同環境（無論是內部部署或雲端環境）的資料管理，讓使用者確信在這些程序中，資料完整且不會遭到竄改。

NFSv4.2 安全性標籤有中定義的注意事項標示為 NFSv4.2。

控制資料存取的範例

以下儲存在 John R Smith 的 PKI 認證書中的資料項目範例，說明如何將 NetApp 的方法套用至檔案，並提供精細的存取控制。

這些範例僅供說明用途，政府有責任定義什麼是 NFSv4.2 安全性標籤和 xatts 。為了簡化更新和保留標籤的作業，我們省略了相關詳細資料。

金鑰	價值
entitySecurityMark	T:S01 = 未分類

金鑰	價值

資訊	{
	"commonName": {
	"value": "Smith John R jrsmith"
	},
	"emailAddresses": [
	{
	"value": "jrsmith@dod.mil"
	}
	],
	"employeeId": {
	"value": "00000387835"
	},
	"firstName": {
	"value": "John"
	},
	"lastName": {
	"value": "Smith"
	},
	"telephoneNumber": {
	"value": "938/260-9537"
	},
	"uid": {
	"value": "jrsmith"
	}
	}

規格	" 職稱 "
UUID	b4111349-7875-4115-AD30-0928565f2e15

管理組織	{
	"value": "DoD"
	}

金鑰	價值

簡報	[
	  {
	  "value": "ABC1000"
	  },
	  {
	  "value": "DEF1001"
	  },
	  {
	  "value": "EFG2000"
	  }
	]

公民身分	{
	  "value": "US"
	}

餘隙	[
	  {
	  "value": "TS"
	  },
	  {
	  "value": "S"
	  },
	  {
	  "value": "C"
	  },
	  {
	  "value": "U"
	  }
	]

國家分支機構	[
	  {
	  "value": "USA"
	  }
	]

金鑰	價值

數位識別碼	<pre>{
	  "classification": "UNCLASSIFIED",
	  "value": "cn=smith john r jrsmith, ou=dod, o=u.s.
	government, c=us"
	}</pre>

dissemTos	<pre>{
	  "value": "DoD"
	}</pre>

二合一組織	<pre>{
	  "value": "DoD"
	}</pre>

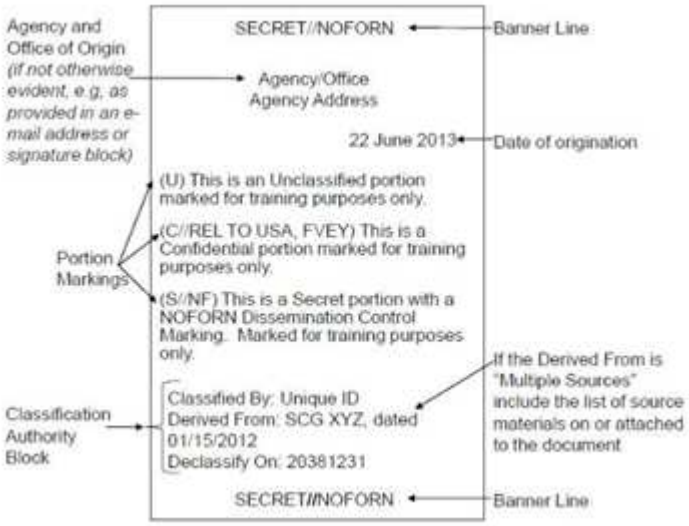
entityType	<pre>{
	  "value": "GOV"
	}</pre>

fineAccessControls	<pre>[
	  {
	  "value": "SI"
	  },
	  {
	  "value": "TK"
	  },
	  {
	  "value": "NSYS"
	  }
	]</pre>

這些 PKI 授權可顯示 John R. Smith 的存取詳細資料，包括依資料類型和歸屬來存取。

如果 John R. Smith 根據相關的政策指引指示建立並儲存名為「 *sample_Analysis .doc* 」的文件，使用者將根據文件分類，新增適當的橫幅和部分標記，代理商和原產地，以及適當的分類授權區塊，如下圖所示。這種豐富的中繼資料只有在經過自然語言處理（ NLP ）掃描，並套用規則以使標記具有意義之後，才能理解。NetApp BlueXP 分類等工具雖然可以做到這一點，但對於存取控制決策來說效率較低，因為它們需要權限才能查看文件內部。

未經分類的 **CAPCO** 文件部分標示



在 IC-TDF 中繼資料與檔案分開儲存的情況下， NetApp 主張額外提供一層精細的存取控制。這包括在目錄層級儲存存取控制資訊，以及與每個檔案相關聯。例如，請考慮連結至檔案的下列標記：

- NFSv4.2 安全標籤：用於做出安全決策
- xattis ：提供與檔案及組織方案需求相關的補充資訊

下列金鑰值配對是中繼資料的範例，可儲存為 xatts ，並提供檔案建立者及相關安全性分類的詳細資訊。用戶端應用程式可以利用這項中繼資料來做出明智的存取決策，並根據組織標準和要求來組織檔案。

金鑰	價值
`user.uuid`	`"761d2e3c-e778-4ee4-997b-3bb9a6a1d3fa"`
`user.entitySecurityMark`	`"UNCLASSIFIED"`
`user.specification`	`"INFO"`

金鑰	價值

user.Info	{
	"commonName": {
	"value": "Smith John R jrsmith"
	},
	"currentOrganization": {
	"value": "TUV33"
	},
	"displayName": {
	"value": "John Smith"
	},
	"emailAddresses": [
	"jrsmith@example.org"
	],
	"employeeId": {
	"value": "00000405732"
	},
	"firstName": {
	"value": "John"
	},
	"lastName": {
	"value": "Smith"
	},
	"managers": [
	{
	"value": ""
	}
	],
	"organizations": [
	{
	"value": "TUV33"
	},
	{
	"value": "WXY44"
	}
	],
	"personalTitle": {
	"value": ""
	},
	"secureTelephoneNumber": {
	"value": "506-7718"
	},
	"telephoneNumber": {
	"value": "264/160-7187"
	},
	"title": {
	"value": "Software Engineer"
	},

金鑰	價值
user.geo_point	[-78.7941, 35.7956]

```
    }
  }
```

稽核標籤變更

稽核對 xattis 或 NFS 安全性標籤所做的變更，是檔案系統管理與安全性的關鍵層面。標準檔案系統稽核工具可監控及記錄檔案系統的所有變更，包括修改延伸屬性和安全性標籤。

在 Linux 環境中， `auditd`常駐程式通常用於建立檔案系統事件的稽核。它可讓系統管理員設定規則，以監控與 `xattr` 變更相關的特定系統呼叫，例如 `setxattr`，`lsetxattr`以及 `fsetxattr`設定屬性和 `removexattr`，`lremovexattr`以及 `fremovexattr`移除屬性。

ONTAP FPolicy 提供強大的架構，可即時監控及控制檔案作業，進而擴充這些功能。FPolicy 可設定為支援各種 xattr 事件，提供對檔案作業的精細控制，以及強制執行全方位資料管理原則的能力。

對於使用 xattis 的使用者，尤其是在 NFSv3 和 NFSv4 環境中，僅支援特定的檔案作業和篩選器組合來進行監控。NFSv3 和 NFSv4 檔案存取事件的 FPolicy 監控支援的檔案作業和篩選器組合清單詳述如下：

支援的檔案作業	支援的篩選器
setattr	offline-bit, setattr_with_owner_change, setattr_with_group_change, setattr_with_mode_change, setattr_with_modify_time_change, setattr_with_access_time_change, setattr_with_size_change, exclude_directory

setattr 作業的 **auditd** 記錄片段範例：

```
type=SYSCALL msg=audit(1713451401.168:106964): arch=c000003e syscall=188
success=yes exit=0 a0=7fac252f0590 a1=7fac251d4750 a2=7fac252e50a0 a3=25
items=1 ppid=247417 pid=247563 auid=1112 uid=1112 gid=1112 euid=1112
suid=1112 fsuid=1112 egid=1112 sgid=1112 fsgid=1112 tty=pts0 ses=141
comm="python3" exe="/usr/bin/python3.9"
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
key="*set-xattr*"ARCH=x86_64 SYSCALL=**setxattr** AUID="jrsmith"
UID="jrsmith" GID="jrsmith" EUID="jrsmith" SUID="jrsmith"
FSUID="jrsmith" EGID="jrsmith" SGID="jrsmith" FSGID="jrsmith"
```

為使用 xattis 的使用者啟用 ONTAP FPolicy ，可提供一層可見度和控制權，這對於維護檔案系統的完整性和安全性至關重要。利用 FPolicy 的進階監控功能，組織可以確保追蹤，稽核 xatts 的所有變更，並符合其安全性與法規遵循標準。這種主動式檔案系統管理方法，是為何強烈建議任何想要加強資料治理和保護策略的組織採用 ONTAP FPolicy 的原因。

與 **ABAC** 身分識別與存取控制軟體整合

為了充分運用屬性型存取控制（ ABAC ）的功能， ONTAP 可與 ABAC 導向的身分識別與存取管理軟體整合。

NetApp 與此內容並行，也使用 GreyBox 執行參考實作。此內容的一項假設是，政府的身分識別，驗證和存取服務至少包括原則執行點（ PEP ）和原則決策點（ PDP ），以作為存取檔案系統的中介。

在實際的設定中，組織會混合使用 NFS 安全性標籤和 xattis 。這些資料用於代表各種中繼資料，包括分類，安全性，應用程式和內容，這些都是做出 ABAC 決策的重要工具。例如， xattr 可用於儲存 PDP 用於其決策程序的資源屬性。可以定義屬性來代表檔案的分類層級（例如，「未分類」，「機密」，「秘密」或「最高機密」）。然後， PDP 可以利用此屬性來強制執行原則，限制使用者只能存取其分類層級等於或低於淨空層級的檔案。

ABAC 流程範例

1. 使用者向系統存取 PEP 提供認證（例如， PKI ， OAuth ， SAML ），並從 PDP 取得結果。

   PEP 的角色是攔截使用者的存取要求，並將其轉送至 PDP 。

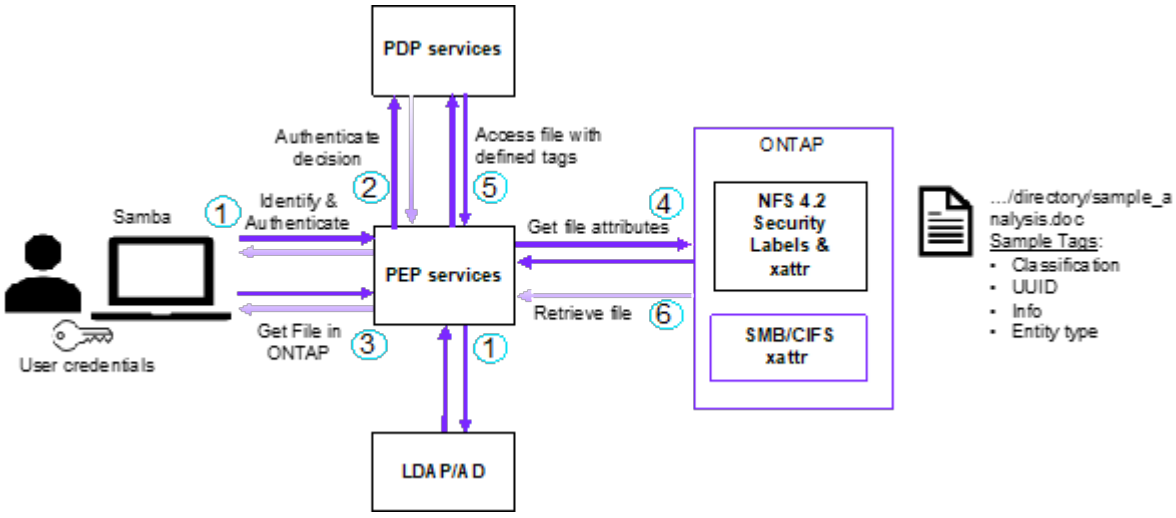
2. 然後， PDP 會根據已建立的 ABAC 原則來評估此要求。

   這些原則會考量與使用者，相關資源及周邊環境相關的各種屬性。根據這些原則， PDP 會決定是否允許存取，然後將此決定傳回給 PEP 。

   PDP 為 PEP 提供強制政策。然後，根據 PDP 的決定， PEP 會強制執行此決定，授予或拒絕使用者的存取要求。

3. 成功要求後，使用者會要求儲存在 ONTAP （例如 AFF ， AFF C ）中的檔案。
4. 如果申請成功，則 PEP 會從文件中取得精細的存取控制標籤。
5. PEP 根據該使用者的認證要求使用者的原則。
6. 如果使用者有權存取檔案，且可讓使用者擷取檔案，則 PEP 會根據原則和標籤做出決定。

實際存取可能是使用未透過代理的權杖來完成。



相關資訊

- "NetApp ONTAP 中的 NFS ：最佳實務做法與實作指南"
- 徵求意見（ RFC ）

- RFC 2203 ： RPCSEC_GSS 傳輸協定規格
- RFC 3530 ：網路檔案系統（ NFS ）第 4 版傳輸協定