瞭解 IBM InfoSphere MDM Server 的安全性，第一部分：Master Data Management Server 安全性概觀

MDM Server 8 的驗證、授權及審核

等級：中級

Miguel A Ortiz, Jr. (maortiz@us.ibm.com)，IBM 軟體工程師

Lee McCallum (lmccallu@ca.ibm.com)，IBM 顧問 IT 架構設計師

2008 年 9 月 11 日

Master Data Management (MDM) 解決方案的最終目標是成爲整個企業中所有重要共享資料的授權性來源，因此，這些資訊的安全性最爲關鍵。IBM InfoSphere MDM Server 直接處理的安全性及其作業環境提供的安全性可分爲好幾個部分。本系列文章的第一部分著重於前者安全性，並詳述其中幾個元件。本系列的後續文章會詳細介紹如何使用及配置這些元件，以解決實際業務問題。

前言

InfoSphere MDM Server 的安全範圍

IBM InfoSphere MDM Server 可提供中央架構，解決企業的主要資料管理問題，包括帳戶、客戶及產品資料。在這種環境下，保護資料的機密性、完整性及可用性至關重要，而不當的資訊安全措施所帶來的風險可能會導致商業智慧毀損、信用卡被盜用、違反隱私權及法律訴訟。

本系列所有文章的軟體堆疊

所有 MDM Server 的相關討論都是關於 InfoSphere MDM Server 8.0 版及其堆疊。本文的立場爲熟悉 MDM Server 及產品手冊所使用的術語。

本文引用 "Enterprise Master Data Management: An SOA Approach to Managing Core Information"（本文的資源一節即可找到）所提到的邏輯 SOA 安全架構，其中將安全服務分爲三個層次：

- **商業安全服務**：負責完成企業的安全及隱私權目標，包括無可否認服務、法規遵循及報告等。
- **安全原則管理**：負責確保整個企業的安全原則定義和管理一致，這一層就像商業安全服務和 IT 安全服務之間的連結，範圍包括原則管理及發佈。
- **IT 安全服務**：負責提供企業所需的核心安全服務，這一層的重點包括驗證和機密服務。

本文著重討論 MDM Server 的元件，這些元件負責 MDM IT 安全服務的鑑別、授權及審核功能，這三個領域可提供進階功能，以建立使用者的身分、服務存取權，然後提供個別使用者的作業記錄。此外，本文也會概述設計 MDM 解決方案時的安全環境注意事項。

InfoSphere MDM Server 的安全圖解

爲了方便說明，本文參考圖 1 所說明的基本 MDM 交易範例。

圖 1. 簡單的 MDM 實務範例

此範例是有關一般使用者（在此案例中是 Jane Doe）與 MDM 用戶端應用程式（如客服中心）之間的互動，用戶端應用程式最後會使用 MDM Server 作爲主要資料來源。圖 1 是使用者 Jane 更新客戶 (Maria) 資料的範例。

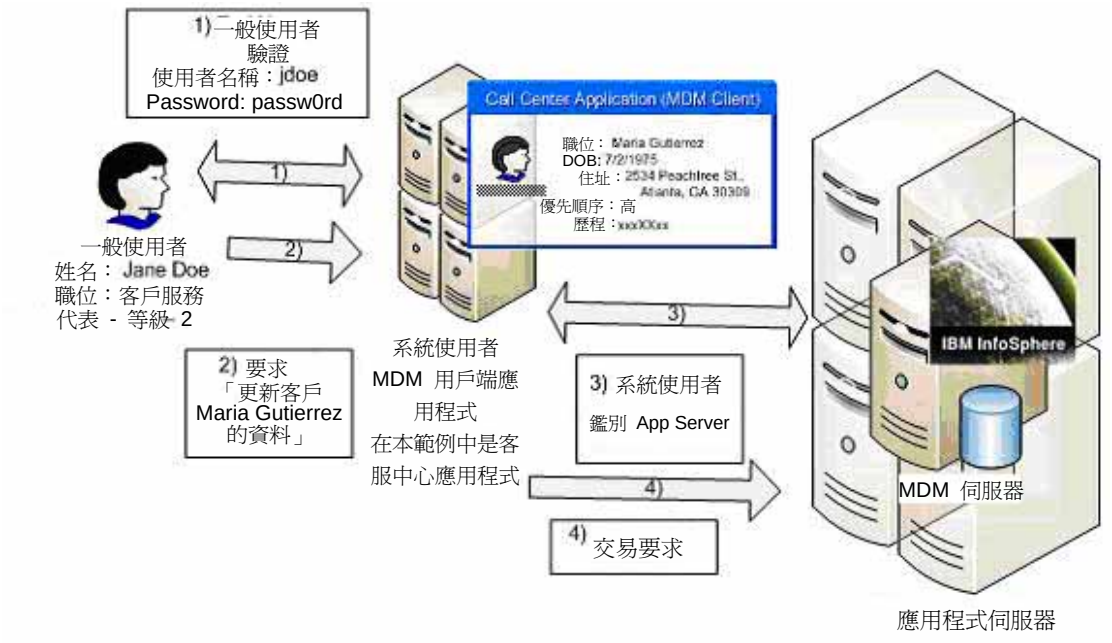
驗證及身分主張

一般使用者與系統使用者身分

在 MDM 架構中，一般使用者與系統使用者有所不同，一般使用者是指利用系統使用者而間接產生 MDM 交易的實體，此實體或許是人或系統。在本案例中，一般使用者是 Jane，也就是使用客服中心應用程式的客服人員，Jane 也許根本沒有察覺這些互動會導致呼叫 MDM Server。

在此實務範例中，客服中心應用程式（又稱爲 MDM 用戶端應用程式）就是系統使用者，系統使用者會充當一般使用者與 MDM Server 資料的橋樑，也就是一般使用者的介面應用程式，並且將使用者要求轉化爲一系列 MDM Server 交易。請注意，系統使用者與 MDM Server 之間有一種信任關係。

圖 2. 簡單的 MDM 驗證流程



一般使用者驗證

若要在 MDM 架構中進行一般使用者驗證，請記住下列事項：

- 一般使用者絕不直接與 MDM Server 互動，而是透過系統使用者進行間接互動。
- MDM Server 與系統使用者之間有一種信任關係。

基於以上兩項，MDM Server 會委託系統使用者執行充分鑑別及認證驗證。認證驗證的範例如下：使用者名稱與密碼、憑證或記號。

系統使用者鑑別

若要讓系統使用者存取所有 MDM Server 元件，就必須鑑別 J2EE 儲存器並建立可靠的通道。J2EE 儲存器是指用來管理 MDM Server 的應用程式伺服器，目前支援 Web Logic 及 WebSphere Application Server。

此外，系統使用者也必須納入 ServiceConsumer 角色，此角色可提供有限的 MDM 元件存取權。本章的授權一節會再說明此角色。

身分主張

雖然 MDM Server 委託系統使用者進行一般使用者鑑別，但 MDM Server 必須知道一般使用者的身分，才能提供交易與資料授權，在此環境中，系統使用者會根據每個交易確立一般使用者的身分。

該使用者資訊會傳送到 MDM Server，即交易訊息主文中的 DWL Control Stub，下列範例 XML 交易訊息會強調顯示此資訊，這也是圖 2 中的步驟 4。

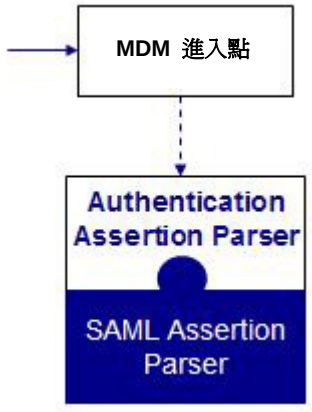
清單 1. XML 交易訊息中的 DWL Control

```
<?xml version="1.0" encoding=UTF-8"?>
<TCRMService>
        <RequestControl>
                <requestID> 504000</requestID>

                <DWLControl>
                        <requesterName>jdoe</requesterName>
                        <userRole>CallCentAppUser</userRole>
                        <userRole>CstSuppRepL2</userRole>
                </DWLControl>

        </RequestControl>
        <TCRMTx>
                <TCRMTxType>updatePerson</TCRMTxType>
                <TCRMTxObject>TCRMPersonBObj</TCRMTxObject>
                <TCRMObject>
                        <TCRMPersonBObj>
                                <PersonPartyId>111</PersonPartyID>
                                <TCRMPersonNameBObj>
                                        <GivenNameOne>Maria</GivenNameOne>
                                </TCRMPersonNameBObj>
                        </TCRMPersonBObj>
                </TCRMObject>
        </TCRMTx>
</TCRMService>
```

圖 3. 驗證主張剖析器



除了標準 DWL Control XML 節點，MDM Server 也允許在 DWL Control Stub 中插入身分記號，然後，AAP 會剖析該記號，並擷取必要資訊。AAP 的預設實作可支援 SAML 1.1，但這個自訂作業點可被取代，以支援其他記號、驗證記號或外部服務，必須注意的是，若在 MDM Server 內，預設不會驗證該主張。

即將發表的相關鑑別主張剖析器文章

本主題系列的後續文章會進一步說明鑑別主張剖析器 (AAP) 的功能。第 5 篇文章會解釋如何使用 Tivoli Federated Identity Manager 擴充 AAP 以支援並驗證其他記號。

授權

EJB 元件授權

EJB 元件授權在應用程式伺服器中加以管理及實施，也就是管理 MDM Server 的位置。透過 Web 服務或 RMI 存取 MDM Server 及順利鑑別應用程式伺服器的用戶端應用程式會賦予 ServiceConsumer 角色。

如果 MDM 用戶端應用程式要透過 Java Messaging Services (JMS) 及 WebSphere MQ (JMS/MQ) 存取 MDM Server，該 JMS/MQ 公用程式會負責驗證應用程式儲存器，以便公用程式本身確立其 Service Consumer 角色。WebSphere MQ 公用程式可能需要進一步設定其安全性，以便僅供 MDM 用戶端應用程式存取 MDM Server。

ServiceConsumer 與 ServiceProvider 角色

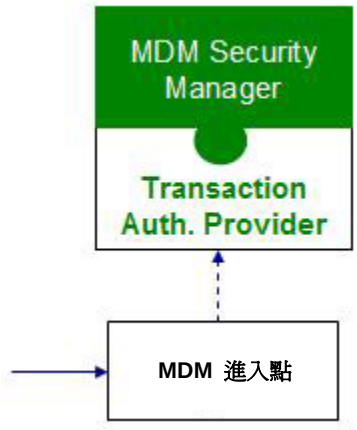
MDM Server 有兩個重要的使用者角色，即 ServiceConsumer 及 ServiceProvider。每個 MDM 進入點元件（包括 Web 服務、服務控制器及程序控制）都可以配置設定，僅針對擁有 ServiceConsumer 角色的系統使用者賦予存取權，然後，這些進入點會在轉遞交易給 MDM Server 的內容進行處理時，繼續使用 ServiceProvider 角色作爲 Run As 安全角色。

ServiceConsumer 角色可提供 MDM Server 元件的有限存取權。必須注意的是，在 MDM Server 所在的安全網域中，ServiceConsumer 角色會依預設指派給 All Authenticated。建議配置此角色，以便僅納入有合理原因要存取 MDM Server 的特定系統使用者。

交易授權

交易授權是 MDM Server 所執行的第一層授權。此程序由 Transaction Authorization Provider 元件執行，並判斷該使用者是否可以呼叫所要求的交易。依預設是透過用作 Transaction Authorization Provider 的 MDM Security Manager 來配置 MDM Server。MDM Security Manager 是 MDM Server 的豐富元件，其中包括有使用者和群組人員資訊的資料模型。此模型可直接連結 MDM Server 的 meta 資料模型，以識別使用者和群組可呼叫的交易。

圖 4. 交易授權



Transaction Authorization Provider 元件可配置來使用 LDAP 伺服器或自行建置的解決方案，而不需要 MDM Security Manager。事實上，您可配置多個交易授權提供程式來執行複雜的供應計畫。

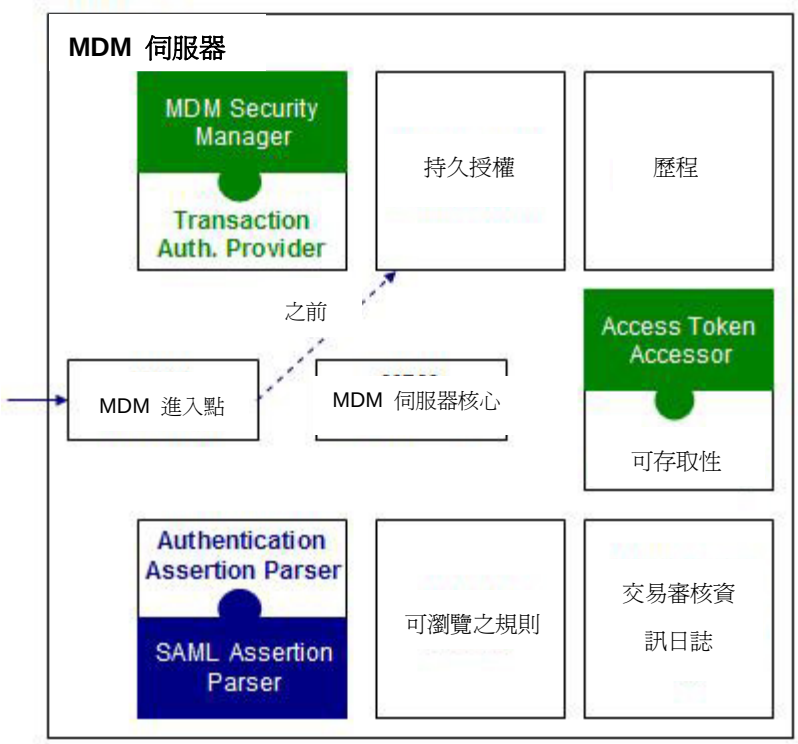
圖 5. 交易授權實作方案

若一般使用者沒有獲得呼叫此服務的授權，就會出現錯誤，同時標示該交易需要回復。

持久授權

持久授權是 MDM Server 執行的第二層授權。MDM Server 會依此確認使用者是否有權更改他們要更改的資料，然後再呼叫控制器層次的交易。例如，一般使用者 (Jane Doe) 可能可以瀏覽 Maria Gutierrez 的記錄，但 Jane 也許不能更改 Maria 的優先順序欄位。此限制是在 Persistency Entitlements 元件中配置。

圖 6. 持久授權的流程



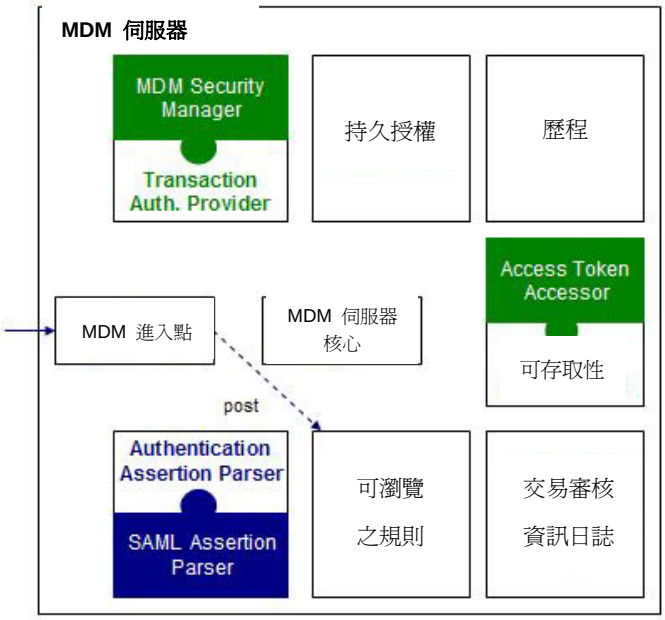
在此實務案例中，Jane 想要更新 Maria 的名稱，並且檢查 Jane 是否有權修改名稱欄位，如果 Jane 確實已獲授權，該交易就會繼續進行；若未獲授權，系統就會出現錯誤，該交易也會標示爲需要回復。

MDM Server 中可進行大量配置，以設定如何判斷該使用者可持續保存的屬性和實體。如需進一步資訊，請參閱 MDM 開發人員手冊。

可瀏覽之規則 (RoV)

RoV 是 MDM Server 中的第三層授權。此授權可執行授權程序，限制使用者在呼叫控制器層次交易後能瀏覽的記錄數量。

圖. RoV 流程

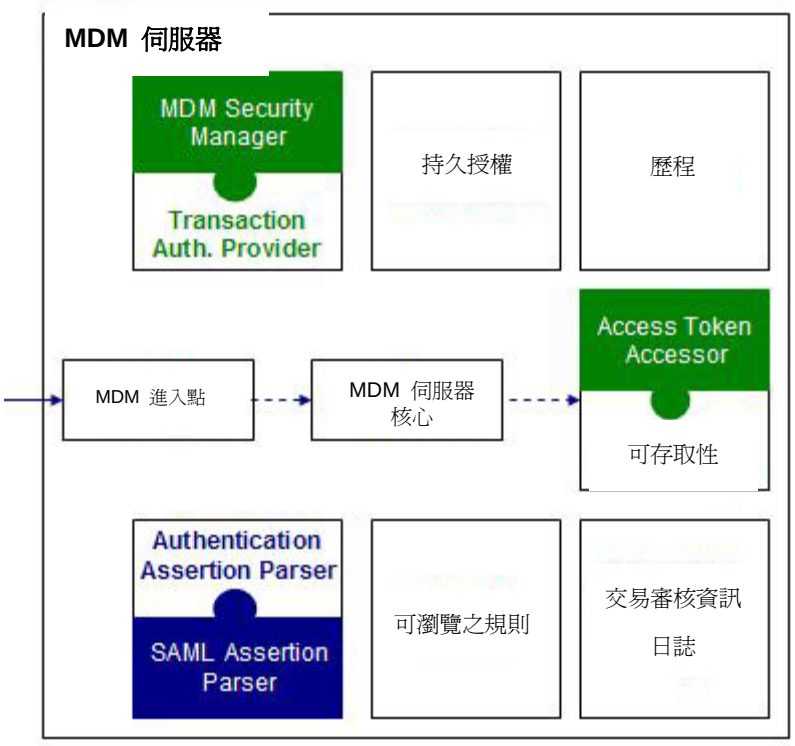


例如，身爲等級 2 的客服人員 Jane 可查看高優先順序及低優先順序的客戶，但較低等級的客服人員可能無法查看高優先順序客戶。由於所存資料有不同的機密性且組織內有各種職責角色，這對主要資料管理來說尤其重要。

存取記號

存取記號是另一種 RoV，可提供較粗略的授權層級，同時提高效能。存取記號的概念與標籤型授權控制十分類似，記號會指派給特定使用者或群組，以及特定使用者能存取的記錄，若有要求，使用者只能存取有指派相關記號的記錄。

圖 8. 存取記號的流程



例如，Jane 可能有一份由她負責的客戶名單，在此情況下，即可將記號指派給 Jane 及其客戶記錄。如果 Jane 要求查看所有客戶，就只會顯示她的客戶名稱。

與使用者的群組成員資格相反，記號資訊不會在 DWL Control 中傳送。此資訊會保留在 MDM Server 資料庫中，透過每個交易進行存取。此外，指派記號給群組或記錄也不是 MDM Server 的職責。

審核

交易審核資訊日誌 (TAIL)

交易獲得充分授權後，TAIL 就會記錄日誌項目。您可配置 MDM Server 將所有外部（控制器層次）和內部（元件層次）交易，以及主要概念資訊（如實體 ID）記錄到應用程式的作業表格，十分方便。您可使用 MDM Server Administration 服務中的 Transaction Audit Information 畫面來配置事件日誌，其中會提供服務根據使用者類型、交易類型、實體及日期範圍來擷取此資訊。所記錄的交易和資料可在 TAIL 資料模型中加以配置。

如需 TAIL 的詳細資訊，請參閱 "IBM InfoSphere Master Data Management Server (MDM Server) System Management Guide."

歷程

最後，確認交易後就會呼叫一或多個資料庫觸發程序，以更新相關歷程表格，並儲存變更記錄及變更者資料等。在變更時留下變更記錄可在需要時重建記錄，而且必要時也能進行特定記錄的完整審核追蹤。

結論

MDM Server 可提供許多功能來進行主要資料架構的驗證、授權及審核。MDM Server 可進行複雜的自訂作業，是配置現有元件與服務（如使用存取記號）及全面取代這些元件與服務以因應特定複雜需求的平台，如提供整合 LDAP 的自訂剖析器來提供交易使用者驗證。本主題系列的後續文章會介紹自訂及配置應用程式安全功能的不同方法。

資源

學習

- "Enterprise Master Data Management: An SOA Approach to Managing Core Information"：取得架構設計師、技術分析師、顧問、解決方案設計師及資深 IT 決策者等實務工作人員適用的授權性、跨平台 MDM 技術參考手冊。
- "IBM InfoSphere MDM Server Information Center" 立即查看產品安全功能的豐富資訊，如上述每個元件的詳細配置資訊。
- 如需這些議題及其他技術主題的相關書籍，請瀏覽技術書局。
- developerWorks 資訊管理區：進一步瞭解 DB2，立即查看技術說明文件、技術文章、教育訓練、下載檔案及產品資訊等。
- 最新的 developerWorks 技術活動及網路廣播。

取得產品與技術

- 使用 IBM 試用軟體建置您的下一個開發專案，可直接從 developerWorks 下載。

討論

- 瀏覽 developerWorks 部落格並參與 developerWorks 社群。

作者簡介

Miguel A. Ortiz, Jr. 是 IBM Austin 實驗室 Information Platform and Solutions 團隊的軟體工程師，主要負責 MDM Server 安全性、IP 產品整合。

Lee McCallum 是 IBM Toronto 實驗室的顧問 IT 架構設計師，主要負責設計及領導 MDM Server 的功能開發，著重在 Product Doma
貢獻在建置 J2EE 平台的產品，但空閒時也涉足其他技術領域，如最近的 Ruby on Rails。