執行 Amazon Neptune 資料庫ISVs 的多租用戶指引

AWS 方案指引

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS 方案指引: 執行 Amazon Neptune 資料庫ISVs 的多租用戶指引

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商標和商業外觀不得用於任何非 Amazon 的產品或服務，也不能以任何可能造成客戶混淆、任何貶低或使 Amazon 名譽受損的方式使用 Amazon 的商標和商業外觀。所有其他非 Amazon 擁有的商標均為其各自擁有者的財產，這些擁有者可能附屬於 Amazon，或與 Amazon 有合作關係，亦或受到 Amazon 贊助。

Table of Contents

簡介 1
資料分割模型 2
Silo-model 3
每個租戶的叢集 3
孤島模型的實作指南 4
集區模型 6
LPGs的集區模型 7
屬性策略 7
字首標籤策略 9
多標籤策略 11
LPG 模型的效能影響 13
RDF 集區模型 14
使用圖形存放區 HTTP 通訊協定的 SPARQL 查詢選項 14
RDF 的租用戶隔離 15
準備成長 15
多租用戶案例的限制 16
混合模型 17
最佳實務 18
使用最新版本更新您的 Neptune 叢集 18
使用 deltas 而不是刪除和取代資料擷取 18
示範 Neptune 成本如何隨著租戶而演變 19
根據客戶需求擴展叢集 19
後續步驟 20
資源 21
貢獻者 22
文件歷史紀錄 23
詞彙表 24
..... 24
A 24
B 27
C 28
D 31
E 34
F 36

G 37
H 38
I 39
L 41
M 42
O 46
P 48
Q 50
R 50
S 53
T 56
U 57
V 58
W 58
Z 59
..... lx

ISVs 執行 Amazon Neptune 資料庫的多租戶指南

Amazon Web Services（貢獻者）

2024 年 8 月（文件歷史記錄）

多租戶是一種電腦系統架構，其中應用程式的單一執行個體可服務多個客戶。每個客戶都稱為租戶。在多租戶架構中，這些應用程式執行個體會在共用環境中運作，其中每個租戶實際上都位於相同的基礎設施上，但在邏輯上是分開的。

作為獨立軟體供應商（ISV），您可以使用 Amazon Neptune 為需要跨高度連線資料導覽的應用程式提供動力。您可能正在管理帳戶中的雲端型軟體即服務 SaaS）應用程式，並為租戶提供訂閱。然後，租戶可以透過網際網路或私下透過 存取服務 AWS PrivateLink。此模型的經濟性適用於雙方，因為租戶可以存取比購買、建置和維護成本更低的軟體。作為 ISV，您可以為訂閱收取的費用高於建立和維護軟體的費用。問題是您如何將業務擴展到多個租戶。

多租戶ISVs提供重要的經濟和營運優勢。多租戶架構為您的組織提供更好的投資回報（ROI）。多租戶也簡化了操作需求，讓您的組織可以更快地移動，並降低將軟體交付給租戶的成本。

本文件提供使用 Amazon Neptune 有效執行多租戶ISV應用程式的指引。本指南是以多年來取得的最佳實務為基礎，這些最佳實務支援 ISVs成功地將 SaaS 解決方案交付給其客戶。在組織目標和架構原則的背景下評估本指南，將可協助您找到最佳化解決方案的方法。

> **Note**
>
> 本文件不提供完整的最佳實務清單。它補充了適用於 Amazon Neptune 的 AWS Well-Architected Framework 文件，為多租戶ISV工作負載提供其他特定指南。我們建議您在設計解決方案時檢閱這兩個文件中的考量事項。

SaaS 資料分割模型

SaaS 開發人員面臨的挑戰之一，是設計架構模式，以在多租戶環境中代表和組織資料。這些多租戶儲存機制和模式通常稱為資料分割。

在多租戶 SaaS 環境中，區分資料分割和租戶隔離非常重要。這些概念雖然相關，但不是同義字。資料分割是指儲存每個租戶資料的方法。不過，僅分割並不保證租戶隔離。為了確保某個租戶的資料無法供另一個租戶存取，則需要採取其他措施。

多租戶 SaaS 系統中的三種常見資料分割模型是孤立、集區和混合模式。您選擇的任何模型取決於下列因素：

- 合規
- 噪音鄰里
- 分層策略
- 操作需求
- 租用戶隔離需求

此外， 上可用的每個資料庫類型 AWS 通常會提供唯一的資料分割和租用戶隔離模型集合。在查看如何組織租戶圖形以支援解決方案的各種需求時，請考慮 Amazon Neptune 提供的模型。

許多人從下列其中一項聲明ISVs開始在 Neptune 上設計：

- 此ISV解決方案需要跨不同叢集進行客戶實體隔離。
- ISV 解決方案需要建構，例如傳統關聯式資料庫管理系統中找到的具名資料庫或結構描述。

經過考量後，ISVs請了解這些聲明並不正確，因為在幾乎所有工作負載下，每個客戶在資料庫中都有中斷連線的圖表。實作本文件中討論的資料建模和存取指南，可防止跨越這些資料界限並維護客戶資料隱私權。

本指南同時說明孤島模型和集區模型 ，但大多數ISVs人選擇集區模型的成本和操作效率。本指南簡短討論混合模型，結合孤立系統和集區模型的各個層面。有些 為其最大客戶ISVs使用混合模型，以適應圖形大小的法規或合規要求。

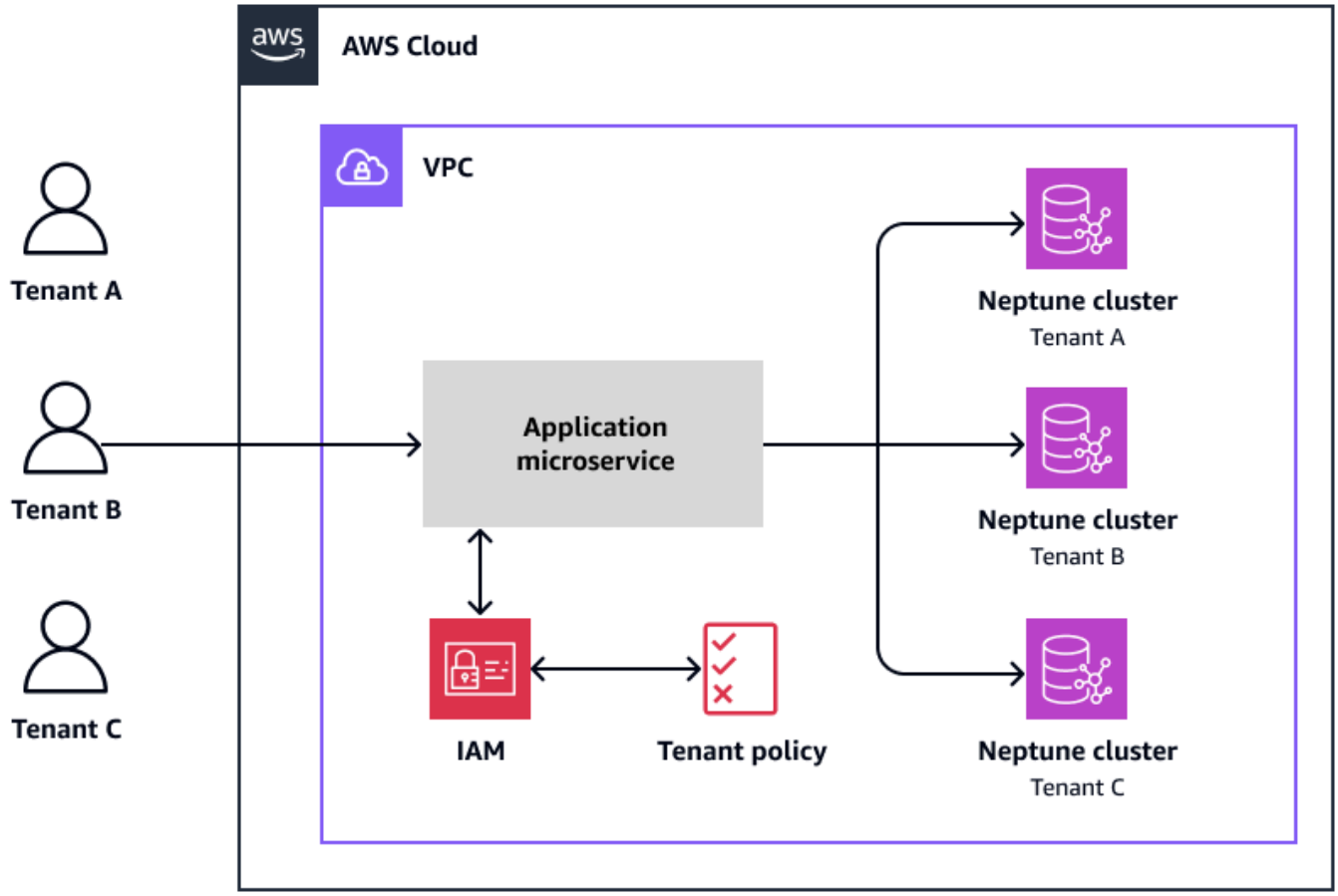
Silo 模型多租戶

由於合規和法規要求，某些多租戶 SaaS 環境可能需要將租戶的資料部署在完全分開的資源上。在某些情況下，大型客戶需要專用叢集來減少嘈雜的鄰里影響。在這些情況下，您可以套用孤島模型。

在孤島模型中，租戶資料的儲存與任何其他租戶資料完全隔離。用於表示租戶資料的所有建構都被視為該用戶端的實體唯一，這表示每個租戶通常都有不同的儲存、監控和管理。每個租用戶也會有一個單獨的 AWS Key Management Service（AWS KMS）金鑰進行加密。在 Amazon Neptune 中，孤島是每個租戶的一個叢集。

每個租戶的叢集

您可以透過每個叢集有一個租戶，使用 Neptune 實作孤島模型。下圖顯示三個租用戶在虛擬私有雲端（VPC）中存取應用程式微服務，每個租用戶都有單獨的叢集。



每個叢集都有其個別端點，以協助確保不同的存取點，以進行有效的資料互動和管理。透過將每個租戶放置在自己的叢集中，您可以在租戶之間建立定義明確的界限，以確保客戶的資料與其他租戶的資料成

功隔離。此隔離也吸引具有嚴格法規和安全限制的 SaaS 解決方案。此外，當每個租戶擁有自己的叢集時，您不必擔心噪音鄰，其中一個租戶施加的負載可能會對其他租戶的體驗造成不利影響。

雖然 cluster-per-tenant 孤島模型具有優勢，但它也會帶來管理和敏捷性挑戰。此模型的分散式性質使得彙整和評估租戶活動以及所有租戶的運作狀態變得更加困難。部署也變得更具挑戰性，因為設定新租戶現在需要佈建個別叢集。當用戶端升級和版本與資料庫升級緊密結合時，使用共用用戶端層的環境中升級變得更具挑戰性。

Neptune 同時支援無伺服器和佈建叢集。評估無伺服器或佈建執行個體是否更能處理您的應用程式工作負載。一般而言，如果您的工作負載有固定的需求層級，佈建的執行個體將更具成本效益。Serverless 已針對要求嚴苛、高度可變的工作負載進行最佳化，其資料庫使用量短，接著是長時間的輕度活動或無活動。

在每個租用戶使用 Neptune 佈建叢集時，您必須選取近似租用戶需求最大負載的執行個體大小。這種對伺服器的依賴也會對您的 SaaS 環境的擴展效率和成本產生串聯影響。雖然 SaaS 的目標是根據實際租戶負載動態調整大小，但 Neptune 佈建叢集會要求您過度佈建，以考慮負載中更大量的用量和尖峰時段。過度佈建會增加每個租用戶的成本。此外，隨著租用戶用量隨時間的變化，必須針對每個租用戶分別套用叢集的擴展或縮減。

Neptune 團隊通常會針對孤島模型提供建議，因為閒置資源所產生的成本較高，而且有其他操作複雜性。不過，對於受到高度管制或敏感的工作負載，客戶可能願意支付額外的成本。

孤島模型的實作指南

若要實作 cluster-per-tenant 孤立隔離模型，請建立 AWS Identity and Access Management（IAM）data-access 政策。這些政策透過確保租戶只能存取包含其自身資料的 Neptune 叢集來控制對租戶 Neptune 叢集的存取。將每個租戶IAM的政策連接至IAM角色。然後，應用程式微服務會使用 IAM角色，使用 AWS Security Token Service（）`AssumeRole`方法產生精細的臨時憑證AWS STS。這些憑證只能存取該租戶的 Neptune 叢集，用於連線至租戶的 Neptune 叢集。

下列程式碼片段顯示以資料為基礎的IAM政策範例：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "neptune-db:ReadDataViaQuery",
        "neptune-db:WriteDataViaQuery"
```

```
      ],
      "Resource": "arn:aws:neptune-db:<region>:<account-id>:tenant-1-cluster/*",
      "Condition": {
        "ArnEquals": {
          "aws:PrincipalArn": "arn:aws:iam::<account-id>:role/tenant-role-1"
        }
      }
    }
  ]
}
```

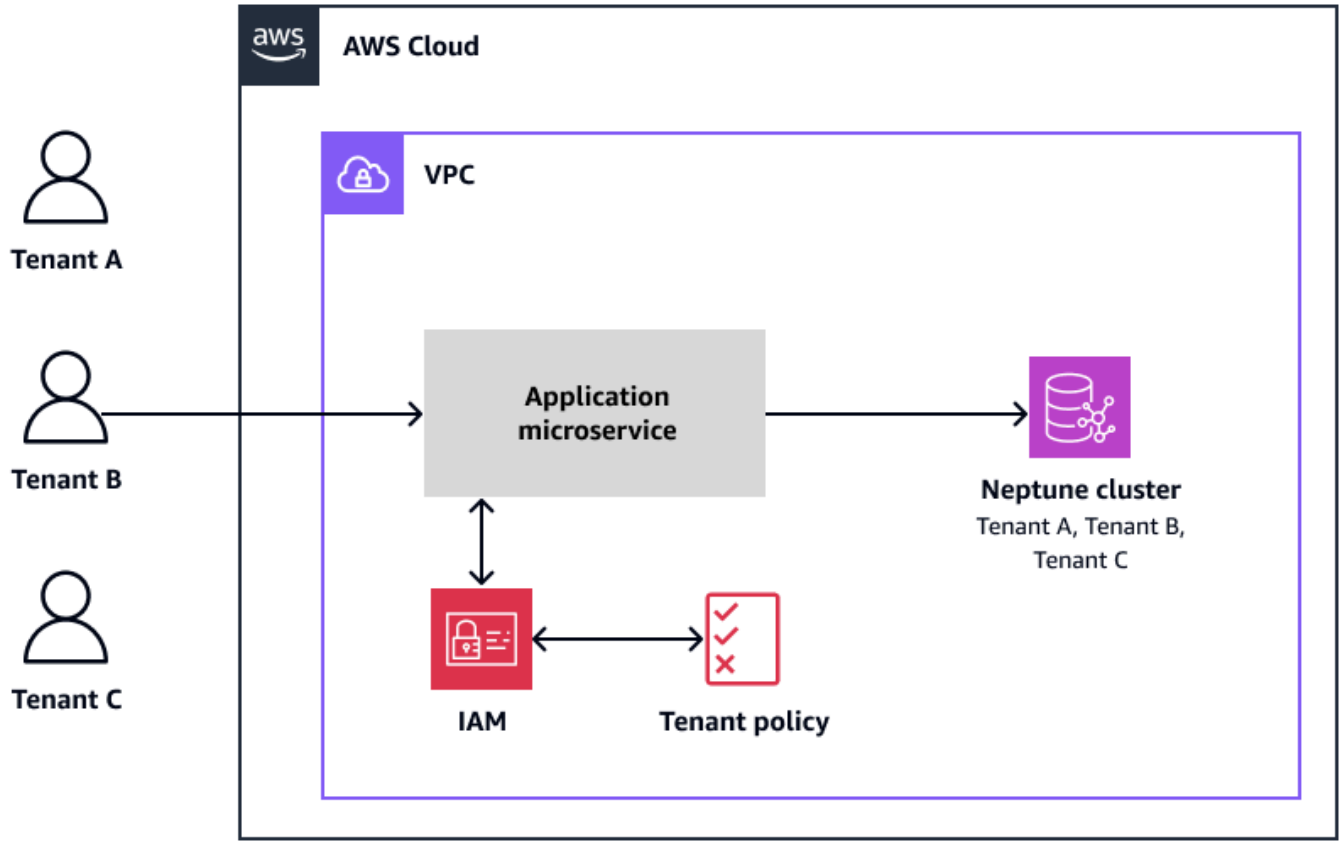
此程式碼提供範例租用戶 `tenant-1`，具有各自 Neptune 叢集的讀取和寫入查詢存取權。`Condition` 元素可確保只有擔任`tentant-1`IAM角色（）的呼叫實體（主體`tenant-role-1`）才能存取 `tenant-1`的 Neptune 叢集。

集區模型多租用

有時候，由於成本或營運開銷，實作孤立模型並不必要或可行：

- 您可能沒有資源來維護每個租用戶的個別叢集。
- 可能不需要實際分隔每個租戶的資料，而且邏輯分隔足以滿足其需求和合規要求。

下圖顯示集區模型，其中租用戶資料會放置在單一 Amazon Neptune 叢集中，且所有租用戶共用共同資料庫。



此集區隔離模型可減少管理開銷，並可提高營運效率，因為管理的叢集較少。此外，運算資源可以跨多個客戶共用，而不是在客戶非作用中期間保持閒置。

當您使用集區模型時，有兩種方式可建立資料模型。您的方法取決於您是使用資源描述架構 (RDF) 建置已標記的屬性圖形 (LPG) 還是圖形。 ???

標記屬性圖表的集區模型

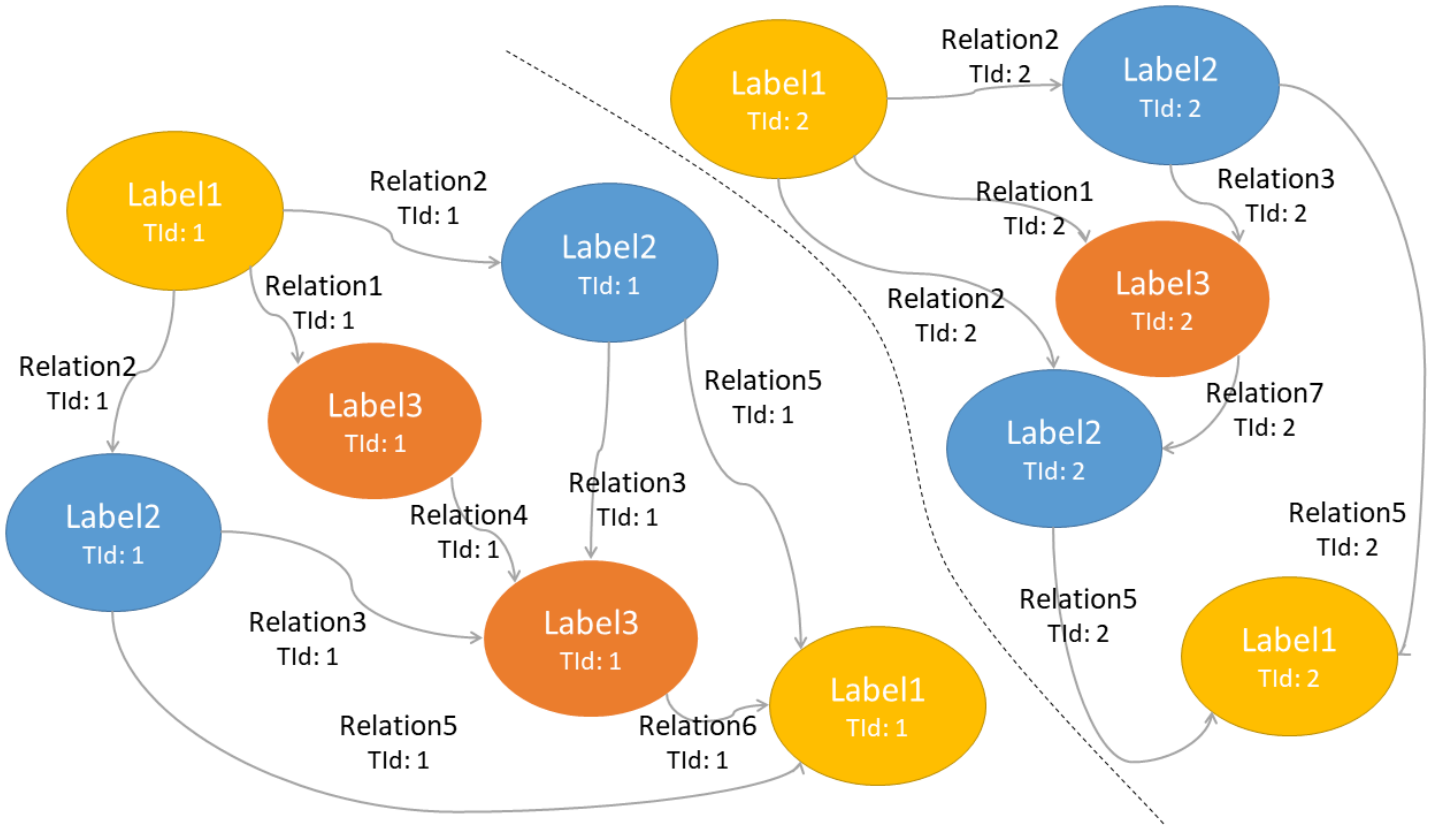
Amazon Neptune 上的 LPGs集區模型有三種不同的方法：

- 屬性策略 – 當您需要優先使用已建立的程式庫建構時，例如 Apache TinkerPop Gremlin 語言的 PartitionStrategy 而非效能，請選擇屬性策略。
- 字首標籤策略 – 根據效能和限制雜訊鄰近效果，我們建議大多數案例使用字首標籤策略。
- 多標籤策略 – 多標籤策略改善了前綴標籤策略的效能。它還支援執行跨叢集上所有租用戶的查詢（例如，用於報告或監控所有租用戶的 ISV 查詢）。

屬性策略

使用 LPGs，使用者可以將鍵值對屬性新增至節點、頂點和邊緣。為了實現邏輯分離，大多數客戶直覺地將此建模為每個節點和邊緣上具有通用租用戶屬性索引鍵的唯一屬性。租用戶屬性金鑰代表擁有節點的所有租用戶。租用戶識別符是識別個別租用戶的唯一值。

下圖顯示此模型。兩個中斷連接的子圖具有各種標記的節點和邊緣，租用戶屬性索引鍵由 表示`TId`。一個子圖的每個節點和邊緣都有 `TId`的值`1`。在另一個子圖中，每個節點和邊緣`TId`的值為 2。



在標記的屬性圖表中，有兩種管理此項目的方法。Gremlin 查詢語言提供 PartitionStrategy 周遊程式庫，以協助管理資料的資料分割。下列範例中的程式碼預期每個節點和邊緣都有名為 的屬性TId：

```
strategy1 = new PartitionStrategy(partitionKey: "TId", writePartition: "1",
 readPartitions: ["1"])
strategy2 = new PartitionStrategy(partitionKey: "TId", writePartition: "2",
 readPartitions: ["2"])
```

寫入新節點或邊緣時，"2"會根據是否strategy2選取 strategy1或 ，以 "1"或 的值"TId"新增 屬性。對於具有 "TId"之 的客戶"1"，您可以使用 strategy1。下列範例顯示為該客戶撰寫資料：

```
g.withStrategies(strategy1).addV("Label1").property("Value", "123456").property(id,
 "Item_1")
```

對於讀取查詢， "TId == '1'"或 的篩選條件"TId == '2'"會strategy2分別使用 strategy1或 新增至每個節點或邊緣周遊。這些分割區策略可簡化您的程式碼，但並非必要。使用 策略的好處是在授權層級插入，並傳遞至形成查詢的較低層級程式碼。這會將決定客戶識別符 (TId) 的程式碼與查詢的邏輯分開。

下列範例程式碼顯示讀取資料的 Gremlin 查詢：

```
g.withStrategies(strategy1).V().hasLabel("Label1")
```

上述程式碼等同於下列範例：

```
g.V().hasLabel("Label1").has("TId", "1")
```

同樣地，使用 Gremlin 寫入資料時，您可以使用下列查詢：

```
g.withStrategies(strategy1).addV("Label1").property("Value").property(id, "Item_1")
```

上述程式碼等同於下列範例，該範例不使用 分割區策略，因此需要明確寫入 "TId" 屬性：

```
g.addV("Label1").property("TId", "1").property("Value").property(id, "Item_1")
```

在 openCypher 中，這些程式庫不存在。您有責任撰寫和修改查詢，將租戶識別符新增為節點和邊緣上的屬性。例如：

```
CREATE (n:Item {`~id`: 'Item_1', Value: '123456', TId: '1'})
CREATE (n:Item {`~id`: 'Item_2', Value: '123456', TId: '2'})
```

請注意 Gremlin 程式碼之間沒有分割區策略的相似性。然後，您可以使用下列程式碼讀取從第一個CREATE陳述式寫入的節點：

```
MATCH (n:Item {TId: '1'})
RETURN n
--or
MATCH (n:Item)
WHERE n.TId == '1'
RETURN n
```

當您想要使用原生 TinkerPop Gremlin 建構，例如 PartitionStrategy 時，可以選擇 屬性策略。不過，相較於前綴標籤策略，此模型在 Amazon Neptune 上有效能缺點。如需這些效能缺點的討論，請參閱 LPG 模型的效能影響一節。

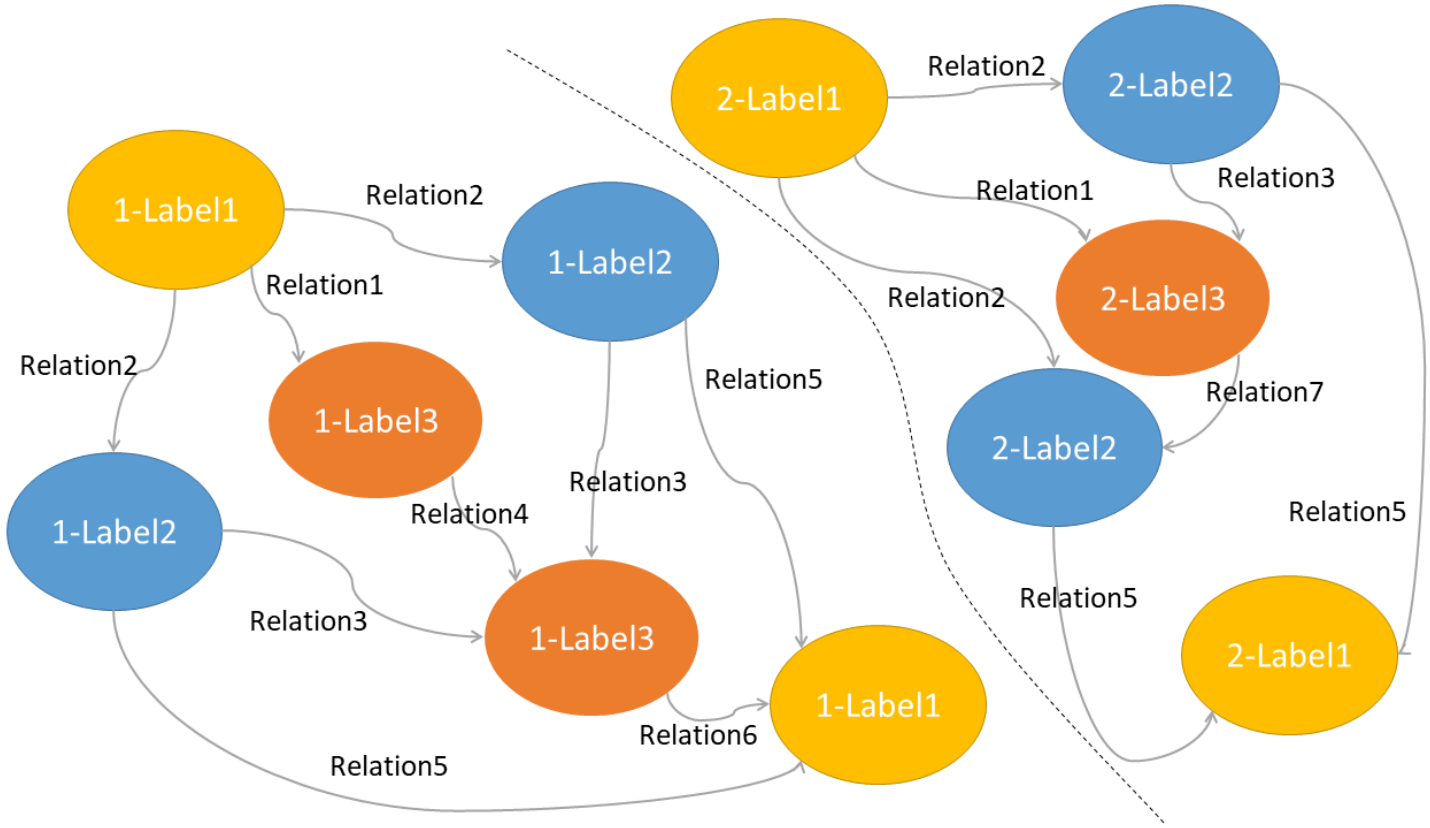
如果符合下列條件，請考慮僅在節點上建立屬性策略的模型，而不是在邊緣：

- 您的圖形邊緣明顯比標籤多。
- 每個租用戶都是中斷連線的圖形。
- 您只能使用節點做為起點，而不是標籤來存取圖形。

字首標籤策略

如果效能是首要考量，強烈建議您考慮屬性策略的字首標籤策略。

在字首標籤策略中，您可以使用租戶識別符和節點標籤的組合來標記每個節點。例如，如果租用戶的識別符為 "1"且節點標籤為 "Label1"，您可以將節點標籤指定為 "1-Label1"。下圖顯示使用此模型的兩個中斷連線子圖。



在 Gremlin 中寫入資料時，您可以將識別號碼新增至任何節點的標籤：

```
g.addV("1-Label1")
g.addV("2-Label6")
```

查詢此圖形時，您可以檢查節點上是否存在此字首：

```
g.V().hasLabel("1-Label1")
```

在 openCypher 中，您可以使用CREATE陳述式寫入資料：

```
CREATE (n:`1-Label1` {`~id`: 'Item_1', Value: 'XYZ123456'})
```

若要查詢您在 openCypher 中撰寫的資料，請使用下列程式碼：

```
MATCH n= (:`1-Label1`)
RETURN n
```

字首標籤策略假設所有節點都指派給一或多個租用戶，並且未在邊緣範圍內指派許可。避免在邊緣標籤上使用此策略，因為這將導致大量述詞，並對 Neptune 效能產生負面影響。

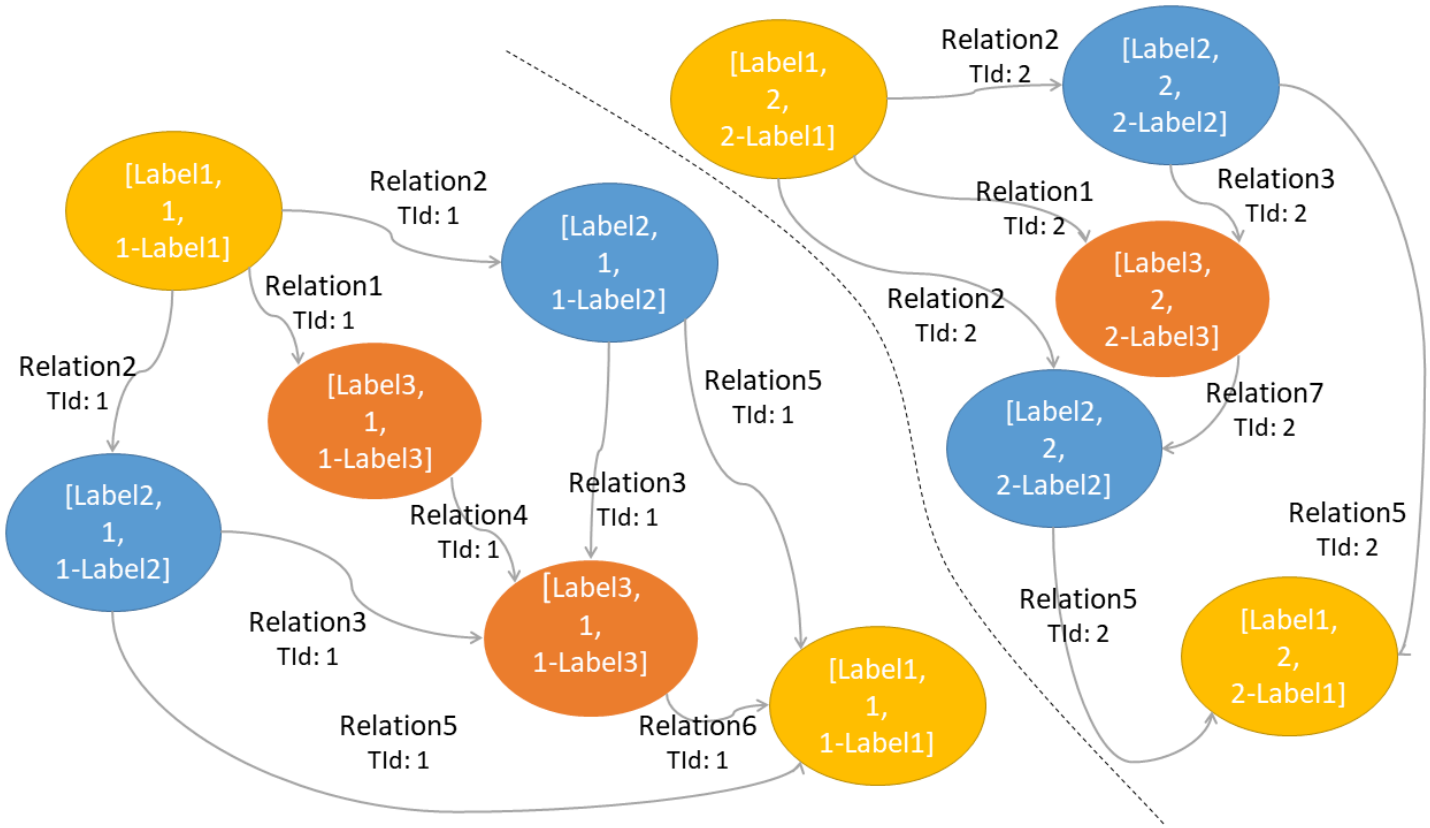
字首標籤方法有兩個主要缺點。首先，執行跨租用戶的任何查詢並不容易。例如，查詢會計算指定標籤的所有節點，以進行報告或監控。如果這是您的使用案例，請考慮將此策略與多標籤策略結合。如需結合策略的詳細資訊，請參閱混合模型一節。

其次，字首標籤策略需要控制，強制對每個查詢適當套用適當的字首，以防止資料外洩。不過，對於需要低延遲查詢的工作負載而言，此策略是最有效率的選項，我們強烈建議您這麼做。LPG 模型的效能影響區段提供為什麼這是最有效策略的範例。

多標籤策略

第三個選項是使用多標籤策略。對於此方法，您可以將額外的標籤新增至圖形上的每個節點。例如，如果您需要篩選指定租用戶的所有資料，請新增租用戶 ID 標籤。如果您需要篩選指定標籤的所有資料，無論租用戶為何，請新增該標籤。下圖顯示針對每個節點使用三個標籤所套用的多標籤策略。

您現在可以使用三種不同的模式來存取圖形：



- 篩選 `Label1`以傳回所有租用戶`Label1`中具有 的所有節點。
- 篩選 `1`以傳回租戶 1 的所有節點。
- 篩選 `1-Label1` 以僅傳回具有標籤 的租用戶 1 的所有節點`Label1`。

對於 LPGs，有兩種方式可以實作此項目。

在 Gremlin 中，您可以使用名為 SubgraphStrategy 的周遊策略，將所有查詢的範圍限制為僅具有特定標籤的頂點，例如 `"Label1"`：

```
g.withStrategies(
    new SubgraphStrategy(
        vertices=hasLabel("Label1")
    )
)
```

與 PartitionStrategy 不同，SubgraphStrategy 只會影響讀取資料，不會影響寫入資料。若要寫入資料，請在每個查詢中手動指派標籤：

```
g.addV("Label1").property("Value","XYZ123456")
.addV("Label2").property("Value","XYZ123456")
```

讀取資料時，您可以使用 SubgraphStrategy 透過 查詢所有節點`"Label1"`：

```
g.withStrategies(
new SubgraphStrategy(vertices=.hasLabel("Label1"))
).
V().has("Value","XYZ123456")
```

Neptune 只會傳回第一個記錄，其具有 `"Label1"`和 的值`"XYZ123456"`。它相當於下列查詢，不使用 SubgraphStrategy：

```
g.V().hasLabel("Label1").hasValue("XYZ123456")
```

在此基本查詢中，SubgraphStrategy 使用起來更為複雜。請記住，您的程式庫可以提供已定義策略g的執行個體。開發人員不必確保套用適當的篩選條件：

```
def getGraphTraversal():
return g.withStrategies(new SubgraphStrategy(vertices=.hasLabel("Label1"))

getGraphTraversal().has("Value","XYZ123456")
```

openCypher 程式庫沒有這些建構，因此您必須為每個節點建立多個標籤：

```
CREATE (n:`1`:`Label1`:`1-Label1` {`~id`: 'Item_1', Value: '12345'})
```

當您使用這些標籤篩選子圖時，您可以傳回具有您要尋找之客戶標籤的節點，或與具有該標籤的其他節點共用關係的節點：

```
MATCH n=(:Label1:`1`)
// or
MATCH n=(:`1-Label1`)
```

多標籤策略可讓您根據類型 (`Label1`) 或租用戶 (1) 來查詢節點，或在效能最為重要時，使用更有效率的字首標籤策略 ()`1-Label1`。

此策略的主要缺點是每個標籤都是存放在圖形中的額外物件。物件是 LPGs 中節點或邊緣上的節點、邊緣或屬性。擷取速度由每秒物件測量和限制，儲存成本取決於消耗的 GB 數。這表示額外的物件可能會產生大規模的可測量影響。

LPG 模型的效能影響

Amazon Neptune 的 AWS 技能建置器課程資料建模詳細說明 Neptune 資料模型內部和建模影響，但我們將在此摘要說明這些設計的重要考量。 Amazon Neptune 考慮在單一 Neptune 叢集上擁有三個租用戶 (T1、T2, T3)。這些租用戶具有下列屬性：

- 租戶 1 (T1) 總共有 1 億個節點，1000 萬個是類型項目。
- 租戶 2 (T2) 共有 1，000 萬個節點，100 萬個是類型項目。
- 租戶 3 (T3) 總共有 1 億個節點，100 萬個是類型項目。

執行查詢，該查詢將使用 屬性策略擷取租用戶 3 的項目。Neptune 會檢查兩個索引呼叫的統計資料：

- 其中 `tenant property key=T3`有 1 億個結果
- 其中 `label = Item`有 1，200 萬筆結果 (1，000 萬筆來自 T1 + 100 萬筆來自 T2 + 100 萬筆來自 T3)

Neptune 查詢最佳化工具會判斷後者查詢最適合先套用 (1，200 萬個結果），然後檢查每個項目是否有 `tenant property key=T3`。您可以擷取 1，200 萬個項目來尋找 100 萬個結果。

請注意此查詢的雜訊鄰居影響。如果您每個租用戶有 1 億個項目節點，第一個查詢會有 3 億個結果，而不是 1，200 萬個 （為了說明起見，這過於簡化。 Neptune 最佳化工具可能已套用不同的操作順序）。

接著，請考慮字首標籤策略。進行單一索引呼叫`label=T3-Item`，其中 會傳回 100 萬個結果。這可實現與 屬性策略相同的結果，但擷取的記錄減少 1，100 萬筆。此外，您不再有吵雜的鄰里問題，因為標籤不會在索引中重疊。

多標籤策略不會直接提供對屬性策略的查詢效能改善。當搜尋空間也相當時，依屬性值篩選會與依標籤值篩選相當。反之，多標籤策略支援更多彈性。 多標籤策略提供的效能等同於 `label=T3`或標籤 的前綴標籤策略`T3-Item`。多標籤策略提供的效能相當於 的屬性策略`label=Item`。好處是支援各種存取模式。

RDF 集區模型

資源描述架構 (RDF) 具有具名圖形的概念，可提供分隔資料的邏輯方式。在 Amazon Neptune 中，您有預設的命名圖形和使用者定義的命名圖形。您可以建立任意數量的具名圖形。統稱為 RDF 資料集。預設或使用者定義的所有具名圖形都是由 RDF 資料集內的國際化資源識別符 (IRI) 定義。在 Neptune 中，除非使用者在寫入資料時宣告具名圖形，否則所有三元組都會視為預設具名圖形的一部分。

具名圖形有多個使用案例：

- 資料分割和資料隔離
- 資料來源
- 版本控制
- Inference

本指南著重於資料分割使用案例。我們建議為每個租用戶建立一個使用者定義的具名圖形。

使用圖形存放區 HTTP 通訊協定的 SPARQL 查詢選項

下列範例查詢使用 SPARQL 通訊協定和 RDF 查詢語言 (SPARQL) 和圖形存放區 HTTP 通訊協定來查詢或建立租用戶的具名圖形。

- `HTTP GET` – 若要擷取租戶的特定圖形：

```
curl --request GET 'https://your-neptune-endpoint:port/sparql/gsp/?graph=http%3A//
www.example.com/named/tenant1'
```

- `HTTP PUT` – 若要使用請求中指定的承載建立或取代特定具名圖形：

```
curl --request PUT -H "Content-Type: text/turtle" \  --data-raw "@prefix ex: http://
example.com/ . ex:subject ex:predicate ex:object ." \
```

```
'https://your-neptune-endpoint:port/sparql/gsp/?graph=http%3A//www.example.com/named/
tenant1'
```

在 RDF 中，物件是三元組。

- HTTP POST – 若要在圖形不存在時建立新的具名圖形，或與現有圖形合併：

```
curl --request POST -H "Content-Type: text/turtle" \
--data-raw "@prefix ex: http://example.com/ . ex:subject ex:predicate ex:object ." \

'https://your-neptune-endpoint:port/sparql/gsp/?graph=http%3A//www.example.com/named/
tenant1'
```

RDF 的租用戶隔離

若要在應用程式層使用必要的護欄對資料進行邏輯隔離，請在租用戶和使用者定義的具名圖形之間建立映射。當您為 RDF 資料集設計多租戶時，請注意 RDF 和 SPARQL 的下列層面：

- 在 Neptune 中，當您在不指定具名圖形的情況下進行查詢時，它會擷取資料庫中所有具名圖形中符合模式的所有三元組。
- 在 RDF 中，不同具名圖形節點之間的連線沒有限制。例如，在上圖中， 中的節點:G1可以透過 邊緣連接到 G2中的節點。

例如，如果特定租用戶的最終使用者提交查詢至 API，API 應先驗證下列要求，再將查詢提交至 Neptune 資料庫：

- 任何範圍在單一租用戶的查詢都必須指定具名圖形。否則，您會有跨租用戶洩漏資料的風險。
- 更新或刪除查詢應一律指定具名圖形。
- 邊緣或關係任一端的節點應一律屬於正確的具名圖形。

如需最佳實務的詳細資訊，請參閱 Neptune 文件。

準備成長

當您成功使用集區模型時，您最終會超出單一 Neptune 叢集的大小。租用戶增加，或租用戶數量增加，而且所有客戶所需的資料擷取率都超過叢集的功能。發生這種情況時，您需要將客戶分割到多個叢

集。預先為此組態進行設計，而不是稍後嘗試進行修改。即使您的初始擴展只使用單一叢集， 仍會模擬您未來達到該擴展時，將租用戶路由到多個叢集所需的元件。

如果您的解決方案根據您的租戶大小需要更多資源，也請準備其成長。如果單一叢集上的數個客戶大幅成長，該叢集可能不再支援您的需求。設計策略，使用 Amazon Neptune 資料庫複製功能將租戶移至另一個叢集，或將現有叢集分割為兩個叢集。

熟悉 Neptune Copy-on-Write通訊協定，這可在您實作資料庫複製時節省成本。如果您因為擷取瓶頸而分割叢集，則不從叢集刪除資料可能會更有效率，前提是您的政策允許這麼做。如果資料頁面未變更，則兩個叢集會共用資料頁面，但如果資料頁面遭到修改則不會共用（因為其中有些資料遭到刪除）。

> **Note**
>
> 本指南適用於撰寫本文時的最新 Neptune 版本，即 Neptune 1.3.1 版。隨著 Neptune 儲存層的演進，本指南可能會在未來版本中變更。

多租用戶案例的限制

請注意，某些 Neptune 功能並非針對多租用戶案例而建置。租用戶不應直接存取集區模型中的 Neptune 端點，因為這些多租用戶策略不會在資料庫層級強制執行。一律在客戶與 Neptune 端點之間保留某種代理，以強制執行本文件中所述的設計。這類代理的範例包括下列項目：

- 在用戶端層中附加標籤篩選條件
- 擁有將身分驗證字符映射至租戶 ID 並將此篩選條件插入查詢的 API

本指南也適用於讓客戶直接存取 Neptune 圖形筆記本、Neptune 圖形探索程式或 Neptune 串流等功能。

混合模型多租戶

SaaS 解決方案通常會使用孤島和集區模型的混合。各種因素會影響何時以及如何在相同環境中使用孤立系統和集區模型的決定。

其中一個因素是分層，其中 SaaS 解決方案為每個租戶層提供獨特的體驗。例如，如果您的層是免費、標準和高級，您的免費層租用戶資料可能會使用集區模型儲存在共用的 Neptune 叢集中。對於 Standard 和 Premium 層租用戶，您可以使用 cluster-per-tenant 孤島模型。

此外，某些 SaaS 供應商也可以在共用的 Amazon Neptune 叢集上建置其集區解決方案，作為其基礎。隨後，他們可以為需要孤立儲存的租戶建立單獨的 Neptune 叢集，通常是因為合規和監管要求。

雖然這可能會為您的資料存取層和管理設定檔增加複雜程度，但它也可以為您的企業提供一種方法來將產品分層以滿足客戶要求。

的操作最佳實務 ISVs

本節中的許多指導方針是所有客戶的最佳實務，但它們已為 增加了重要性ISVs。

使用最新版本更新您的 Neptune 叢集

在 Amazon Neptune 版本備註 中，您可以看到每個版本都具有許多錯誤修正、效能改善和新功能。盡可能將 Neptune 叢集保持在最新版本上。

如果您在工作負載中發現先前未發現的錯誤，且叢集位於最新版本，Neptune 工程師可以為您的叢集建立私有修補程式（如果有必要且您想要）。修補程式可以橋接，直到該修正一般可用時的下一個版本為止。若要協助將叢集更新至最新版本，請使用 Neptune Blue/Green 解決方案 。

使用 deltas 而不是刪除和取代資料擷取

您可以使用數種技術，將資料擷取或寫入 Neptune。許多客戶會嘗試在每次在饋送中收到變更時刪除並重新插入其圖形，以簡化其資料擷取。他們可能會將`last-modified`屬性新增至每個節點，並定期掃描自某些指定日期以來尚未修改的節點，然後刪除它們。雖然這些技術簡化了資料擷取程序，但它們對您的 Neptune 叢集具有長期運作狀態和可擴展性影響。

首先，Neptune 使用字串的字典編碼。除非您明確指定節點和邊緣IDs的 ，否則 Neptune 會為 ID 產生表示GUID字串，並將該字串儲存在字典中。如果您不斷刪除和新增物件，則自動產生的 IDs會在字典中產生 bloat。

其次，Neptune 會擴展至每秒最大擷取約 120 K 物件。如果您持續刪除並新增物件，則會在實質上未變更的物件上消耗大量頻寬。這限制了您可以在叢集上託管的租戶數量、需要叢集中較大的寫入器執行個體，以及需要更多 I/O 操作。所有這些因素都會增加您的成本。

強烈建議您開發一種方法來計算已變更的真實差異，而不是使用刪除和新增方法。不過，某些資料來源不有利於此（例如，傳回目前狀態的API呼叫，或是未確切追蹤變更的事件）。如果您的原始資料來源不有利於識別變更，請使用擷取、轉換和載入（ETL）程序來計算差異。例如，您可以 Parquet 格式維護每個先前資料擷取的快照，使用 AWS Glue 計算這些快照之間的差異，並僅將差異推送至 Neptune。

示範 Neptune 成本如何隨著租戶而演變

無論您是使用孤立系統、集區或混合模型，您的雲端成本都會隨著租戶的大小而擴展。需要更多並行連線的租用戶比較少並行連線的租用戶需要更大的執行個體或更多的僅供讀取複本。這同樣適用於需要更快速擷取資料的租戶。

Neptune 叢集成本的三個元件是執行個體大小（和數量）、資料大小（GB 個月）和 I/O 操作（每百萬）。雖然這些成本通常是工作負載特定的，但它們會隨著大小和資料量而擴展，但可以使用 AWS 工具來測量。根據租戶規模的關鍵指標追蹤和了解規模經濟，包括其規模隨著時間的變化。如果 I/O 費用的不可預測性影響您的利潤，請考慮選擇 Neptune I/O 最佳化儲存，以獲得更可預測的成本。

根據客戶需求擴展叢集

Neptune 執行個體大小大小適中沒有已試過或真實的公式。Neptune 文件提供指引，但有太多變數建議直接映射。這些變數包括但不限於下列項目：

- 資料模型
- 資料形狀
- 查詢並行
- 查詢複雜性。

規劃測試，以判斷工作負載和租戶設定檔的最佳大小。一般而言，我們建議您使用佈建的執行個體來提高成本效益和可預測性。如果您的客戶體驗目標優先考慮成本的最佳擴展，請考慮使用 Neptune Serverless 執行個體，以確保無論工作負載波動如何，都能有更一致的體驗。

如果您的租戶讀取工作負載的峰值和低谷有顯著差異，請將 Neptune Serverless 執行個體與 Neptune 自動擴展 結合。 新的僅供讀取複本初始化後通常需要 10-15 分鐘才能上線。這表示，僅自動擴展可以處理流量長時間變更，但不足以快速變更活動的尖峰。透過結合 Neptune Serverless 和 Neptune 自動擴展，您可以向上或向下擴展執行個體，並向外擴展僅供讀取複本的數量。

如果您的租戶具有顯著不同的工作負載描述檔或服務層級協議（SLAs），請考慮使用自訂端點和專用僅供讀取複本，將流量引導至針對該流量最佳化的執行個體。最佳化可以包括執行個體的不同大小、特定查詢模式，或預先暖機緩衝快取。

後續步驟

如果您剛開始為多租用戶ISV應用程式實作 Amazon Neptune 的旅程，請將額外的考量納入您想要的模型。變更模型之後在旅程中會更昂貴。

如果您在旅程中提早，請確認您使用符合您需求的最佳模型，以及遵循該模型的指引。

請事先計畫。當您在旅程的早期時，很誘人地會延遲跨叢集共用客戶或最佳化ETL程序的工作，以提供變更的差異，而不是刪除和重新新增頂點和邊緣。當您擴展時，這些決策可能會對效能和成本產生負面影響。

最後，如果您已順利完成旅程，本指南可能會向您保證您的架構是最佳的，或者它可能會提供變更來改善您的架構。

如果您對本指南有疑問或需要進一步協助，請聯絡您的 AWS 帳戶 團隊，並要求與 Neptune 專家進行工作階段。

資源

- Amazon Neptune 文件
- Amazon Neptune 的資料建模（課程）
- 套用 AWS Well-Architected Framework for Amazon Neptune
- SaaS Lens Well-Architected 架構
- 上的多租戶架構指南 AWS
- SaaS 租戶隔離策略：在多租戶環境中隔離資源
- Apache TinkerPop 文件
- SPARQL

貢獻者

本指南的貢獻者包括：

- Brian O'Keefe，校長 WW SSA Neptune， AWS
- Veeresham Gande，資深技術客戶經理， AWS
- Dana Owens，啟動解決方案架構師， AWS
- Nima Seifi，啟動解決方案架構師， AWS

文件歷史記錄

下表描述了本指南的重大變更。如果您想要收到未來更新的通知，您可以訂閱RSS摘要 。

變更	描述	日期
初次出版	—	2024 年 9 月 3 日

AWS 規範性指引詞彙表

以下是 AWS Prescriptive Guidance 提供的策略、指南和模式中常用的術語。若要建議項目，請使用詞彙表末尾的提供意見回饋連結。

數字

7 R

將應用程式移至雲端的七種常見遷移策略。這些策略以 Gartner 在 2011 年確定的 5 R 為基礎，包括以下內容：

- 重構/重新架構 – 充分利用雲端原生功能來移動應用程式並修改其架構，以提高敏捷性、效能和可擴展性。這通常涉及移植作業系統和資料庫。範例：將您的現場部署 Oracle 資料庫遷移至 Amazon Aurora PostgreSQL 相容版本。
- 平台轉換 (隨即重塑) – 將應用程式移至雲端，並引入一定程度的優化以利用雲端功能。範例：將您的現場部署 Oracle 資料庫遷移至 中的 Amazon Relational Database Service (Amazon RDS) for Oracle AWS 雲端。
- 重新購買 (捨棄再購買) – 切換至不同的產品，通常從傳統授權移至 SaaS 模型。範例：將您的客戶關係管理 (CRM) 系統遷移至 Salesforce.com。
- 主機轉換 (隨即轉移) – 將應用程式移至雲端，而不進行任何變更以利用雲端功能。範例：將您的現場部署 Oracle 資料庫遷移至 中 EC2 執行個體上的 Oracle AWS 雲端。
- 重新放置 (虛擬機器監視器等級隨即轉移) – 將基礎設施移至雲端，無需購買新硬體、重寫應用程式或修改現有操作。您可以將伺服器從內部部署平台遷移到相同平台的雲端服務。範例：將 Microsoft Hyper-V應用程式遷移至 AWS。
- 保留 (重新檢視) – 將應用程式保留在來源環境中。其中可能包括需要重要重構的應用程式，且您希望將該工作延遲到以後，以及您想要保留的舊版應用程式，因為沒有業務理由來進行遷移。
- 淘汰 – 解除委任或移除來源環境中不再需要的應用程式。

A

ABAC

請參閱屬性型存取控制。

抽象服務

請參閱 受管服務。

ACID

請參閱原子性、一致性、隔離性、耐久性。

主動-主動式遷移

一種資料庫遷移方法，其中來源和目標資料庫保持同步 (透過使用雙向複寫工具或雙重寫入操作)，且兩個資料庫都在遷移期間處理來自連接應用程式的交易。此方法支援小型、受控制批次的遷移，而不需要一次性切換。它更靈活，但比主動-被動遷移需要更多的工作。

主動-被動式遷移

一種資料庫遷移方法，其中來源和目標資料庫保持同步，但只有來源資料庫處理來自連接應用程式的交易，同時將資料複寫至目標資料庫。目標資料庫在遷移期間不接受任何交易。

彙總函數

在一組資料列上運作的 SQL 函數，會計算群組的單一傳回值。彙總函數的範例包括 SUM和 MAX。

AI

請參閱人工智慧。

AIOps

請參閱人工智慧操作。

匿名化

在資料集中永久刪除個人資訊的程序。匿名化有助於保護個人隱私權。匿名資料不再被視為個人資料。

反模式

經常用於重複性問題的解決方案，其中解決方案具有反生產力、無效或比替代解決方案更有效。

應用程式控制

一種安全方法，僅允許使用核准的應用程式，以協助保護系統免受惡意軟體攻擊。

應用程式組合

有關組織使用的每個應用程式的詳細資訊的集合，包括建置和維護應用程式的成本及其商業價值。此資訊是產品組合探索和分析程序的關鍵，有助於識別要遷移、現代化和優化的應用程式並排定其優先順序。

人工智慧 (AI)

電腦科學領域，致力於使用運算技術來執行通常與人類相關的認知功能，例如學習、解決問題和識別模式。如需詳細資訊，請參閱什麼是人工智慧？

人工智慧操作 (AIOps)

使用機器學習技術解決操作問題、減少操作事件和人工干預以及提高服務品質的程序。如需有關如何在 AWS 遷移策略中使用 AIOps 的詳細資訊，請參閱操作整合指南。

非對稱加密

一種加密演算法，它使用一對金鑰：一個用於加密的公有金鑰和一個用於解密的私有金鑰。您可以共用公有金鑰，因為它不用於解密，但對私有金鑰存取應受到高度限制。

原子性、一致性、隔離性、耐久性 (ACID)

一組軟體屬性，即使在出現錯誤、電源故障或其他問題的情況下，也能確保資料庫的資料有效性和操作可靠性。

屬性型存取控制 (ABAC)

根據使用者屬性 (例如部門、工作職責和團隊名稱) 建立精細許可的實務。如需詳細資訊，請參閱《 AWS Identity and Access Management (IAM) 文件》中的 ABAC for AWS。

授權資料來源

您存放主要版本資料的位置，被視為最可靠的資訊來源。您可以將授權資料來源中的資料複製到其他位置，以處理或修改資料，例如匿名、修訂或假名化資料。

可用區域

中的不同位置 AWS 區域 ，可隔離其他可用區域中的故障，並提供相同區域中其他可用區域的低成本、低延遲網路連線。

AWS 雲端採用架構 (AWS CAF)

的指導方針和最佳實務架構 AWS ，可協助組織制定高效且有效的計劃，以成功地移至雲端。 AWS CAF 將指導方針組織到六個重點領域：業務、人員、治理、平台、安全和營運。業務、人員和控管層面著重於業務技能和程序；平台、安全和操作層面著重於技術技能和程序。例如，人員層面針對處理人力資源 (HR)、人員配備功能和人員管理的利害關係人。因此， AWS CAF 為人員開發、訓練和通訊提供指引，協助組織做好成功採用雲端的準備。如需詳細資訊，請參閱 AWS CAF 網站和 AWS CAF 白皮書。

AWS 工作負載資格架構 (AWS WQF)

一種工具，可評估資料庫遷移工作負載、建議遷移策略，並提供工作預估值。 AWS WQF 隨附於 AWS Schema Conversion Tool (AWS SCT)。它會分析資料庫結構描述和程式碼物件、應用程式程式碼、相依性和效能特性，並提供評估報告。

B

錯誤的機器人

旨在中斷或傷害個人或組織的機器人。

BCP

請參閱業務持續性規劃。

行為圖

資源行為的統一互動式檢視，以及一段時間後的互動。您可以將行為圖與 Amazon Detective 搭配使用來檢查失敗的登入嘗試、可疑的 API 呼叫和類似動作。如需詳細資訊，請參閱偵測文件中的行為圖中的資料。

大端序系統

首先儲存最高有效位元組的系統。另請參閱 Endianness。

二進制分類

預測二進制結果的過程 (兩個可能的類別之一)。例如，ML 模型可能需要預測諸如「此電子郵件是否是垃圾郵件？」等問題 或「產品是書還是汽車？」

Bloom 篩選條件

一種機率性、記憶體高效的資料結構，用於測試元素是否為集的成員。

藍/綠部署

一種部署策略，您可以在其中建立兩個不同但相同的環境。您可以在一個環境 （藍色） 中執行目前的應用程式版本，並在另一個環境 （綠色） 中執行新的應用程式版本。此策略可協助您快速復原，並將影響降至最低。

機器人

透過網際網路執行自動化任務並模擬人類活動或互動的軟體應用程式。有些機器人有用或有益，例如在網際網路上為資訊編製索引的 Web 爬蟲程式。有些其他機器人稱為惡意機器人，旨在中斷或傷害個人或組織。

殭屍網路

受到惡意軟體感染且受單一方控制之機器人的網路，稱為機器人繼承器或機器人運算子。殭屍網路是擴展機器人及其影響的最佳已知機制。

分支

程式碼儲存庫包含的區域。儲存庫中建立的第一個分支是主要分支。您可以從現有分支建立新分支，然後在新分支中開發功能或修正錯誤。您建立用來建立功能的分支通常稱為功能分支。當準備好發佈功能時，可以將功能分支合併回主要分支。如需詳細資訊，請參閱關於分支 (GitHub 文件)。

碎片存取

在特殊情況下，以及透過核准的程序，讓使用者能夠快速存取他們通常無權存取 AWS 帳戶 的 。如需詳細資訊，請參閱 Well-Architected 指南中的 AWS 實作打破玻璃程序指標。

棕地策略

環境中的現有基礎設施。對系統架構採用棕地策略時，可以根據目前系統和基礎設施的限制來設計架構。如果正在擴展現有基礎設施，則可能會混合棕地和綠地策略。

緩衝快取

儲存最常存取資料的記憶體區域。

業務能力

業務如何創造價值 (例如，銷售、客戶服務或營銷)。業務能力可驅動微服務架構和開發決策。如需詳細資訊，請參閱在 AWS上執行容器化微服務白皮書的圍繞業務能力進行組織部分。

業務連續性規劃 (BCP)

一種解決破壞性事件 (如大規模遷移) 對營運的潛在影響並使業務能夠快速恢復營運的計畫。

C

CAF

請參閱AWS 雲端採用架構。

Canary 部署

版本對最終使用者的緩慢和增量版本。當您有信心時，您可以部署新版本並完全取代目前的版本。

CCoE

請參閱 Cloud Center of Excellence。

CDC

請參閱變更資料擷取。

變更資料擷取 (CDC)

追蹤對資料來源 (例如資料庫表格) 的變更並記錄有關變更的中繼資料的程序。您可以將 CDC 用於各種用途，例如稽核或複寫目標系統中的變更以保持同步。

混沌工程

故意引入故障或破壞性事件，以測試系統的彈性。您可以使用 AWS Fault Injection Service (AWS FIS) 執行實驗，為您的 AWS 工作負載帶來壓力，並評估其回應。

CI/CD

請參閱持續整合和持續交付。

分類

有助於產生預測的分類程序。用於分類問題的 ML 模型可預測離散值。離散值永遠彼此不同。例如，模型可能需要評估影像中是否有汽車。

用戶端加密

在目標 AWS 服務 接收資料之前，在本機加密資料。

雲端卓越中心 (CCoE)

一個多學科團隊，可推動整個組織的雲端採用工作，包括開發雲端最佳實務、調動資源、制定遷移時間表以及領導組織進行大規模轉型。如需詳細資訊，請參閱 AWS 雲端 企業策略部落格上的 CCoE 文章。

雲端運算

通常用於遠端資料儲存和 IoT 裝置管理的雲端技術。雲端運算通常連接到邊緣運算技術。

雲端操作模型

在 IT 組織中，用於建置、成熟和最佳化一或多個雲端環境的操作模型。如需詳細資訊，請參閱建置您的雲端操作模型。

採用雲端階段

組織在遷移至 時通常會經歷的四個階段 AWS 雲端：

- 專案 – 執行一些與雲端相關的專案以進行概念驗證和學習用途
- 基礎 – 進行基礎投資以擴展雲端採用 (例如，建立登陸區域、定義 CCoE、建立營運模型)

- 遷移 – 遷移個別應用程式
- 重塑 – 優化產品和服務，並在雲端中創新

這些階段由 Stephen Orban 於部落格文章 The Journey Toward Cloud-First 和 Enterprise Strategy 部落格上的採用階段中定義。 AWS 雲端 如需有關它們如何與 AWS 遷移策略相關的詳細資訊，請參閱遷移整備指南。

CMDB

請參閱組態管理資料庫。

程式碼儲存庫

透過版本控制程序來儲存及更新原始程式碼和其他資產 (例如文件、範例和指令碼) 的位置。常見的雲端儲存庫包括 GitHub或 Bitbucket Cloud。程式碼的每個版本都稱為分支。在微服務結構中，每個儲存庫都專用於單個功能。單一 CI/CD 管道可以使用多個儲存庫。

冷快取

一種緩衝快取，它是空的、未填充的，或者包含過時或不相關的資料。這會影響效能，因為資料庫執行個體必須從主記憶體或磁碟讀取，這比從緩衝快取讀取更慢。

冷資料

很少存取且通常是歷史資料的資料。查詢這類資料時，通常可接受慢查詢。將此資料移至效能較低且成本較低的儲存層或類別，可以降低成本。

電腦視覺 (CV)

使用機器學習從數位影像和影片等視覺化格式分析和擷取資訊的 AI 欄位。例如，Amazon SageMaker AI 提供 CV 的影像處理演算法。

組態偏離

對於工作負載，組態會從預期狀態變更。這可能會導致工作負載變得不合規，而且通常是漸進和無意的。

組態管理資料庫 (CMDB)

儲存和管理有關資料庫及其 IT 環境的資訊的儲存庫，同時包括硬體和軟體元件及其組態。您通常在遷移的產品組合探索和分析階段使用 CMDB 中的資料。

一致性套件

您可以組合的 AWS Config 規則和修補動作集合，以自訂您的合規和安全檢查。您可以使用 YAML 範本，將一致性套件部署為 AWS 帳戶 和 區域中或整個組織的單一實體。如需詳細資訊，請參閱 AWS Config 文件中的一致性套件。

持續整合和持續交付 (CI/CD)

自動化軟體發行程序的來源、建置、測試、暫存和生產階段的程序。CI/CD 通常被描述為管道。CI/CD 可協助您將程序自動化、提升生產力、改善程式碼品質以及加快交付速度。如需詳細資訊，請參閱持續交付的優點。CD 也可表示持續部署。如需詳細資訊，請參閱持續交付與持續部署。

CV

請參閱電腦視覺。

D

靜態資料

網路中靜止的資料，例如儲存中的資料。

資料分類

根據重要性和敏感性來識別和分類網路資料的程序。它是所有網路安全風險管理策略的關鍵組成部分，因為它可以協助您確定適當的資料保護和保留控制。資料分類是 AWS Well-Architected Framework 中安全支柱的元件。如需詳細資訊，請參閱資料分類。

資料偏離

生產資料與用於訓練 ML 模型的資料之間有意義的變化，或輸入資料隨時間有意義的變更。資料偏離可以降低 ML 模型預測的整體品質、準確性和公平性。

傳輸中的資料

在您的網路中主動移動的資料，例如在網路資源之間移動。

資料網格

架構架構，提供分散式、分散式資料擁有權與集中式管理。

資料最小化

僅收集和處理嚴格必要資料的原則。在 中實作資料最小化 AWS 雲端 可以降低隱私權風險、成本和分析碳足跡。

資料周邊

AWS 環境中的一組預防性防護機制，可協助確保只有信任的身分才能從預期的網路存取信任的資源。如需詳細資訊，請參閱在 上建置資料周邊 AWS。

資料預先處理

將原始資料轉換成 ML 模型可輕鬆剖析的格式。預處理資料可能意味著移除某些欄或列，並解決遺失、不一致或重複的值。

資料來源

在整個生命週期中追蹤資料的原始伺服器和歷史記錄的程序，例如資料的產生、傳輸和儲存方式。

資料主體

正在收集和處理其資料的個人。

資料倉儲

支援商業智慧的資料管理系統，例如 分析。資料倉儲通常包含大量歷史資料，通常用於查詢和分析。

資料庫定義語言 (DDL)

用於建立或修改資料庫中資料表和物件之結構的陳述式或命令。

資料庫處理語言 (DML)

用於修改 (插入、更新和刪除) 資料庫中資訊的陳述式或命令。

DDL

請參閱資料庫定義語言。

深度整體

結合多個深度學習模型進行預測。可以使用深度整體來獲得更準確的預測或估計預測中的不確定性。

深度學習

一個機器學習子領域，它使用多層人工神經網路來識別感興趣的輸入資料與目標變數之間的對應關係。

深度防禦

這是一種資訊安全方法，其中一系列的安全機制和控制項會在整個電腦網路中精心分層，以保護網路和其中資料的機密性、完整性和可用性。當您在 上採用此策略時 AWS，您可以在 AWS Organizations 結構的不同層新增多個控制項，以協助保護資源。例如，defense-in-depth方法可能會結合多重要素驗證、網路分割和加密。

委派的管理員

在 中 AWS Organizations，相容的服務可以註冊 AWS 成員帳戶，以管理組織的帳戶和管理該服務的許可。此帳戶稱為該服務的委派管理員。如需詳細資訊和相容服務清單，請參閱 AWS Organizations 文件中的可搭配 AWS Organizations運作的服務。

部署

在目標環境中提供應用程式、新功能或程式碼修正的程序。部署涉及在程式碼庫中實作變更，然後在應用程式環境中建置和執行該程式碼庫。

開發環境

請參閱 環境。

偵測性控制

一種安全控制，用於在事件發生後偵測、記錄和提醒。這些控制是第二道防線，提醒您注意繞過現有預防性控制的安全事件。如需詳細資訊，請參閱在 AWS上實作安全控制中的偵測性控制。

開發值串流映射 (DVSM)

一種程序，用於識別對軟體開發生命週期中的速度和品質造成負面影響的限制並排定優先順序。DVSM 延伸了原本專為精簡製造實務設計的價值串流映射程序。它著重於透過軟體開發程序建立和移動價值所需的步驟和團隊。

數位分身

真實世界系統的虛擬呈現，例如建築物、工廠、工業設備或生產線。數位分身支援預測性維護、遠端監控和生產最佳化。

維度資料表

在星星結構描述中，較小的資料表包含有關事實資料表中量化資料的資料屬性。維度資料表屬性通常是文字欄位或離散數字，其行為類似於文字。這些屬性通常用於查詢限制、篩選和結果集標記。

災難

防止工作負載或系統在其主要部署位置中實現其業務目標的事件。這些事件可能是自然災難、技術故障或人為動作的結果，例如意外設定錯誤或惡意軟體攻擊。

災難復原 (DR)

您用來將災難造成的停機時間和資料遺失降至最低的策略和程序。如需詳細資訊，請參閱 AWS Well-Architected Framework 中的 上工作負載災難復原 AWS：雲端中的復原。

DML

請參閱資料庫處理語言。

領域驅動的設計

一種開發複雜軟體系統的方法，它會將其元件與每個元件所服務的不斷發展的領域或核心業務目標相關聯。Eric Evans 在其著作 Domain-Driven Design: Tackling Complexity in the Heart of Software (Boston: Addison-Wesley Professional, 2003) 中介紹了這一概念。如需有關如何將領域驅動的設計與 strangler fig 模式搭配使用的資訊，請參閱使用容器和 Amazon API Gateway 逐步現代化舊版 Microsoft ASP.NET (ASMX) Web 服務。

DR

請參閱災難復原。

偏離偵測

追蹤與基準組態的偏差。例如，您可以使用 AWS CloudFormation 來偵測系統資源中的偏離，也可以使用 AWS Control Tower 來偵測登陸區域中可能影響控管要求合規性的變更。 https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/using-cfn-stack-drift.html

DVSM

請參閱開發值串流映射。

E

EDA

請參閱探索性資料分析。

EDI

請參閱電子資料交換。

邊緣運算

提升 IoT 網路邊緣智慧型裝置運算能力的技術。與雲端運算相比，邊緣運算可以減少通訊延遲並改善回應時間。

電子資料交換 (EDI)

在組織之間自動交換商業文件。如需詳細資訊，請參閱什麼是電子資料交換。

加密

一種運算程序，可將人類可讀取的純文字資料轉換為加密文字。

加密金鑰

由加密演算法產生的隨機位元的加密字串。金鑰長度可能有所不同，每個金鑰的設計都是不可預測且唯一的。

端序

位元組在電腦記憶體中的儲存順序。大端序系統首先儲存最高有效位元組。小端序系統首先儲存最低有效位元組。

端點

請參閱 服務端點。

端點服務

您可以在虛擬私有雲端 (VPC) 中託管以與其他使用者共用的服務。您可以使用 建立端點服務，AWS PrivateLink 並將許可授予其他 AWS 帳戶 或 AWS Identity and Access Management (IAM) 委託人。這些帳戶或主體可以透過建立介面 VPC 端點私下連接至您的端點服務。如需詳細資訊，請參閱 Amazon Virtual Private Cloud (Amazon VPC) 文件中的建立端點服務。

企業資源規劃 (ERP)

一種系統，可自動化和管理企業的關鍵業務流程（例如會計、MES 和專案管理）。

信封加密

使用另一個加密金鑰對某個加密金鑰進行加密的程序。如需詳細資訊，請參閱 AWS Key Management Service (AWS KMS) 文件中的信封加密。

環境

執行中應用程式的執行個體。以下是雲端運算中常見的環境類型：

- 開發環境 – 執行中應用程式的執行個體，只有負責維護應用程式的核心團隊才能使用。開發環境用來測試變更，然後再將開發環境提升到較高的環境。此類型的環境有時稱為測試環境。
- 較低的環境 – 應用程式的所有開發環境，例如用於初始建置和測試的開發環境。
- 生產環境 – 最終使用者可以存取的執行中應用程式的執行個體。在 CI/CD 管道中，生產環境是最後一個部署環境。
- 較高的環境 – 核心開發團隊以外的使用者可存取的所有環境。這可能包括生產環境、生產前環境以及用於使用者接受度測試的環境。

epic

在敏捷方法中，有助於組織工作並排定工作優先順序的功能類別。epic 提供要求和實作任務的高層級描述。例如， AWS CAF 安全概念包括身分和存取管理、偵測控制、基礎設施安全、資料保護和事件回應。如需有關 AWS 遷移策略中的 Epic 的詳細資訊，請參閱計畫實作指南。

ERP

請參閱企業資源規劃。

探索性資料分析 (EDA)

分析資料集以了解其主要特性的過程。您收集或彙總資料，然後執行初步調查以尋找模式、偵測異常並檢查假設。透過計算摘要統計並建立資料可視化來執行 EDA。

F

事實資料表

星狀結構描述中的中央資料表。它存放有關業務操作的量化資料。一般而言，事實資料表包含兩種類型的資料欄：包含度量的資料，以及包含維度資料表外部索引鍵的資料欄。

快速失敗

一種使用頻繁和增量測試來縮短開發生命週期的理念。這是敏捷方法的關鍵部分。

故障隔離界限

在 中 AWS 雲端，像是可用區域 AWS 區域、控制平面或資料平面等邊界會限制故障的影響，並有助於改善工作負載的彈性。如需詳細資訊，請參閱AWS 故障隔離界限。

功能分支

請參閱分支。

特徵

用來進行預測的輸入資料。例如，在製造環境中，特徵可能是定期從製造生產線擷取的影像。

功能重要性

特徵對於模型的預測有多重要。這通常表示為可以透過各種技術來計算的數值得分，例如 Shapley Additive Explanations (SHAP) 和積分梯度。如需詳細資訊，請參閱 的機器學習模型可解譯性 AWS。

特徵轉換

優化 ML 程序的資料，包括使用其他來源豐富資料、調整值、或從單一資料欄位擷取多組資訊。這可讓 ML 模型從資料中受益。例如，如果將「2021-05-27 00:15:37」日期劃分為「2021」、「五月」、「週四」和「15」，則可以協助學習演算法學習與不同資料元件相關聯的細微模式。

少量擷取提示

在要求 LLM 執行類似的任務之前，提供少量示範任務和所需輸出的範例。此技術是內容內學習的應用程式，其中模型會從內嵌在提示中的範例 (快照) 中學習。對於需要特定格式、推理或網域知識的任務，少量的提示非常有效。另請參閱零鏡頭提示。

FGAC

請參閱精細存取控制。

精細存取控制 (FGAC)

使用多個條件來允許或拒絕存取請求。

閃切遷移

一種資料庫遷移方法，透過變更資料擷取使用連續資料複寫，以盡可能在最短的時間內遷移資料，而不是使用分階段方法。目標是將停機時間降至最低。

FM

請參閱基礎模型。

基礎模型 (FM)

大型深度學習神經網路，已針對廣義和未標記資料的大量資料集進行訓練。FMs 能夠執行各種一般任務，例如了解語言、產生文字和影像，以及以自然語言交談。如需詳細資訊，請參閱什麼是基礎模型。

G

生成式 AI

已針對大量資料進行訓練的 AI 模型子集，可使用簡單的文字提示建立新的內容和成品，例如影像、影片、文字和音訊。如需詳細資訊，請參閱什麼是生成式 AI。

地理封鎖

請參閱地理限制。

地理限制 (地理封鎖)

Amazon CloudFront 中的選項，可防止特定國家/地區的使用者存取內容分發。您可以使用允許清單或封鎖清單來指定核准和禁止的國家/地區。如需詳細資訊，請參閱 CloudFront 文件中的限制內容的地理分佈。

Gitflow 工作流程

這是一種方法，其中較低和較高環境在原始碼儲存庫中使用不同分支。Gitflow 工作流程會被視為舊版，而以幹線為基礎的工作流程是現代、偏好的方法。

黃金影像

系統或軟體的快照，做為部署該系統或軟體新執行個體的範本。例如，在製造中，黃金映像可用於在多個裝置上佈建軟體，並有助於提高裝置製造操作的速度、可擴展性和生產力。

綠地策略

新環境中缺乏現有基礎設施。對系統架構採用綠地策略時，可以選擇所有新技術，而不會限制與現有基礎設施的相容性，也稱為棕地。如果正在擴展現有基礎設施，則可能會混合棕地和綠地策略。

防護機制

有助於跨組織單位 (OU) 來管控資源、政策和合規的高層級規則。預防性防護機制會強制執行政策，以確保符合合規標準。透過使用服務控制政策和 IAM 許可界限來將其實作。偵測性防護機制可偵測政策違規和合規問題，並產生提醒以便修正。它們是透過使用 AWS Config AWS Security Hub、Amazon GuardDuty、、Amazon Inspector AWS Trusted Advisor和自訂 AWS Lambda 檢查來實作。

H

HA

請參閱高可用性。

異質資料庫遷移

將來源資料庫遷移至使用不同資料庫引擎的目標資料庫 (例如，Oracle 至 Amazon Aurora)。異質遷移通常是重新架構工作的一部分，而轉換結構描述可能是一項複雜任務。AWS 提供有助於結構描述轉換的 AWS SCT。

高可用性 (HA)

在遇到挑戰或災難時，工作負載能夠在不介入的情況下持續運作。HA 系統的設計目的是自動容錯移轉、持續提供高品質的效能，並處理不同的負載和故障，並將效能影響降至最低。

歷史現代化

一種方法，用於現代化和升級操作技術 (OT) 系統，以更好地滿足製造業的需求。歷史資料是一種資料庫，用於從工廠中的各種來源收集和存放資料。

保留資料

從用於訓練機器學習模型的資料集中保留的部分歷史標記資料。您可以使用保留資料，透過比較模型預測與保留資料來評估模型效能。

異質資料庫遷移

將您的來源資料庫遷移至共用相同資料庫引擎的目標資料庫 (例如，Microsoft SQL Server 至 Amazon RDS for SQL Server)。同質遷移通常是主機轉換或平台轉換工作的一部分。您可以使用原生資料庫公用程式來遷移結構描述。

熱資料

經常存取的資料，例如即時資料或最近的轉譯資料。此資料通常需要高效能儲存層或類別，才能提供快速的查詢回應。

修補程序

緊急修正生產環境中的關鍵問題。由於其緊迫性，通常會在典型 DevOps 發行工作流程之外執行修補程式。

超級護理期間

在切換後，遷移團隊在雲端管理和監控遷移的應用程式以解決任何問題的時段。通常，此期間的長度為 1-4 天。在超級護理期間結束時，遷移團隊通常會將應用程式的責任轉移給雲端營運團隊。

I

IaC

將基礎設施視為程式碼。

身分型政策

連接至一或多個 IAM 主體的政策，可定義其在 AWS 雲端 環境中的許可。

閒置應用程式

90 天期間 CPU 和記憶體平均使用率在 5% 至 20% 之間的應用程式。在遷移專案中，通常會淘汰這些應用程式或將其保留在內部部署。

IIoT

請參閱工業物聯網。

不可變的基礎設施

為生產工作負載部署新基礎設施的模型，而不是更新、修補或修改現有的基礎設施。不可變基礎設施本質上比可變基礎設施更一致、可靠且可預測。如需詳細資訊，請參閱 AWS Well-Architected Framework 中的使用不可變基礎設施部署最佳實務。

傳入 (輸入) VPC

在 AWS 多帳戶架構中，接受、檢查和路由來自應用程式外部之網路連線的 VPC。AWS 安全參考架構建議您使用傳入、傳出和檢查 VPC 來設定網路帳戶，以保護應用程式與更廣泛的網際網路之間的雙向介面。

增量遷移

一種切換策略，您可以在其中將應用程式分成小部分遷移，而不是執行單一、完整的切換。例如，您最初可能只將一些微服務或使用者移至新系統。確認所有項目都正常運作之後，您可以逐步移動其他微服務或使用者，直到可以解除委任舊式系統。此策略可降低與大型遷移關聯的風險。

工業 4.0

2016 年 Klaus Schwab 推出的術語，透過連線能力、即時資料、自動化、分析和 AI/ML 的進展，指製造程序的現代化。

基礎設施

應用程式環境中包含的所有資源和資產。

基礎設施即程式碼 (IaC)

透過一組組態檔案來佈建和管理應用程式基礎設施的程序。IaC 旨在協助您集中管理基礎設施，標準化資源並快速擴展，以便新環境可重複、可靠且一致。

工業物聯網 (IIoT)

在製造業、能源、汽車、醫療保健、生命科學和農業等產業領域使用網際網路連線的感測器和裝置。如需詳細資訊，請參閱建立工業物聯網 (IIoT) 數位轉型策略。

檢查 VPC

在 AWS 多帳戶架構中，集中式 VPC 可管理 VPCs 之間（在相同或不同的 中 AWS 區域)、網際網路和內部部署網路之間的網路流量檢查。AWS 安全參考架構建議您使用傳入、傳出和檢查 VPC 來設定網路帳戶，以保護應用程式與更廣泛的網際網路之間的雙向介面。

物聯網 (IoT)

具有內嵌式感測器或處理器的相連實體物體網路，其透過網際網路或本地通訊網路與其他裝置和系統進行通訊。如需詳細資訊，請參閱什麼是 IoT？

可解釋性

機器學習模型的一個特徵，描述了人類能夠理解模型的預測如何依賴於其輸入的程度。如需詳細資訊，請參閱 的機器學習模型可解譯性 AWS。

IoT

請參閱物聯網。

IT 資訊庫 (ITIL)

一組用於交付 IT 服務並使這些服務與業務需求保持一致的最佳實務。ITIL 為 ITSM 提供了基礎。

IT 服務管理 (ITSM)

與組織的設計、實作、管理和支援 IT 服務關聯的活動。如需有關將雲端操作與 ITSM 工具整合的資訊，請參閱操作整合指南。

ITIL

請參閱 IT 資訊庫。

ITSM

請參閱 IT 服務管理。

L

標籤型存取控制 (LBAC)

強制存取控制 (MAC) 的實作，其中使用者和資料本身都會獲得明確指派的安全標籤值。使用者安全標籤和資料安全標籤之間的交集會決定使用者可以看到哪些資料列和資料欄。

登陸區域

登陸區域是架構良好的多帳戶 AWS 環境，可擴展且安全。這是一個起點，您的組織可以從此起點快速啟動和部署工作負載與應用程式，並對其安全和基礎設施環境充滿信心。如需有關登陸區域的詳細資訊，請參閱設定安全且可擴展的多帳戶 AWS 環境。

大型語言模型 (LLM)

預先訓練大量資料的深度學習 AI 模型。LLM 可以執行多個任務，例如回答問題、摘要文件、將文字翻譯成其他語言，以及完成句子。如需詳細資訊，請參閱什麼是 LLMs。

大型遷移

遷移 300 部或更多伺服器。

LBAC

請參閱標籤型存取控制。

最低權限

授予執行任務所需之最低許可的安全最佳實務。如需詳細資訊，請參閱 IAM 文件中的套用最低權限許可。

隨即轉移

請參閱 7 個 R。

小端序系統

首先儲存最低有效位元組的系統。另請參閱 Endianness。

LLM

請參閱大型語言模型。

較低的環境

請參閱 環境。

M

機器學習 (ML)

一種使用演算法和技術進行模式識別和學習的人工智慧。機器學習會進行分析並從記錄的資料 (例如物聯網 (IoT) 資料) 中學習，以根據模式產生統計模型。如需詳細資訊，請參閱機器學習。

主要分支

請參閱分支。

惡意軟體

旨在危及電腦安全或隱私權的軟體。惡意軟體可能會中斷電腦系統、洩露敏感資訊，或取得未經授權的存取。惡意軟體的範例包括病毒、蠕蟲、勒索軟體、特洛伊木馬、間諜軟體和鍵盤記錄器。

受管服務

AWS 服務 會 AWS 操作基礎設施層、作業系統和平台，而您會存取端點來存放和擷取資料。Amazon Simple Storage Service (Amazon S3) 和 Amazon DynamoDB 是受管服務的範例。這些也稱為抽象服務。

製造執行系統 (MES)

一種軟體系統，用於追蹤、監控、記錄和控制生產程序，將原物料轉換為現場成品。

MAP

請參閱遷移加速計劃。

機制

建立工具、推動工具採用，然後檢查結果以進行調整的完整程序。機制是在操作時強化和改善自身的循環。如需詳細資訊，請參閱 AWS Well-Architected Framework 中的建置機制。

成員帳戶

除了屬於組織一部分的管理帳戶 AWS 帳戶 之外的所有 AWS Organizations。一個帳戶一次只能是一個組織的成員。

製造執行系統

請參閱製造執行系統。

訊息佇列遙測傳輸 (MQTT)

根據發佈/訂閱模式的輕量型machine-to-machine(M2M) 通訊協定，適用於資源受限的 IoT 裝置。

微服務

一種小型的獨立服務，它可透過定義明確的 API 進行通訊，通常由小型獨立團隊擁有。例如，保險系統可能包含對應至業務能力 (例如銷售或行銷) 或子領域 (例如購買、索賠或分析) 的微服務。微服務的優點包括靈活性、彈性擴展、輕鬆部署、可重複使用的程式碼和適應力。如需詳細資訊，請參閱使用無 AWS 伺服器服務整合微服務。

微服務架構

一種使用獨立元件來建置應用程式的方法，這些元件會以微服務形式執行每個應用程式程序。這些微服務會使用輕量型 API，透過明確定義的介面進行通訊。此架構中的每個微服務都可以進行

更新、部署和擴展，以滿足應用程式特定功能的需求。如需詳細資訊，請參閱在 上實作微服務 AWS。

Migration Acceleration Program (MAP)

一種 AWS 計畫，提供諮詢支援、訓練和服務，協助組織建立強大的營運基礎，以移至雲端，並協助抵銷遷移的初始成本。MAP 包括用於有條不紊地執行舊式遷移的遷移方法以及一組用於自動化和加速常見遷移案例的工具。

大規模遷移

將大部分應用程式組合依波次移至雲端的程序，在每個波次中，都會以更快的速度移動更多應用程式。此階段使用從早期階段學到的最佳實務和經驗教訓來實作團隊、工具和流程的遷移工廠，以透過自動化和敏捷交付簡化工作負載的遷移。這是 AWS 遷移策略的第三階段。

遷移工廠

可透過自動化、敏捷的方法簡化工作負載遷移的跨職能團隊。遷移工廠團隊通常包括營運、業務分析師和擁有者、遷移工程師、開發人員以及從事 Sprint 工作的 DevOps 專業人員。20% 至 50% 之間的企業應用程式組合包含可透過工廠方法優化的重複模式。如需詳細資訊，請參閱此內容集中的遷移工廠的討論和雲端遷移工廠指南。

遷移中繼資料

有關完成遷移所需的應用程式和伺服器的資訊。每種遷移模式都需要一組不同的遷移中繼資料。遷移中繼資料的範例包括目標子網路、安全群組和 AWS 帳戶。

遷移模式

可重複的遷移任務，詳細描述遷移策略、遷移目的地以及所使用的遷移應用程式或服務。範例：使用 AWS Application Migration Service 重新託管遷移至 Amazon EC2。

遷移組合評定 (MPA)

線上工具，提供驗證商業案例以遷移至 的資訊 AWS 雲端。MPA 提供詳細的組合評定 (伺服器適當規模、定價、總體擁有成本比較、遷移成本分析) 以及遷移規劃 (應用程式資料分析和資料收集、應用程式分組、遷移優先順序，以及波次規劃)。MPA 工具 （需要登入） 可供所有 AWS 顧問和 APN 合作夥伴顧問免費使用。

遷移準備程度評定 (MRA)

使用 AWS CAF 取得組織雲端整備狀態的洞見、識別優缺點，以及建立行動計劃以消除已識別差距的程序。如需詳細資訊，請參閱遷移準備程度指南。MRA 是 AWS 遷移策略的第一階段。

遷移策略

用來將工作負載遷移至 的方法 AWS 雲端。如需詳細資訊，請參閱此詞彙表中的 7 個 Rs 項目，並請參閱動員您的組織以加速大規模遷移。

機器學習 (ML)

請參閱機器學習。

現代化

將過時的 (舊版或單一) 應用程式及其基礎架構轉換為雲端中靈活、富有彈性且高度可用的系統，以降低成本、提高效率並充分利用創新。如需詳細資訊，請參閱《》中的現代化應用程式的策略 AWS 雲端。

現代化準備程度評定

這項評估可協助判斷組織應用程式的現代化準備程度；識別優點、風險和相依性；並確定組織能夠在多大程度上支援這些應用程式的未來狀態。評定的結果就是目標架構的藍圖、詳細說明現代化程序的開發階段和里程碑的路線圖、以及解決已發現的差距之行動計畫。如需詳細資訊，請參閱《》中的評估應用程式的現代化準備 AWS 雲端程度。

單一應用程式 (單一)

透過緊密結合的程序作為單一服務執行的應用程式。單一應用程式有幾個缺點。如果一個應用程式功能遇到需求激增，則必須擴展整個架構。當程式碼庫增長時，新增或改進單一應用程式的功能也會變得更加複雜。若要解決這些問題，可以使用微服務架構。如需詳細資訊，請參閱將單一體系分解為微服務。

MPA

請參閱遷移產品組合評估。

MQTT

請參閱訊息佇列遙測傳輸。

多類別分類

一個有助於產生多類別預測的過程 (預測兩個以上的結果之一)。例如，機器學習模型可能會詢問「此產品是書籍、汽車還是電話？」 或者「這個客戶對哪種產品類別最感興趣？」

可變基礎設施

更新和修改生產工作負載現有基礎設施的模型。為了提高一致性、可靠性和可預測性， AWS Well-Architected Framework 建議使用不可變基礎設施做為最佳實務。

O

OAC

請參閱原始存取控制。

OAI

請參閱原始存取身分。

OCM

請參閱組織變更管理。

離線遷移

一種遷移方法，可在遷移過程中刪除來源工作負載。此方法涉及延長停機時間，通常用於小型非關鍵工作負載。

OI

請參閱 操作整合。

OLA

請參閱操作層級協議。

線上遷移

一種遷移方法，無需離線即可將來源工作負載複製到目標系統。連接至工作負載的應用程式可在遷移期間繼續運作。此方法涉及零至最短停機時間，通常用於關鍵的生產工作負載。

OPC-UA

請參閱開放程序通訊 - 統一架構。

開放程序通訊 - 統一架構 (OPC-UA)

用於工業自動化的machine-to-machine(M2M) 通訊協定。OPC-UA 提供資料加密、身分驗證和授權機制的互通性標準。

操作水準協議 (OLA)

一份協議，闡明 IT 職能群組承諾向彼此提供的內容，以支援服務水準協議 (SLA)。

操作整備審查 (ORR)

問題和相關最佳實務的檢查清單，可協助您了解、評估、預防或減少事件和可能失敗的範圍。如需詳細資訊，請參閱 AWS Well-Architected Framework 中的操作準備度審查 (ORR)。

操作技術 (OT)

使用實體環境控制工業操作、設備和基礎設施的硬體和軟體系統。在製造業中，整合 OT 和資訊技術 (IT) 系統是工業 4.0 轉型的關鍵重點。

操作整合 (OI)

在雲端中將操作現代化的程序，其中包括準備程度規劃、自動化和整合。如需詳細資訊，請參閱操作整合指南。

組織追蹤

由 建立的線索 AWS CloudTrail 會記錄 AWS 帳戶 組織中所有 的所有事件 AWS Organizations。在屬於組織的每個 AWS 帳戶 中建立此追蹤，它會跟蹤每個帳戶中的活動。如需詳細資訊，請參閱 CloudTrail 文件中的建立組織追蹤。

組織變更管理 (OCM)

用於從人員、文化和領導力層面管理重大、顛覆性業務轉型的架構。OCM 透過加速變更採用、解決過渡問題，以及推動文化和組織變更，協助組織為新系統和策略做好準備，並轉移至新系統和策略。在 AWS 遷移策略中，此架構稱為人員加速，因為雲端採用專案所需的變更速度。如需詳細資訊，請參閱 OCM 指南。

原始存取控制 (OAC)

CloudFront 中的增強型選項，用於限制存取以保護 Amazon Simple Storage Service (Amazon S3) 內容。OAC 支援所有 S3 儲存貯體中的所有伺服器端加密 AWS KMS (SSE-KMS) AWS 區域，以及對 S3 儲存貯體的動態`PUT`和`DELETE`請求。

原始存取身分 (OAI)

CloudFront 中的一個選項，用於限制存取以保護 Amazon S3 內容。當您使用 OAI 時，CloudFront 會建立一個可供 Amazon S3 進行驗證的主體。經驗證的主體只能透過特定 CloudFront 分發來存取 S3 儲存貯體中的內容。另請參閱 OAC，它可提供更精細且增強的存取控制。

ORR

請參閱操作整備審核。

OT

請參閱操作技術。

傳出 (輸出) VPC

在 AWS 多帳戶架構中，處理從應用程式內啟動之網路連線的 VPC。AWS 安全參考架構建議您使用傳入、傳出和檢查 VPC 來設定網路帳戶，以保護應用程式與更廣泛的網際網路之間的雙向介面。

P

許可界限

附接至 IAM 主體的 IAM 管理政策，可設定使用者或角色擁有的最大許可。如需詳細資訊，請參閱 IAM 文件中的許可界限。

個人身分識別資訊 (PII)

當直接檢視或與其他相關資料配對時，可用來合理推斷個人身分的資訊。PII 的範例包括名稱、地址和聯絡資訊。

PII

請參閱個人身分識別資訊。

手冊

一組預先定義的步驟，可擷取與遷移關聯的工作，例如在雲端中提供核心操作功能。手冊可以採用指令碼、自動化執行手冊或操作現代化環境所需的程序或步驟摘要的形式。

PLC

請參閱可程式設計邏輯控制器。

PLM

請參閱產品生命週期管理。

政策

可定義許可的物件（請參閱身分型政策)、指定存取條件（請參閱資源型政策)，或定義組織中所有帳戶的最大許可 AWS Organizations（請參閱服務控制政策)。

混合持久性

根據資料存取模式和其他需求，獨立選擇微服務的資料儲存技術。如果您的微服務具有相同的資料儲存技術，則其可能會遇到實作挑戰或效能不佳。如果微服務使用最適合其需求的資料儲存，則

可以更輕鬆地實作並達到更好的效能和可擴展性。如需詳細資訊，請參閱在微服務中啟用資料持久性。

組合評定

探索、分析應用程式組合並排定其優先順序以規劃遷移的程序。如需詳細資訊，請參閱評估遷移準備程度。

述詞

傳回 `true`或 的查詢條件`false`，通常位於 `WHERE`子句中。

述詞下推

一種資料庫查詢最佳化技術，可在傳輸前篩選查詢中的資料。這可減少必須從關聯式資料庫擷取和處理的資料量，並改善查詢效能。

預防性控制

旨在防止事件發生的安全控制。這些控制是第一道防線，可協助防止對網路的未經授權存取或不必要變更。如需詳細資訊，請參閱在 AWS上實作安全控制中的預防性控制。

委託人

中可執行動作和存取資源 AWS 的實體。此實體通常是 AWS 帳戶、IAM 角色或使用者的根使用者。如需詳細資訊，請參閱 IAM 文件中角色術語和概念中的主體。

設計隱私權

透過整個開發程序將隱私權納入考量的系統工程方法。

私有託管區域

一種容器，它包含有關您希望 Amazon Route 53 如何回應一個或多個 VPC 內的域及其子域之 DNS 查詢的資訊。如需詳細資訊，請參閱 Route 53 文件中的使用私有託管區域。

主動控制

旨在防止部署不合規資源的安全控制。這些控制項會在佈建資源之前對其進行掃描。如果資源不符合控制項，則不會佈建。如需詳細資訊，請參閱 AWS Control Tower 文件中的控制項參考指南，並參閱實作安全控制項中的主動控制項。 AWS

產品生命週期管理 (PLM)

管理產品整個生命週期的資料和程序，從設計、開發和啟動，到成長和成熟，再到拒絕和移除。

生產環境

請參閱 環境。

可程式設計邏輯控制器 (PLC)

在製造中，高度可靠、可調整的電腦，可監控機器並自動化製造程序。

提示鏈結

使用一個 LLM 提示的輸出做為下一個提示的輸入，以產生更好的回應。此技術用於將複雜任務分解為子任務，或反覆精簡或展開初步回應。它有助於提高模型回應的準確性和相關性，並允許更精細、個人化的結果。

擬匿名化

將資料集中的個人識別符取代為預留位置值的程序。假名化有助於保護個人隱私權。假名化資料仍被視為個人資料。

發佈/訂閱 (pub/sub)

一種模式，可啟用微服務之間的非同步通訊，以提高可擴展性和回應能力。例如，在微服務型 MES 中，微服務可以將事件訊息發佈到其他微服務可訂閱的頻道。系統可以新增新的微服務，而無需變更發佈服務。

Q

查詢計劃

一系列步驟，如指示，用於存取 SQL 關聯式資料庫系統中的資料。

查詢計劃迴歸

在資料庫服務優化工具選擇的計畫比對資料庫環境進行指定的變更之前的計畫不太理想時。這可能因為對統計資料、限制條件、環境設定、查詢參數繫結的變更以及資料庫引擎的更新所導致。

R

RACI 矩陣

請參閱負責、負責、諮詢、告知 (RACI)。

RAG

請參閱擷取增強產生。

勒索軟體

一種惡意軟體，旨在阻止對計算機系統或資料的存取，直到付款為止。

RASCI 矩陣

請參閱負責、負責、諮詢、告知 (RACI)。

RCAC

請參閱資料列和資料欄存取控制。

僅供讀取複本

用於唯讀用途的資料庫複本。您可以將查詢路由至僅供讀取複本以減少主資料庫的負載。

重新架構師

請參閱 7 個 R。

復原點目標 (RPO)

自上次資料復原點以來可接受的時間上限。這會決定最後一個復原點與服務中斷之間可接受的資料遺失。

復原時間目標 (RTO)

服務中斷與服務還原之間的可接受延遲上限。

重構

請參閱 7 個 R。

區域

地理區域中的 AWS 資源集合。每個 AWS 區域 都獨立於其他 ，以提供容錯能力、穩定性和彈性。如需詳細資訊，請參閱指定 AWS 區域 您的帳戶可以使用哪些 。

迴歸

預測數值的 ML 技術。例如，為了解決「這房子會賣什麼價格？」的問題 ML 模型可以使用線性迴歸模型，根據已知的房屋事實 (例如，平方英尺) 來預測房屋的銷售價格。

重新託管

請參閱 7 個 R。

版本

在部署程序中，它是將變更提升至生產環境的動作。

重新定位

請參閱 7 個 R。

Replatform

請參閱 7 個 R。

回購

請參閱 7 個 R。

彈性

應用程式抵禦中斷或從中斷中復原的能力。在 中規劃彈性時，高可用性和災難復原是常見的考量 AWS 雲端。如需詳細資訊，請參閱AWS 雲端 彈性。

資源型政策

附接至資源的政策，例如 Amazon S3 儲存貯體、端點或加密金鑰。這種類型的政策會指定允許存取哪些主體、支援的動作以及必須滿足的任何其他條件。

負責者、當責者、事先諮詢者和事後告知者 (RACI) 矩陣

矩陣，定義所有參與遷移活動和雲端操作之各方的角色和責任。矩陣名稱衍生自矩陣中定義的責任類型：負責人 (R)、責任 (A)、已諮詢 (C) 和知情 (I)。支援 (S) 類型為選用。如果您包含支援，則矩陣稱為 RASCI 矩陣，如果您排除它，則稱為 RACI 矩陣。

回應性控制

一種安全控制，旨在驅動不良事件或偏離安全基準的補救措施。如需詳細資訊，請參閱在 AWS上實作安全控制中的回應性控制。

保留

請參閱 7 個 R。

淘汰

請參閱 7 個 R。

檢索增強生成 (RAG)

一種生成式 AI 技術，其中 LLM 會在產生回應之前參考訓練資料來源以外的授權資料來源。例如，RAG 模型可能會對組織的知識庫或自訂資料執行語意搜尋。如需詳細資訊，請參閱什麼是 RAG。

輪換

定期更新秘密的程序，讓攻擊者更難存取登入資料。

資料列和資料欄存取控制 (RCAC)

使用已定義存取規則的基本、彈性 SQL 表達式。RCAC 包含資料列許可和資料欄遮罩。

RPO

請參閱復原點目標。

RTO

請參閱復原時間目標。

執行手冊

執行特定任務所需的一組手動或自動程序。這些通常是為了簡化重複性操作或錯誤率較高的程序而建置。

S

SAML 2.0

許多身分提供者 (IdP) 使用的開放標準。此功能會啟用聯合單一登入 (SSO)，讓使用者可以登入 AWS Management Console 或呼叫 AWS API 操作，而不必為您組織中的每個人在 IAM 中建立使用者。如需有關以 SAML 2.0 為基礎的聯合詳細資訊，請參閱 IAM 文件中的關於以 SAML 2.0 為基礎的聯合。

SCADA

請參閱監督控制和資料擷取。

SCP

請參閱服務控制政策。

秘密

您以加密形式存放的 AWS Secrets Manager機密或限制資訊，例如密碼或使用者登入資料。它由秘密值及其中繼資料組成。秘密值可以是二進位、單一字串或多個字串。如需詳細資訊，請參閱 Secrets Manager 文件中的 Secrets Manager 秘密中的什麼內容？。

設計安全性

透過整個開發程序將安全性納入考量的系統工程方法。

安全控制

一種技術或管理防護機制，它可預防、偵測或降低威脅行為者利用安全漏洞的能力。安全控制有四種主要類型：預防性、偵測性、回應性和主動性。

安全強化

減少受攻擊面以使其更能抵抗攻擊的過程。這可能包括一些動作，例如移除不再需要的資源、實作授予最低權限的安全最佳實務、或停用組態檔案中不必要的功能。

安全資訊與事件管理 (SIEM) 系統

結合安全資訊管理 (SIM) 和安全事件管理 (SEM) 系統的工具與服務。SIEM 系統會收集、監控和分析來自伺服器、網路、裝置和其他來源的資料，以偵測威脅和安全漏洞，並產生提醒。

安全回應自動化

預先定義和程式設計的動作，旨在自動回應或修復安全事件。這些自動化可做為偵測或回應式安全控制，協助您實作 AWS 安全最佳實務。自動化回應動作的範例包括修改 VPC 安全群組、修補 Amazon EC2 執行個體或輪換登入資料。

伺服器端加密

由 AWS 服務 接收資料的 在其目的地加密資料。

服務控制政策 (SCP)

為 AWS Organizations中的組織的所有帳戶提供集中控制許可的政策。SCP 會定義防護機制或設定管理員可委派給使用者或角色的動作限制。您可以使用 SCP 作為允許清單或拒絕清單，以指定允許或禁止哪些服務或動作。如需詳細資訊，請參閱 AWS Organizations 文件中的服務控制政策。

服務端點

的進入點 URL AWS 服務。您可以使用端點，透過程式設計方式連接至目標服務。如需詳細資訊，請參閱 AWS 一般參考 中的 AWS 服務 端點。

服務水準協議 (SLA)

一份協議，闡明 IT 團隊承諾向客戶提供的服務，例如服務正常執行時間和效能。

服務層級指標 (SLI)

服務效能層面的測量，例如其錯誤率、可用性或輸送量。

服務層級目標 (SLO)

代表服務運作狀態的目標指標，由服務層級指標測量。

共同責任模式

描述您與 共同 AWS 承擔雲端安全與合規責任的模型。 AWS 負責雲端的安全，而 負責雲端的安全。如需詳細資訊，請參閱共同責任模式。

SIEM

請參閱安全資訊和事件管理系統。

單一故障點 (SPOF)

應用程式的單一關鍵元件故障，可能會中斷系統。

SLA

請參閱服務層級協議。

SLI

請參閱服務層級指標。

SLO

請參閱服務層級目標。

先拆分後播種模型

擴展和加速現代化專案的模式。定義新功能和產品版本時，核心團隊會進行拆分以建立新的產品團隊。這有助於擴展組織的能力和服務，提高開發人員生產力，並支援快速創新。如需詳細資訊，請參閱 中的階段式應用程式現代化方法 AWS 雲端。

SPOF

請參閱單一故障點。

星狀結構描述

使用一個大型事實資料表來存放交易或測量資料的資料庫組織結構，並使用一或多個較小的維度資料表來存放資料屬性。此結構旨在用於資料倉儲或商業智慧用途。

Strangler Fig 模式

一種現代化單一系統的方法，它會逐步重寫和取代系統功能，直到舊式系統停止使用為止。此模式源自無花果藤，它長成一棵馴化樹並最終戰勝且取代了其宿主。該模式由 Martin Fowler 引入，作

為重寫單一系統時管理風險的方式。如需有關如何套用此模式的範例，請參閱使用容器和 Amazon API Gateway 逐步現代化舊版 Microsoft ASP.NET (ASMX) Web 服務。

子網

您 VPC 中的 IP 地址範圍。子網必須位於單一可用區域。

監控控制和資料擷取 (SCADA)

在製造中，使用硬體和軟體來監控實體資產和生產操作的系統。

對稱加密

使用相同金鑰來加密及解密資料的加密演算法。

合成測試

以模擬使用者互動的方式測試系統，以偵測潛在問題或監控效能。您可以使用 Amazon CloudWatch Synthetics 來建立這些測試。

系統提示

一種向 LLM 提供內容、指示或指導方針以指示其行為的技術。系統提示有助於設定內容，並建立與使用者互動的規則。

T

標籤

做為中繼資料以組織 AWS 資源的鍵值對。標籤可協助您管理、識別、組織、搜尋及篩選資源。如需詳細資訊，請參閱標記您的 AWS 資源。

目標變數

您嘗試在受監督的 ML 中預測的值。這也被稱為結果變數。例如，在製造設定中，目標變數可能是產品瑕疵。

任務清單

用於透過執行手冊追蹤進度的工具。任務清單包含執行手冊的概觀以及要完成的一般任務清單。對於每個一般任務，它包括所需的預估時間量、擁有者和進度。

測試環境

請參閱 環境。

訓練

為 ML 模型提供資料以供學習。訓練資料必須包含正確答案。學習演算法會在訓練資料中尋找將輸入資料屬性映射至目標的模式 (您想要預測的答案)。它會輸出擷取這些模式的 ML 模型。可以使用 ML 模型，來預測您不知道的目標新資料。

傳輸閘道

可以用於互連 VPC 和內部部署網路的網路傳輸中樞。如需詳細資訊，請參閱 AWS Transit Gateway 文件中的什麼是傳輸閘道。

主幹型工作流程

這是一種方法，開發人員可在功能分支中本地建置和測試功能，然後將這些變更合併到主要分支中。然後，主要分支會依序建置到開發環境、生產前環境和生產環境中。

受信任的存取權

將許可授予您指定的服務，以代表您在組織中 AWS Organizations 及其帳戶中執行任務。受信任的服務會在需要該角色時，在每個帳戶中建立服務連結角色，以便為您執行管理工作。如需詳細資訊，請參閱 文件中的 AWS Organizations 搭配使用 AWS Organizations 與其他 AWS 服務。

調校

變更訓練程序的各個層面，以提高 ML 模型的準確性。例如，可以透過產生標籤集、新增標籤、然後在不同的設定下多次重複這些步驟來訓練 ML 模型，以優化模型。

雙比薩團隊

兩個比薩就能吃飽的小型 DevOps 團隊。雙披薩團隊規模可確保軟體開發中的最佳協作。

U

不確定性

這是一個概念，指的是不精確、不完整或未知的資訊，其可能會破壞預測性 ML 模型的可靠性。有兩種類型的不確定性：認知不確定性是由有限的、不完整的資料引起的，而隨機不確定性是由資料中固有的噪聲和隨機性引起的。如需詳細資訊，請參閱量化深度學習系統的不確定性指南。

未區分的任務

也稱為繁重工作，這是建立和操作應用程式的必要工作，但不為最終使用者提供直接價值或提供競爭優勢。未區分任務的範例包括採購、維護和容量規劃。

較高的環境

請參閱 環境。

V

清空

一種資料庫維護操作，涉及增量更新後的清理工作，以回收儲存並提升效能。

版本控制

追蹤變更的程序和工具，例如儲存庫中原始程式碼的變更。

VPC 對等互連

兩個 VPC 之間的連線，可讓您使用私有 IP 地址路由流量。如需詳細資訊，請參閱 Amazon VPC 文件中的什麼是 VPC 對等互連。

漏洞

危害系統安全性的軟體或硬體瑕疵。

W

暖快取

包含經常存取的目前相關資料的緩衝快取。資料庫執行個體可以從緩衝快取讀取，這比從主記憶體或磁碟讀取更快。

暖資料

不常存取的資料。查詢這類資料時，通常可接受中等速度的查詢。

視窗函數

SQL 函數，對與目前記錄有某種程度關聯的資料列群組執行計算。視窗函數適用於處理任務，例如根據目前資料列的相對位置計算移動平均值或存取資料列的值。

工作負載

提供商業價值的資源和程式碼集合，例如面向客戶的應用程式或後端流程。

工作串流

遷移專案中負責一組特定任務的功能群組。每個工作串流都是獨立的，但支援專案中的其他工作串流。例如，組合工作串流負責排定應用程式、波次規劃和收集遷移中繼資料的優先順序。組合工作串流將這些資產交付至遷移工作串流，然後再遷移伺服器和應用程式。

WORM

請參閱寫入一次，讀取許多。

WQF

請參閱AWS 工作負載資格架構。

寫入一次，讀取許多 (WORM)

儲存模型，可一次性寫入資料，並防止刪除或修改資料。授權使用者可以視需要多次讀取資料，但無法變更資料。此資料儲存基礎設施被視為不可變。

Z

零時差入侵

利用零時差漏洞的攻擊，通常是惡意軟體。

零時差漏洞

生產系統中未緩解的缺陷或漏洞。威脅行為者可以使用這種類型的漏洞來攻擊系統。開發人員經常因為攻擊而意識到漏洞。

零鏡頭提示

提供 LLM 執行任務的指示，但沒有可協助引導任務的範例 (快照)。LLM 必須使用其預先訓練的知識來處理任務。零鏡頭提示的有效性取決於任務的複雜性和提示的品質。另請參閱少量擷取提示。

殭屍應用程式

CPU 和記憶體平均使用率低於 5% 的應用程式。在遷移專案中，通常會淘汰這些應用程式。

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。