



## **TR-4921** : 勒索軟體防禦

How to enable StorageGRID in your environment

NetApp  
July 05, 2024

# 目錄

TR-4921：勒索軟體防禦 .....	1
保護 StorageGRID S3 物件免受勒索軟體的侵害 .....	1
使用物件鎖定的勒索軟體防禦 .....	1
使用複製的貯體搭配版本管理功能來防範勒索軟體 .....	4
使用具有保護性 IAM 原則的版本管理功能來防範勒索軟體 .....	6

# TR-4921：勒索軟體防禦

## 保護 StorageGRID S3 物件免受勒索軟體的侵害

瞭解勒索軟體攻擊、以及如何使用 StorageGRID 安全最佳實務來保護資料。

勒索軟體攻擊不斷增加。本文件針對如何保護 StorageGRID 上的物件資料提供一些建議。

現今的勒索軟體是資料中心永遠存在的危險。勒索軟體旨在加密資料、使依賴資料的使用者和應用程式無法使用。保護從強化網路和可靠使用者安全實務的一般防禦措施開始、我們必須遵循資料存取安全實務。

勒索軟體是當今最大的安全威脅之一。NetApp StorageGRID 團隊正與我們的客戶合作、以對抗這些威脅。使用物件鎖定和版本設定功能、您可以防範不必要的變更、並從惡意攻擊中恢復。資料安全性是一項多層風險、您的物件儲存設備只是資料中心的一部分。

### StorageGRID 最佳實務做法

對於 StorageGRID、安全性最佳實務做法應包括使用 HTTPS 搭配簽署的憑證、以進行管理和物件存取。為應用程式和個人建立專屬的使用者帳戶、請勿使用租戶根帳戶來存取應用程式或存取使用者資料。換句話說、請遵循最低權限原則。使用具有定義身分識別與存取管理 (IAM) 原則的安全性群組來管理使用者權限、以及存取應用程式和使用者的專屬帳戶。有了這些措施、您仍必須確保資料受到保護。在 Simple Storage Service (S3) 的情況下、當物件經過修改以加密時、則是透過覆寫原始物件來完成。

### 防禦方法

S3 API 的主要勒索軟體保護機制是實作物件鎖定。並非所有應用程式都與物件鎖定相容、因此本報告中說明的還有兩個其他選項可保護您的物件：複寫到另一個已啟用版本設定的儲存庫、以及使用 IAM 原則進行版本設定。

### 何處可找到其他資訊

若要深入瞭解本文所述資訊、請檢閱下列文件和 / 或網站：

- NetApp StorageGRID 文件中心 <https://docs.netapp.com/us-en/storagegrid-118/>
- NetApp StorageGRID 啟用 <https://docs.netapp.com/us-en/storagegrid-enable/>
- StorageGRID 文件資源頁面 <https://www.netapp.com/data-storage/storagegrid/documentation/>
- NetApp 產品文件 <https://www.netapp.com/support-and-training/documentation/>

## 使用物件鎖定的勒索軟體防禦

探索 StorageGRID 中的物件鎖定如何提供 WORM 模式來防止資料刪除或覆寫、以及它如何符合法規要求。

物件鎖定提供 WORM 模式、可防止物件遭到刪除或覆寫。StorageGRID 實作物件鎖定 "Cohasset 已評估" 有助於符合法規要求、支援合法持有、符合性模式、以及物件保留的治理模式、以及預設貯體保留原則。您必須啟用物件鎖定、以做為貯體建立和版本設定的一部分。物件的特定版本已鎖定、如果未定義版本 ID、則保留會置於物件的目前版本上。如果目前版本已設定保留、並嘗試刪除、修改或覆寫物件、則會以刪除標記或物件的新修訂

版做為目前版本來建立新版本、鎖定的版本會保留為非目前版本。對於尚未相容的應用程式、您仍可以使用物件鎖定和儲存在貯體上的預設保留組態。定義組態之後、這會將物件保留套用至置入貯體的每個新物件。只要將應用程式設定為在保留時間過去之前不刪除或覆寫物件、就會生效。

以下是使用物件鎖定 API 的幾個範例：

物件鎖定合法保留是套用至物件的簡單開 / 關狀態。

```
aws s3api put-object-legal-hold --bucket mybucket --key myfile.txt --legal-hold Status=ON --endpoint-url https://s3.company.com
```

如果成功、設定合法保留狀態不會傳回任何值、因此可以使用「取得」操作來驗證。

```
aws s3api get-object-legal-hold --bucket mybucket --key myfile.txt --endpoint-url https://s3.company.com
{
  "LegalHold": {
    "Status": "ON"
  }
}
```

若要關閉合法保留、請套用關閉狀態。

```
aws s3api put-object-legal-hold --bucket mybucket --key myfile.txt --legal-hold Status=OFF --endpoint-url https://s3.company.com
aws s3api get-object-legal-hold --bucket mybucket --key myfile.txt --endpoint-url https://s3.company.com
{
  "LegalHold": {
    "Status": "OFF"
  }
}
```

設定物件保留會以保留到時間戳記完成。

```
aws s3api put-object-retention --bucket mybucket --key myfile.txt --retention '{"Mode": "COMPLIANCE", "RetainUntilDate": "2022-06-10T16:00:00"}' --endpoint-url https://s3.company.com
```

同樣地、成功後沒有傳回的值、因此您可以使用 GET 通話來驗證保留狀態。

```
aws s3api get-object-retention --bucket mybucket --key myfile.txt
--endpoint-url https://s3.company.com
{
  "Retention": {
    "Mode": "COMPLIANCE",
    "RetainUntilDate": "2022-06-10T16:00:00+00:00"
  }
}
```

在啟用物件鎖定的貯體上放置預設保留、會使用以天和年為單位的保留期間。

```
aws s3api put-object-lock-configuration --bucket mybucket --object-lock-configuration '{ "ObjectLockEnabled": "Enabled", "Rule": { "DefaultRetention": { "Mode": "COMPLIANCE", "Days": 1 } } }' --endpoint-url https://s3.company.com
```

如同大多數的作業一樣、成功時不會傳回任何回應、因此我們可以執行 Get 來驗證組態。

```
aws s3api get-object-lock-configuration --bucket mybucket --endpoint-url https://s3.company.com
{
  "ObjectLockConfiguration": {
    "ObjectLockEnabled": "Enabled",
    "Rule": {
      "DefaultRetention": {
        "Mode": "COMPLIANCE",
        "Days": 1
      }
    }
  }
}
```

接下來、您可以在套用保留組態的情況下、將物件放入貯體中。

```
aws s3 cp myfile.txt s3://mybucket --endpoint-url https://s3.company.com
```

Put 作業會傳回回應。

```
upload: ./myfile.txt to s3://mybucket/myfile.txt
```

在保留物件上、上一個範例中、貯體上設定的保留期間會轉換成物件上的保留時間戳記。

```
aws s3api get-object-retention --bucket mybucket --key myfile.txt
--endpoint-url https://s3.company.com
{
  "Retention": {
    "Mode": "COMPLIANCE",
    "RetainUntilDate": "2022-03-02T15:22:47.202000+00:00"
  }
}
```

## 使用複製的貯體搭配版本管理功能來防範勒索軟體

瞭解如何使用 StorageGRID CloudMirror 將物件複製到次要儲存庫。

並非所有應用程式和工作負載都能與物件鎖相容。另一個選項是將物件複製到同一個網格中的次要儲存格（最好是存取受限的不同租戶）、或是任何其他具有 StorageGRID 平台服務 CloudMirror 的 S3 端點。

StorageGRID CloudMirror 是 StorageGRID 的一個元件、可設定為在物件擷取到來源儲存區時、將儲存區的物件複製到定義的目的地、而不會複製刪除內容。由於 CloudMirror 是 StorageGRID 的整合式元件、因此它無法被 S3 API 型攻擊關閉或操控。您可以在啟用版本設定的情況下、設定此複製儲存區。在這種情況下、您需要自動清理複製貯體的舊版本、以安全丟棄。因此、您可以使用 StorageGRID ILM 原則引擎。建立規則、根據非目前時間管理物件放置、時間足以識別攻擊並從攻擊中恢復。

這種方法的一個缺點是、它會使用完整的第二個儲存區副本、以及保留一段時間的多個物件版本、來消耗更多儲存空間。此外、有意從主要貯體中刪除的物件必須從複製的貯體中手動移除。產品外部還有其他複製選項、例如 NetApp CloudSync、可針對類似解決方案複製刪除內容。啟用版本設定功能而未啟用物件鎖定功能的次要貯體另一個缺點是存在許多可用來在次要位置造成損害的特殊權限帳戶。優點是、它應該是該端點或租戶貯體的唯一帳戶、而且可能會造成的影響不包括主要位置上的帳戶存取權、反之亦然。

建立來源和目的地儲存區、並使用版本設定目的地之後、您可以設定及啟用複製、如下所示：

### 步驟

1. 若要設定 CloudMirror、請為 S3 目的地建立平台服務端點。

# Create endpoint

1

Enter details

2

Select authentication type  
Optional

## Enter endpoint details

Enter the endpoint's display name, URI, and URN.

Display name [?](#)

MyGrid

URI [?](#)

https://s3.company.com

URN [?](#)

arn:aws:s3:::mybucket

2. 在來源貯體上、將複寫設定為使用已設定的端點。

```
<ReplicationConfiguration>
  <Role></Role>
  <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
      <Bucket>arn:aws:s3:::mybucket</Bucket>
      <StorageClass>STANDARD</StorageClass>
    </Destination>
  </Rule>
</ReplicationConfiguration>
```

3. 建立 ILM 規則以管理儲存配置和版本儲存持續時間管理。在此範例中、會設定要儲存之物件的非最新版本。

## Create ILM Rule Step 1 of 3: Define Basics

Name	MyTenant - version retention
Description	retain non-current versions for 30 days
Tenant Accounts (optional)	mytenant [26261433202363150471]
Bucket Name	contains ~ mybucket

## Create ILM Rule Step 2 of 3: Define Placements

Configure placement instructions to specify how you want objects matched by this rule to be stored.

MyTenant - version retention  
retain non-current versions for 30 days

A rule that uses Noncurrent Time only applies to noncurrent versions of S3 objects.  
You cannot use this rule as the default rule in an ILM policy because it does not apply to current object versions.

Reference Time

Placements Sort by start day

From day  store for  days Add Remove

Type  Location  Add Pool Copies  Temporary location  + X

Retention Diagram Refresh

Duration 30 days Forever

站台 1 有兩份 30 天的複本。您也可以根據在 ILM 規則中使用擷取時間做為參考時間、來設定物件目前版本的規則、以符合來源貯體儲存持續時間。物件版本的儲存位置可以進行銷毀編碼或複寫。

## 使用具有保護性 IAM 原則的版本管理功能來防範勒索軟體

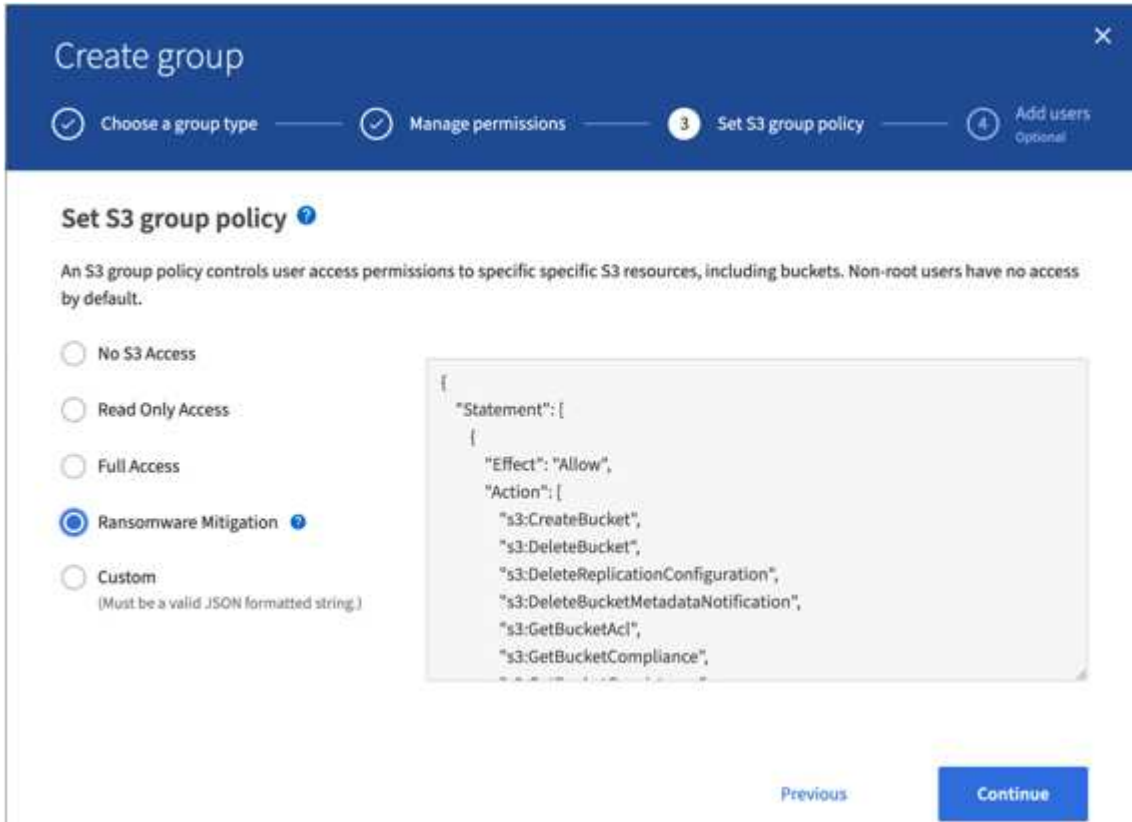
瞭解如何啟用貯體的版本設定功能、並在 StorageGRID 中的使用者安全性群組上實作 IAM 原則、以保護您的資料。

在不使用物件鎖定或複寫的情況下保護資料的方法、是在貯體上啟用版本設定、並在使用者安全性群組上實作 IAM 原則、以限制使用者管理物件版本的能力。發生攻擊時、會建立新的不良資料版本作為目前版本、而最新的非最新版本則是安全無虞的資料。為了取得資料存取權而遭入侵的帳戶無法刪除或以其他方式變更保護資料的非目前版本、以供日後還原作業使用。如同先前的案例、ILM 規則會在您選擇的期間內、管理非目前版本的保留。缺點是、仍然可能存在授權帳戶、導致不良攻擊者遭受攻擊、但所有應用程式服務帳戶和使用者都必須設定更具限制性的存取。限制性群組原則必須明確允許您希望使用者或應用程式能夠執行的每個動作、並明確拒絕您



不希望使用者或應用程式能夠執行的任何動作。NetApp 不建議使用萬用字元允許、因為未來可能會引進新的動作、而且您會想要控制是否允許或拒絕。對於此解決方案、拒絕清單必須包含 DeleteObjectVersion、PuttBucketPolicy、DeleteBucketPolicy、PuttLifecycleConfiguration 和 PuttBucketVersioning、以保護貯體和物件版本的版本設定、避免使用者或程式設計上的變更。

在 StorageGRID 11.7 中、我們推出了新的 S3 群組原則選項「勒索軟體緩解」、以簡化此解決方案的實作。在租戶中建立使用者群組時、選取群組權限之後、您可以看到這個新的選用原則。



以下是群組原則的內容、其中包含明確允許的大部分可用作業、以及最低要求的拒絕。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:CreateBucket",
        "s3>DeleteBucket",
        "s3>DeleteReplicationConfiguration",
        "s3>DeleteBucketMetadataNotification",
        "s3:GetBucketAcl",
        "s3:GetBucketCompliance",
        "s3:GetBucketConsistency",
        "s3:GetBucketLastAccessTime",
        "s3:GetBucketLocation",
        "s3:GetBucketNotification",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketObjectLockConfiguration"
      ]
    }
  ]
}
```

```

"s3:GetBucketPolicy",
"s3:GetBucketMetadataNotification",
"s3:GetReplicationConfiguration",
"s3:GetBucketCORS",
"s3:GetBucketVersioning",
"s3:GetBucketTagging",
"s3:GetEncryptionConfiguration",
"s3:GetLifecycleConfiguration",
"s3:ListBucket",
"s3:ListBucketVersions",
"s3:ListAllMyBuckets",
"s3:ListBucketMultipartUploads",
"s3:PutBucketConsistency",
"s3:PutBucketLastAccessTime",
"s3:PutBucketNotification",
"s3:PutBucketObjectLockConfiguration",
"s3:PutReplicationConfiguration",
"s3:PutBucketCORS",
"s3:PutBucketMetadataNotification",
"s3:PutBucketTagging",
"s3:PutEncryptionConfiguration",
"s3:AbortMultipartUpload",
"s3>DeleteObject",
"s3>DeleteObjectTagging",
"s3>DeleteObjectVersionTagging",
"s3:GetObject",
"s3:GetObjectAcl",
"s3:GetObjectLegalHold",
"s3:GetObjectRetention",
"s3:GetObjectTagging",
"s3:GetObjectVersion",
"s3:GetObjectVersionAcl",
"s3:GetObjectVersionTagging",
"s3:ListMultipartUploadParts",
"s3:PutObject",
"s3:PutObjectAcl",
"s3:PutObjectLegalHold",
"s3:PutObjectRetention",
"s3:PutObjectTagging",
"s3:PutObjectVersionTagging",
"s3:RestoreObject",
"s3:ValidateObject",
"s3:PutBucketCompliance",
"s3:PutObjectVersionAcl"
],
"Resource": "arn:aws:s3:::*"

```

```
    },
    {
      "Effect": "Deny",
      "Action": [
        "s3:DeleteObjectVersion",
        "s3:DeleteBucketPolicy",
        "s3:PutBucketPolicy",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketVersioning"
      ],
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

## 版權資訊

Copyright © 2024 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變更本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

## 商標資訊

NETAPP、NETAPP 標誌及 <http://www.netapp.com/TM> 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。