AWS規範指導

AWS啟動安全基準 (AWSSSB)

AWS規範指導: AWS啟動安全基準 (AWSSSB)

Table of Contents

AWS啟動安全基準 (AWSSSB)

由傑伊邁克爾創建, Amazon Web Services (AWS)

2022 年 4 月 (上次更新 (p. 17): 2022 年 5 月)

Amazon Web Services (AWS) 啟動安全基準 (SSB) 是一組控件，它們為企業在AWS而不降低他們的敏捷性. 本指南中的控制措施設計時考慮到早期初創公司，從而降低了最常見的安全風險，而無需大量努力。隨着組織的發展或滿足大型企業的需求，您可以在這些控制基礎上進行擴展和構建。它們構成了安全狀況的基礎，重點是保護憑據、啟用日誌記錄和可見性、管理聯繫人信息以及實施基本數據邊界。

中的控件AWSSSB 分為兩類：帳户和工作負載。帳户控制有助於保持AWS帳户安全。它包括有關設置用户訪問權限、策略和權限的建議，還包括如何監控您的帳户是否有未經授權或潛在的惡意活動的建議。工作負載控制有助於保護雲中的資源和代碼，例如應用程序、後端流程和數據。它包括諸如加密和縮小訪問範圍等建議。

> Note
>
> 本指南中建議的一些控件替換了初始設置期間配置的默認值，而大多數配置新設置和策略。這份文件絕不應被視為全面的所有可用控制措施。

目標對象

本指南最適合處於開發階段的初創公司，員工和運營最少。

初創公司或處於後期經營和增長階段的其他企業依然可以通過對照當前的做法審查這些控制獲得重大價值。如果發現任何差距，您可以實施本指南中的單個控制，然後評估它們是否適當，作為長期解決方案。

> Note
>
> 本指南中推薦的控件本質上是基礎控件。初創公司或其他在規模或複雜階段經營的公司應酌情增加額外的控制措施。

基本框架和安全責任

AWSWWell-Architected幫助雲架構師為其應用程序和工作負載構建安全、高性能、可恢復性和高效的基礎架構。所以此AWS啟動安全基線與安全要件的AWSWWell-Architected Fell. 所以此安全要件介紹瞭如何利用雲技術來保護數據、系統和資產，以改善您的安全狀況。這樣做有助您符合商業和法規需求，方法是遵循當前AWS建議。

您可以 Well-Architected 使用AWS Well-Architected Tool在您的AWS帳户。

安全與合規是AWS和客户。所以此共同責任模型通常被描述為AWS負責雲端安全（即保護其執行所有服務的基礎設施，這些服務是在AWS 雲端），並且您負責雲中的安全性（由AWS 雲端服務）。在責任分擔模型中，實施本文檔中的安全控制是您作為客户的責任的一部分。

保護您的帳户

本節中的控件和建議有助於保持AWS帳户安全。它強調使用AWS Identity and Access Management(IAM)使用者、使用者組和角色（也稱為校長），限制 root 用户的使用，並需要多重身份驗證。在本節中，您需要確認AWS有必要的聯繫信息，以便與您聯繫有關您的賬户活動和狀態。您也可以建立監視服務，如AWS Trusted Advisor、Amazon GuardDuty 和AWS Budgets，以便您收到賬户中活動的通知，並且在活動未經授權或意外時可以快速響應。

本節包含下列主題：

ACCT.01 — 將帳户級別的聯繫人設置為有效的電子郵件通訊組列表

設置主要聯繫人和備用聯繫人時AWS帳户，請使用電子郵件通訊組列表而不是個人的電子郵件地址。使用電子郵件通訊組列表可確保所有權和可訪問性在組織中的個人進出時得到保留。設定帳單、操作和安全通知的替代聯繫人，並相應地使用適當的電子郵件通訊組列表。AWS使用這些電子郵件地址與您聯繫，因此保留對它們的訪問權限非常重要。

編輯您的帳戶名稱、根使用者密碼或根使用者電子郵件地址

1. 登入帳戶設定頁面，位於 Billing and Cost Management 主控台中的https://console.aws.amazon.com/billing/home?#/account。
2. 在 Account Settings (帳戶設定) 頁面的 Account Settings (帳戶設定) 旁，選擇 Edit (編輯)。
3. 在您要更新的欄位旁，選擇Edit (編輯)。
4. 輸入完變更後，請選擇 Save changes (儲存變更)。
5. 完成所有變更後，請選擇 Done (完成)。

若要編輯您的聯絡資訊

1. 在帳戶設定頁面，在聯絡資訊，選擇Edit (編輯)。
2. 對於您要變更的欄位，輸入更新資訊然後選擇更新。

若要新增、更新或移除替代聯絡人

1. 在帳戶設定頁面，在替代聯絡資訊，選擇Edit (編輯)。
2. 對於您要變更的欄位，輸入更新資訊然後選擇更新。

ACC.02 — 限制使用根用户

root 用户是在您註冊AWS帳户，並且此用户對無法更改的帳户具有完全所有權和權限。僅將 root 用户用於需要它的特定任務。如需詳細資訊，請參閱「」需要根使用者憑證的任務(AWS一般參考資料)。通過使用 IAM 用户或具有 IAM 角色的聯合用户在您的賬户中執行所有其他操作。

限制 root 用户的使用

1. 如所述，需要根使用者的多重驗證 (MFA)。ACCT.05 — 需要多重驗證 (MFA) 才能登入 (p. 4)。
2. 建立您的第一個 IAM 管理員使用者和使用者組（IAM 文檔）。

ACCT.03 — 為每個用户配置控制台訪問

作為基準，請為每個需要訪問AWS Management Console。不要在用户之間共享憑據。

建立 IAM 使用者

1. 建立 IAM 使用者（IAM 文檔）。
2. 應用權限，根據ACC.04 — 通過使用 IAM 用户組分配權限 (p. 3)。

雖然 IAM 用户對AWS，我們建議您使用來自集中身份提供程序 (IdP) 的聯合用户，例如AWS IAM Identity Center (successor to AWS Single Sign-On)(IAM Identity Center）、Okta、活動目錄或 Ping 身份。聯合用户允許您在單個集中位置定義身份，用户可以安全地對多個應用程序和網站進行身份驗證，包括AWS，只需使用一組憑據。如需詳細資訊，請參閱「」中的身分聯合AWS(AWS網站)。

設定聯合身分

1. 如果您是使用IAM Identity Center，請參入門(IAM Identity Center文件中)。
2. 確保 IdP 強制執行多重驗證 (MFA)。

ACC.04 — 通過使用 IAM 用户組分配權限

您可以使用 IAM 用户組為多個 IAM 用户配置權限。根據用户的作業功能將用户分配給用户組。用户組的示例包括應用程序、數據、網絡和開發運營 (DevOps) 工程師。您還可以根據決策權限將用户類型劃分為較小的用户組，例如高級或非高級工程師。

向 IAM 用户組分配權限時，您可以自定義權限，也可以將AWS受管政策，這些策略是由AWS為許多常用案例提供許可。如果您自定義權限，請遵循授予最低權限。最低權限是授予每個使用者執行其任務所需最低許可集的做法。

建立使用者組並指派許可

1. 建立 IAM 使用者羣組（IAM 文檔）。
2. 連接AWS將受管政策連接至 IAM 使用者組（IAM 文檔）。

ACCT.05 — 需要多重驗證 (MFA) 才能登入

啟用 MFAAWS帳户根用户和具有提升權限的任何委託人用户，例如可以創建、更新或刪除資源或訪問對業務運營至關重要的數據的用户。

針對根使用者啟用 MFA

1. 前往 https://console.aws.amazon.com/ 登入 AWS Management Console。
2. 在導覽列右側，選擇您的帳號名稱，然後選擇我的安全登入資料。
3. 如有需要，選擇 Continue to Security Credentials (繼續至安全憑證)。
4. 展開 Multi-Factor Authentication (MFA) 區段。
5. 選擇 Activate MFA (啟用 MFA)。
6. 按照嚮導說明相應地配置 MFA 設備。如需詳細資訊，請參閱「」在中為使用者啟用 MFA 設備 AWS（IAM 文檔）。

若要為您的 IAM 使用者帳户建立 MFA

1. 使用您的AWS帳户 ID 或帳户別名、IAM 使用者名稱及密碼，登入 IAM 主控台，網址為https://console.aws.amazon.com/iam。
2. 在右上方的導覽列中，選擇您的使用者名稱，然後選擇 My Security Credentials (我的安全憑證)。
3. 在 AWS IAM credentials (AWS IAM 憑證) 索引標籤上，在 Multi-factor authentication (多重要素驗證) 區段，選擇 Manage MFA device (管理 MFA 裝置)。

為其他 IAM 用户啟用 MFA

1. 登入AWS Management Console，開啟 IAM 主控台 (https://console.aws.amazon.com/iam。
2. 在導覽窗格中，選擇 Users (使用者)。
3. 選擇要為其啟用 MFA 的使用者名稱，然後選擇 Security credentials (安全憑證) 索引標籤。
4. 在 Assigned MFA device (指派的 MFA 裝置) 旁，選擇 Manage (管理)。
5. 按照嚮導說明相應地配置 MFA 設備。如需詳細資訊，請參閱「」在中為使用者啟用 MFA 設備 AWS（IAM 文檔）。

ACC.06 — 強制執行密碼策略

IAM 用户登錄到AWS Management Console通過使用用户名和密碼的組合, 與 MFA 推薦. 要求密碼遵守強密碼策略，以幫助防止通過暴力或社交工程發現。

如需最新強密碼建議的詳細資訊，請參密碼政策指南在 Center to Internet Security (CIS) 網站。

您可以在自定義 IAM 密碼策略中配置密碼要求。如需詳細資訊，請參閱「」設定 IAM 使用者的帳戶密碼政策（IAM 文檔）。

建立自訂密碼政策

1. 登入AWS Management Console，開啟 IAM 主控台 (https://console.aws.amazon.com/iam。
2. 在導覽窗格中，選擇 Account settings (帳戶設定)。
3. 在 Password policy (密碼政策) 區段中，選擇 Change password policy (變更密碼政策)。
4. 選擇您要套用到密碼政策的選項，然後選擇儲存變更。

第 07 條 — 交付 CloudTrail 日誌到受保護的 S3 存儲桶

使用者、角色和服務在您的AWS帳户記錄為AWS CloudTrail。 CloudTrail 預設為啟用，並在 CloudTrail 控制台，您可以訪問 90 天的事件歷史記錄信息。若要查看、搜尋、下載、存檔、分析和回應您AWS基礎設施，請參使用 CloudTrail 事件歷史記錄檢視事件（CloudTrail 文檔）。

保留 CloudTrail 歷史記錄超過 90 天，就可以建立新追蹤，將日誌檔案交付到 Amazon Simple Storage Service (Amazon S3) 儲存貯體，適用於所有事件類型。當您在 CloudTrail 主控台中會建立多區域線索。

創建提供所有日誌的跟蹤AWS 區域連接至 S3 儲存桶

1. 建立線索（CloudTrail 文檔）。在選擇日誌事件頁面上，執行以下作業：
   a. 適用於API 活動，選擇閱讀和寫入。
   b. 對於預生產環境，請選擇ExcludeAWS KMS事件。這將排除所有AWS Key Management Service(AWS KMS）事件。AWS KMS 閱讀操作，例如`Encrypt`、`Decrypt`，以及`GenerateDataKey`可以生成大量的事件。

      對於生產環境，選擇記錄寫入管理事件，然後清除ExcludeAWS KMS事件。這不包括大量AWS KMS讀取事件，但仍會記錄相關的寫入事件，例如`Disable`、`Delete`，以及`ScheduleKey`。這些是推薦的最低AWS KMS日誌記錄設定。
2. 新的追蹤會出現在 Trails (追蹤) 頁面上。在大約 15 分鐘內, CloudTrail 發佈日誌文件，顯示AWS在您的帳户中進行應用程式設計界面 (API) 調用。您可以在所指定之 S3 儲存貯體中看到日誌檔案。

如需保護儲存貯體的 S3 儲存貯體 CloudTrail 日誌檔案

1. 檢Amazon S3 儲存儲體政策（CloudTrail 文檔），用於存放日誌檔案的任何儲存貯體，並調整其在需要時移除任何不必要的存取。
2. 作為安全最佳實務，請務必手動添加`aws:SourceArn`條件密鑰添加到存儲桶策略。如需詳細資訊，請參閱「」建立或更新 Amazon S3 儲存貯體以存放組織追蹤的日誌檔案（CloudTrail 文檔）。
3. 啟用 MFA Delete（Amazon S3 文檔）。

ACCT.08 — 阻止公共訪問私有 S3 存儲桶

默認情況下，只有AWS賬户和 IAM 委託人（如果使用）具有讀取和寫入由該委託人創建的 Amazon S3 存儲桶的權限。通過使用基於身份的策略授予其他 IAM 委託人的訪問權限，並且可以使用存儲桶策略強制執行訪問條件。您可以創建存儲桶策略，以便向一般公眾授予對存儲桶的訪問權限，公有儲存桶。

用户可能會錯誤配置存儲桶策略並無意中授予公共訪問權限。您可以通過啟用封鎖公有存取權限設置。如果您沒有公用 S3 存儲桶的當前或將 future 的使用案例，請在AWS帳户級別。此設置阻止允許公共訪問的策略。

如需保護儲存貯體的 S3 儲存貯體 CloudTrail 日誌檔案

- 為您的 S3 儲存貯體配置塊公開存取（Amazon S3 文檔）。

AWS Trusted Advisor為允許對公眾進行列表或讀取訪問的 S3 存儲桶生成黃色查找結果，併為允許公共上傳或刪除的存儲桶生成紅色查找結果。作為基準，請遵循控件ACCT.12 — 通過使用Trusted Advisor (p. 6)來識別並更正錯誤配置的存儲桶。Amazon S3 主控台中也會指示公開存取的 S3 儲存貯體。

ACC.09 — 刪除未使用的 VPC、子網路和安全組

要減少出現安全問題的機會，請刪除或關閉任何未使用的資源。在一個新的AWS帳戶，默認情況下，VPC 在每個AWS 區域，使您可以在公有子網中分配公有 IP 地址。但是，如果不需要這些 VPC，這會帶來意外暴露資源的風險。

如果未使用它們，請刪除所有區域中的默認 VPC，而不僅僅是您可能部署工作負載的區域中的 VPC。刪除 VPC 還會刪除其組件，如子網和安全組。

> Note
>
> 您可以在 Amazon EC2 全域檢視主控台上查看所有區域和 VPC，網址為https://console.aws.amazon.com/ec2globalview/home。如需詳細資訊，請參閱「」使用 Amazon EC2 全域檢視列出和篩選跨區域的資源（Amazon EC2 文檔）。

刪除未使用的默認 VPC

1. 刪除您的 VPC（Amazon VPC 文件）。
2. 根據需要對其他區域中的 VPC 重複此選項。

第 10 條 — 配置AWS Budgets監控您的支出

AWS Budgets可在預測成本超過目標閾值時通知監控月度成本和使用情況。預測成本通知可以提供意外活動的指示，除了其他監控系統（例如AWS Trusted Advisor和 Amazon GuardDuty。監控和瞭解您的AWS成本也是良好的操作衛生的一部分。

若要在AWS Budgets

- 建立成本預算(AWS Budgets文件中)。

第 11 條 — 啟用並響應 GuardDuty 通知

亞馬遜 GuardDuty 是一種威脅檢測服務，可持續監控惡意或未經授權的行為，以幫助保護AWS帳戶、工作負載和數據。如果檢測到非預期和潛在惡意活動， GuardDuty 提供詳細的安全調查結果，以實現可見性和補救。 GuardDuty 可以檢測威脅，例如加密貨幣挖掘活動、Tor 客戶端和中繼訪問權限、意外行為以及 IAM 證書被盜用。啟用 GuardDuty 並響應調查結果，以阻止您的AWS環境。如需問題清單中的調查結果的詳 GuardDuty 資訊，請參問題清單類型（GuardDuty 文檔）。

您可以使用亞馬遜 CloudWatch 設置自動通知的事件 GuardDuty 創建查找結果或查找結果更改。首先，您建立 Amazon Simple Notification Service (Amazon SNS) 主題，然後將終端節點或電子郵件地址添加至主題。然後，您設定 CloudWatch 事件 GuardDuty 查找結果，事件規則會通知 Amazon SNS 主題中的終端節點。

啟用 GuardDuty 和 GuardDuty 通知

1. 啟用 Amazon GuardDuty（GuardDuty 文檔）。
2. 建立 CloudWatch 事件規則通知您 GuardDuty 發現（GuardDuty 文檔）。

ACCT.12 — 通過使用Trusted Advisor

AWS Trusted Advisor被動掃描AWS基礎架構，解決與安全性、性能、成本和可靠性相關的高風險或高影響問題。它提供了有關受影響資源和補救建議的詳細信息。如需檢查和說明的完整清單，請參AWS Trusted Advisor檢查參考(Trusted Advisor文件中)。

檢閱Trusted Advisor並根據需要對問題進行補救. 如果您擁有AWS業務 Support 或企業 Support 計劃，您可以訂閱每週發現的電子郵件。如需詳細資訊，請參閱「」設定通知偏好設定(AWS Support文件中)。

若要查看Trusted Advisor

- 檢視每個支票類別，請參照檢視檢查類別(AWS Support文件中)。至少，我們建議您查看建議的動作問題，這是紅色的。

保護您的工作負載

本節中的控制和建議可幫助您保護在AWS，而您正在構建它們。它們強調了管理應用程序祕密和訪問範圍的安全做法，最大限度地減少到私有資源的訪問路由，並使用加密來保護傳輸中和靜態數據。

本節包含下列主題：

WKLD.01 — 將 IAM 角色用於計算環境權限

InAWS Identity and Access Management(IAM)、角色表示一組可由人員或服務在可配置的時間段內承擔的權限。使用角色消除了存儲或管理長期憑據的需要，從而大大減少了意外使用的可能性。將 IAM 角色直接分配給 Elastic Compute Cloud (Amazon EC2) 個體，AWS Fargate任務和服務,AWS Lambda函數和其他AWS計算服務。應用程序使用AWSSDK 並在這些計算環境中運行，自動使用 IAM 角色證書進行身份驗證。

如需範例，請參閱使用 Amazon Elastic Compute Cloud 執行個體的 IAM 角色(YouTube 視頻). 將 IAM 角色用於其他AWS服務是相似的，並且說明可以在AWS文件用於服務。

WKLD.02 — 使用基於資源的策略權限限制憑據使用範圍

策略是可以定義權限或指定訪問條件的對象。主要有兩種類型的政策：

- 以身分為基礎的政策附加到委託人，並定義委託人在AWS環境。
- 以資源為基礎的政策連接到資源，例如 Simple Storage Service (Amazon S3) 桶或虛擬私有雲 (VPC) 端點。這些策略指定允許哪些承擔者訪問、受支持的操作以及必須滿足的任何其他條件。

要允許委託人訪問對資源執行操作，必須在其基於身份的策略中授予權限，並滿足基於資源的策略的條件。如需詳細資訊，請參閱「」以身分為基礎和以資源為基礎的政策（IAM 文檔）。

以資源為基礎的政策的推薦條件包括：

- 僅限於指定組織中的委託人的訪問權限（在AWS Organizations）通過使用`aws:PrincipalOrgID`條件。
- 限制訪問源自特定 VPC 或 VPC 端點的流量，方法是使用`aws:SourceVpc`或者`aws:SourceVpce`條件。
- 允許或拒絕根據來源 IP 地址使用`aws:SourceIp`條件。

以下是使用`aws:PrincipalOrgID`條件來僅允許**<o-xxxxxxxxxxx>**組織訪問**<bucket-name>**S3 儲存貯體：

```
{
   "Version":"2012-10-17",
   "Statement":[
     {
       "Sid":"AllowFromOrganization",
       "Effect":"Allow",
       "Principal":"*",
       "Action":"s3:*",
       "Resource":"arn:aws:s3:::<bucket-name>/*",
       "Condition": {
         "StringEquals": {"aws:PrincipalOrgID":"<o-xxxxxxxxxxx>"}
       }
     }
   ]
}
```

WKLD.03 — 使用臨時祕密或祕密管理服務

應用程序密鑰主要由憑據組成，例如密鑰對、訪問令牌、數字證書以及用户名和密碼組合。應用程序使用這些機密訪問它所依賴的其他服務（如數據庫）。為了幫助保護這些祕密，我們建議它們是短暫的（在請求時生成的，而且使用 IAM 角色）或者是從祕密管理服務中檢索的。這樣可以通過安全性較低的機制（如保留在靜態配置文件中）防止意外泄露。這還可以更輕鬆地將應用程序代碼從開發環境升級到生產環境。

對於祕密管理服務，我們建議使用參數存儲的組合，即AWS Systems Manager，和AWS Secrets Manager：

- 使用參數存儲可以管理密鑰和其他參數，這些參數是單個鍵值對、基於字符串、總長度短且經常訪問的參數。您可以使用AWS Key Management Service(AWS KMS) 密鑰來加密該密鑰。在參數存儲的標準層中存儲參數不收費。有關參數層的詳細信息，請參閱管理參數層（Systems Manager 文檔）。
- 使用 Secrets Manager 可以存儲以文檔形式（如多個相關鍵值對）、大於 4 KB（如數字證書）或從自動旋轉中受益的祕密。

您可以使用參數存儲 API 檢索 Secrets Manager 中存儲的密文。這允許您在使用兩種服務的組合時對應用程序中的代碼進行標準化。

管理參數存儲中的密文

1. 建立對稱AWS KMS鍵(AWS KMS文件中)。
2. 建立 SecureString 參數（Systems Manager 文檔）。參數存儲中的密文使用`SecureString`數據類型。
3. 在您的應用程序中，使用AWS適用於您編程語言的 SDK。如需 Java 範例，請參GetParameter.java(AWS 程式碼範例目錄。

若要在 Secret Manager 中管理祕密

1. 建立秘密（Secrets Manager 文檔）。

2. 從中檢索密AWS Secrets Manager在代碼中（Secrets Manager 文檔）。

   重要的是閱讀使用AWS Secrets Manager客户端緩存庫，以提高使用祕密的可用性和延遲(AWS部落格文章）。使用已經實施了最佳實踐的客户端 SDK 應加快和簡化 Secrets Manager 的使用和集成。

WKLD.04 — 防止應用程序祕密被暴露

在本地開發過程中，應用程序密文可能存儲在本地配置或代碼文件中，並意外簽入到源代碼存儲庫中。託管在公共服務提供商上的不安全的存儲庫可能會受到未經授權的訪問，並隨後發現這些機密。使用可用工具防止簽入密文。在手動代碼審核流程中納入對公開密密文的檢查。

一些常見的工具可以防止應用程序祕密簽入到源代碼存儲庫中：

- 垃圾泄漏(GitHub 儲存庫)
- 輕聲低語(GitHub 儲存庫)
- 偵測機密(GitHub 儲存庫)
- Gitit-Secret(GitHub 儲存庫)
- 鬆露豬(GitHub 儲存庫)

WKLD.05 — 檢測和修復暴露的祕密

InWKLD.03 — 使用臨時祕密或祕密管理服務 (p. 9)和WKLD.04 — 防止應用程序祕密被暴露 (p. 10)，您將採取措施來保護祕密。在此控件中，您可以部署一個解決方案，該解決方案可以檢測祕密是否繞過了這些防護措施，並且可以相應地進行修正。

亞馬遜 CodeGuru 檢查器檢測源代碼中的應用程序機密，並提供一種機制來修復和發佈 Secrets Manager 中檢測到的密文。還提供了用於從 Secrets Manager 中檢索密碼的應用程序代碼。進行成本效益分析，以確定此解決方案是否適合您的業務。作為替代方法，一些開源解決方案WKLD.04 — 防止應用程序祕密被暴露 (p. 10)為現有機密提供檢測功能。

設定 CodeGuru 與 SSecrets Manager 的審核器集成

- 使用 CodeGuru 審閱者識別硬編碼祕密和AWS Secrets Manager來保護它們(AWS博客文章和指導演練）。

WKLD.06 — 使用 Systems Manager 而不是 SSH 或 RDP

公有子網路（具有指向互聯網網關的默認路由）本質上比私有子網路, 那些沒有網際網路路由. 您可以在私有子網中運行 EC2 實例，並使用AWS Systems Manager遠程訪問實例，通過AWS Command Line Interface(AWS CLI）或AWS Management Console。然後，您可以使用AWS CLI或控制台啟動通過安全隧道連接到實例的會話，從而無需管理用於安全外殼 (SSH) 或 Windows 遠程桌面協議 (RDP) 的其他憑據。

使用會話管理器，而不是在公有子網中運行 EC2 實例、運行跳轉框或運行堡壘主機。

設定工作階段管理員

1. 確保 EC2 實例使用的是最新的操作系統亞馬遜計算機映像 (AMI)，如亞馬遜 Linux 2 或 Ubuntu。所以此 AWS Systems Manager代理程式服務器（SSM 代理程式）已預先安裝在 AMI 上。

2. 確保實例通過互聯網網關或 VPC 終端節點連接到這些地址（替換**<region>**使用適當的AWS 區域）：
   a. EC2 消息。 <region>亞 馬遜
   b. SSM。 <region>亞 馬遜
   c. ssmmessages。 <region>亞 馬遜
3. 將附加至AWS受管政策`AmazonSSMManagedInstanceCore`添加到與您的實例相關聯的 IAM 角色。

如需詳細資訊，請參閱「」設定工作階段管理員（Systems Manager 文檔）。

啟動工作階段

- 啟動工作階段（Systems Manager 文檔）。

WKLD.07 — 記錄具有敏感資料的 S3 存儲體的資料事件

在預設情況下，AWS CloudTrail捕獲管理事件，這些事件會在您的帳戶中創建、修改或刪除資源。這些管理事件不會捕獲 Amazon 簡單存儲服務存儲桶中各個對象的讀取或寫入操作。在發生安全事件期間，在單個記錄或對象級別捕獲未經授權的數據訪問或使用非常重要。使用 CloudTrail 記錄存儲敏感數據或關鍵業務數據的任何 S3 存儲桶的數據事件，以便進行檢測和審核。

Note

記錄資料事件需支付額外的費用。如需詳細資訊，請參閱 AWS CloudTrail 定價。

記錄跟蹤的資料事件

1. 登入AWS Management Console，然後開啟 CloudTrail 主控台https://console.aws.amazon.com/cloudtrail/
2. 在導覽窗格中，選擇 Trails (追蹤)，然後選擇追蹤名稱。
3. In一般詳細信息中，選擇 Edit（編輯）以更改以下設置。您無法變更追蹤的名稱。
   a. In資料事件，選擇Edit (編輯)。
   b. 對於 Data source (資料來源)，請選擇 S3。
   c. 適用於所有當前和 future 的 S3 存儲桶，清除閱讀和寫入。
   d. 在單個存儲桶選擇中，瀏覽記錄資料事件的存儲桶。您可以在此視窗中選取多個儲存貯體。選擇新增儲存貯體以記錄更多儲存貯體的資料事件。選擇記錄 Read (讀取) 事件 (例如 `GetObject`)、Write (寫) 事件 (例如 `PutObject`) 還是兩者。
   e. 選擇 Update trail (更新線索)。

WKLD.08 — 加密 Amazon EBS 磁碟區

強制加密 Amazon Elastic Block Store (Amazon EBS) 磁碟區，將其作為AWS帳戶。加密磁碟區具有與未加密磁碟區相同的每秒輸入/輸出操作 (IOPS) 性能，對延遲的影響最小。這可以防止以後出於法規遵從性或其他原因重建卷。如需詳細資訊，請參閱「」Amazon EBS 加密的必須知道的最佳實務(AWS部落格文章）。

加密 Amazon EBS 磁碟區

- 啟用預設加密（Amazon EC2 文檔）。

WKLD.09 — 加密亞馬遜 RDS 數據庫

類似於WKLD.08 — 加密 Amazon EBS 磁碟區 (p. 11)，啟用 Amazon RDS) 資料庫的加密。此加密是在底層磁碟區執行的，具有與未加密磁碟區相同的 IOPS 性能，對延遲的影響最小。如需詳細資訊，請參閱「」加密 Amazon RDS 資源概觀（Amazon RDS 文件）。

加密 RDS 資料庫執行個體

- 加密資料庫執行個體（Amazon RDS 文件）。

WKLD.10 — 將私有資源部署到私有子網中

將不需要直接 Internet 訪問的資源（如 EC2 實例、數據庫、隊列、緩存或其他基礎架構）部署到 VPC 私有子網中。私有子網在其路由表中沒有聲明到連接的 Internet 網關的路由，並且無法接收 Internet 流量。來自發往 Internet 的私有子網的流量必須通過託管AWSNAT 網關或公有子網中運行 NAT 進程的 EC2 實例。如需有關網絡隔離的詳細資訊，請參Amazon VPC 的基礎設施安全性（Amazon VPC 文件）。

創建專用資源和子網時，請使用以下做法：

- 創建私有子網時，禁用自動分配公有 IPv4 地址。
- 創建私有 EC2 實例時，禁用自動指派公有 IP。如果實例因配置錯誤而無意中將公有 IP 部署到公有子網中，這樣就可以防止分配公有 IP。

在需要時，可以將資源的子網指定為其配置的一部分。您可以部署遵循最佳實踐的 VPC，使用模塊化和可擴展的 VPC 體繫結構快速入門(AWSQuick Start)。

WKLD.11 — 使用安全組限制網絡訪問

使用安全組控制到 EC2 實例、RDS 數據庫和其他受支持的資源的流量。安全組充當虛擬防火牆，可應用於任何相關資源組，以便一致地定義允許入站和出站流量的規則。除了基於 IP 地址和端口的規則外，安全組還支持允許來自與其他安全組關聯的資源的流量的規則。例如，數據庫安全組可以具有僅允許來自應用程序服務器安全組的流量的規則。

安全組會允許所有傳出流量，但不允許入站流量。可以刪除出站流量規則，也可以配置添加其他規則來限制出站流量並允許入站流量。如果安全組沒有傳出規則，將不會允許來自您的實例的出站流量。如需詳細資訊，請參閱「」使用安全組控制到資源的流量（Amazon VPC 文件）。

在以下示例中，有三個安全組控制從 Application Load Balancer 到連接到 Amazon RDS for MySQL 數據庫的 EC2 實例的流量。

安全群組	傳入規則	傳出規則
Application Load Balancer 安全	描述：允許來自任何地方的 HTTPS 流量 類型：HTTPS 來源：任何位置-IPv4 (0.0.0.0/0)	描述：允許所有流量到任何位置 類型：所有流量 目標：任何位置-IPv4 (0.0.0.0/0)
EC2 執行個體安全	描述：允許來自 Application Load Balancer 的 HTTP 流量 類型：HTTP	描述：允許所有流量到任何位置 類型：所有流量

安全群組	傳入規則	傳出規則
	來源：Application Load Balancer 安全	目標：任何位置-IPv4 (0.0.0.0/0)
RDS 資料庫安全組	描述：允許來自 EC2 實例的 MySQL 流量 類型：MySQL 來源：EC2 執行個體安全	無傳出規則

WKLD.12 — 使用 VPC 終端節點訪問受支持的服務

在 VPC 中，需要訪問 AWS 或其他外部服務的資源需要通往互聯網的路由（`0.0.0.0/0`）或目標服務的公有 IP 地址。使用 VPC 終端節點啟用從您的 VPC 到受支持的私有 IP 路由AWS或其他服務，防止需要使用 Internet 網路網路、NAT 設備、虛擬私有網路 (VPN) 連接，或AWS Direct Connect連線。

VPC 終端節點支持附加策略和安全組，以進一步控制對服務的訪問。例如，您可以為 Amazon DynamoDB 編寫 VPC 終端節點策略，以便僅允許項目級別的操作，並阻止對 VPC 中所有資源執行表級別的操作，而無論其自身的權限策略如何。您還可以編寫 S3 存儲桶策略，以便僅允許源自特定 VPC 終端節點的請求，從而拒絕所有其他外部訪問。VPC 終端節點還可以具有一個安全組規則，例如，該規則僅限制對與應用程序特定安全組（如 Web 應用程序的業務邏輯層）關聯的 EC2 實例的訪問。

有不同種類的 VPC 終端節點。您可以使用 VPC 界面端點訪問大多數服務。DynamoDB 是使用網關端點進行訪問的。Amazon S3 支援界面端點和網關端點。建議將網關終端節點用於包含在單個AWS帳户和區域，並免費提供額外費用。如果需要更具可擴展性的訪問，例如從其他 VPC、本地網絡或不同的AWS 區域。接口終端節點會產生每小時的正常運行時間費用和每 GB 數據處理費用，這兩種費用都低於將數據發送到`0.0.0.0/0`通過AWSNAT 閘道。

有關使用 VPC 終端節點的其他信息，請參閱以下資源：

- 有關 Amazon S3 在網關和接口端點之間進行選擇的詳細資訊，請參閱為 Amazon S3 選擇 VPC 端點戰略(AWS部落格文章）。
- 建立界面端點（Amazon VPC 文件）。
- 建立閘道端點（Amazon VPC 文件）。
- 如需限制存取特定 VPC 或 VPC 端點的 S3 存儲桶政策，請參限制特定 VPC 的存取（Amazon S3 文檔）。
- 有關限制操作的 DynamoDB 終端節點策略示例，請參閱DynamoDB 的端點政策（Amazon VPC 文件）。

WKLD.13 — 所有公共網絡終端都要求使用 HTTPS

要求 HTTPS 為 Web 終端節點提供額外的可信度，允許您的終端節點使用證書來證明其身份，並確認終端節點與連接的客户端之間的所有流量都已加密。對於公共網站，這提供了更高的搜索引擎排名的額外好處。

許多AWS服務為您的資源提供公共 Web 終端節點，例如AWS Elastic Beanstalk、Amazon CloudFront、Amazon API Gateway lastic Load Balancing 和AWS Amplify。如需如何使用 HTTPS 的説明，請參以下內容：

- Elastic Beanstalk（Elastic Beanstalk 文檔）
- CloudFront（CloudFront 文件）
- Application Load Balancer(AWS知識中心)
- Classic Load Balancer(AWS知識中心)

- Amplify（Amplify 文檔）

託管於 Amazon S3 的靜態網站不支援 HTTPS。要為這些網站要求 HTTPS，您可以使用 CloudFront。公開存取以下方式提供內容的 S3 存取： CloudFront 並非必要項目。

使用 CloudFront 為 Amazon S3 託管的靜態網站提供服務

1. 使用 CloudFront 為 Amazon S3 託管的靜態網站提供服務(AWS知識中心)。
2. 如果要配置對公有 S3 存儲桶的訪問，請查看器和 CloudFront 之間需使用 HTTPS（CloudFront 文檔）。

   如果您要配置對私有 S3 存儲桶的訪問，請使用源存取身分限制存取 Amazon S3 內容（CloudFront 文檔）。

此外，除非需要與舊協議兼容，否則應將 HTTPS 端點配置為需要現代傳輸層安全 (TLS) 協議和密碼。例如，使用`ELBSecurityPolicy-FS-1-2-Res-2020-10`或可用於應用程序負載平衡器 HTTPS 偵聽器的最新策略，而不是默認`ELBSecurityPolicy-2016-08`。最新的策略要求至少 TLS 1.2、正向保密以及與現代 Web 瀏覽器兼容的強密碼。

如需 HTTPS 公有端點的可用安全政策的詳細資訊，請參：

- Classic Load Balancer 適用的預先定義 SSL 安全政策（Elastic Load Balancing）
- Application Load Balancer 的安全政策（Elastic Load Balancing）
- 檢視器和 CloudFront 之間支援的通訊協定和密碼（CloudFront 文件）

WKLD.14 — 為公共端點使用邊緣保護服務

使用邊緣保護服務，而不是直接從計算服務（如 EC2 實例或容器）提供流量服務。這在來自 Internet 的傳入流量和服務於該流量的資源之間提供了額外的安全層。這些服務可以在流量到達內部資源之前篩選不需要的流量、強制加密並應用路由或其他規則（如負載平衡）。

AWS可提供公共端點保護的服務包括AWS WAF、CloudFront、Elastic Load Balancing、API Gateway 和 Amplify 託管。在公有子網中運行基於 VPC 的服務（如 Elastic Load Balancing），作為私有子網中運行的 Web 服務資源的代理服務。

CloudFront、API Gateway 和亞馬遜路由 53 免費提供免費保護，防止第 3 層和第 4 層分佈式拒絕服務 (DDoS) 攻擊，AWS WAF可以防止第 7 層攻擊。

有關開始使用這些服務的說明可以在這裏找到：

- 入門AWS WAF(AWS網站)
- Amazon CloudFront 入門（CloudFront 文件）
- Elastic Load Balancing 入門（Elastic Load Balancing）
- API Gateway 入門（API Gateway 文檔）
- Amplify 託管入門（Amplify 文檔）

WKLD.15 — 在模板中定義安全控制並使用 CI/CD 實踐進行部署

基礎架構即代碼（iAC）是定義所有AWS服務資源和配置，您可以使用持續集成和持續交付 (CI/CD) 管道進行部署，這些管道與用來部署軟件應用程序的管道相同。iAC 服務，例如AWS CloudFormation，支援以 IAM

身分為基礎和以資源為基礎的政策和支援AWS安全服務，例如 Amazon GuardDutyAWS WAF和 Amazon VPC。將這些對象捕獲為 iAC 模板，將模板提交到源代碼存儲庫，然後使用 CI/CD 管道進行部署。

除非另有要求，請在同一存儲庫中使用應用程序代碼提交應用程序權限策略，並在單獨的代碼存儲庫和部署管道中管理常規資源策略和安全服務配置。

如需 IAC 入門的詳細資訊，請AWS，請參AWS Cloud Development Kit (AWS CDK)文件。

貢獻者

本文檔的參與者包括：

- 傑伊·邁克爾，首席解決方案架構師
- 科爾·卡利斯特拉，首席解決方案架構師
- 賈斯汀·普洛克，首席解決方案架構師
- 費薩爾·法魯克，解決方案架構師
- Nguyen，解決方案架構師
- 高級解決方案架構師 Ritik Khatwani
- 保羅·霍金斯，首席信息安全官辦公室主任

特別感謝以下人士，他們也幫助指導和審查：

- Robert Pput
- 邁克·沙利文
- 鮑勃·李 III

文件歷史記錄

下表說明本指南的重大變更。如果您想要收到 future 更新的通知，則可以訂RSS 摘要。

update-history-change	update-history-description	update-history-date
密碼政策 (p. 17)	我們更新了強密碼的建議，以使用互聯網安全中心 (CIS) 的最新指南。	2022 年 5 月 10 日
初次出版 (p. 17)	—	2022 年 4 月 13 日

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。