設定Insight

OnCommand Insight

NetApp
April 01, 2024

目錄

設定Insight

若要設定Insight、您必須啟動Insight授權、設定資料來源、定義使用者和通知、啟用備份、以及執行任何必要的進階組態步驟。

安裝完這個系統後、您必須執行下列設定工作OnCommand Insight ：

- 安裝Insight授權。
- 在Insight中設定您的資料來源。
- 設定使用者帳戶。
- 設定您的電子郵件。
- 視需要定義SNMP、電子郵件或系統記錄通知。
- 啟用Insight資料庫的每週自動備份。
- 執行任何必要的進階組態步驟、包括定義註釋和臨界值。

存取Web UI

安裝OnCommand Insight 完支援後、您必須安裝授權、然後設定Insight來監控環境。若要這麼做、您可以使用網頁瀏覽器存取Insight Web UI。

步驟

1. 執行下列其中一項：
   - 在Insight伺服器上開啟Insight：

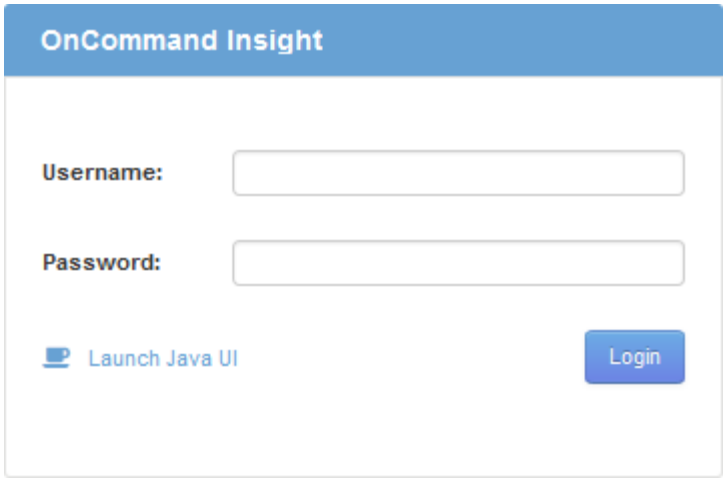
     ```
     https://fqdn
     ```

   - 從任何其他位置開啟Insight：

     ```
     https://fqdn:port
     ```

     連接埠號碼為443或安裝Insight伺服器時所設定的其他連接埠。如果您未在URL中指定連接埠號碼、則連接埠號碼預設為443。

   將顯示「The」（還原）對話方塊OnCommand Insight



：

2. 輸入您的使用者名稱和密碼、然後按一下*登入*。

   如果已安裝授權、則會顯示資料來源設定頁面。

> 不活動30分鐘的Insight瀏覽器工作階段會逾時、系統會自動將您登出系統。為了增加安全性、建議您在登出Insight後關閉瀏覽器。

安裝Insight授權

從NetApp收到內含Insight授權金鑰的授權檔案後、您可以使用設定功能同時安裝所有授權。

關於這項工作

Insight授權金鑰儲存在中 `.txt` 或 `.lcn` 檔案：

步驟

1. 在文字編輯器中開啟授權檔案、然後複製文字。
2. 在瀏覽器中開啟Insight。
3. 在Insight工具列上、按一下*管理*。
4. 按一下*設定*。
5. 按一下「授權」索引標籤。
6. 按一下 * 更新授權 * 。
7. 將授權金鑰文字複製到*授權*文字方塊中。
8. 選取*更新（最常見）*作業。
9. 按一下「 * 儲存 * 」。
10. 如果您使用的是Insight Consumption授權模式、則必須勾選「傳送使用資訊」區段中的「允許傳送使用資訊給**NetApp**」方塊。您的環境必須正確設定並啟用Proxy。

完成後

安裝授權之後、您可以執行下列組態工作：

- 設定資料來源。
- 建立OnCommand Insight 不一樣的使用者帳戶。

不需要授權**OnCommand Insight**

支援Insight Server特定功能的授權OnCommand Insight 。

- 探索

  探索是支援庫存的基本Insight授權。您必須擁有「激發需求」授權才能使用OnCommand Insight 此功能、而且「激發需求」授權必須與至少一個「保證」、「執行」或「規劃」授權配對。

- 保證

  Assure授權可支援保證功能、包括全域和SAN路徑原則、以及違規管理。Assure授權也可讓您檢視及管理弱點。

- 執行

  執行授權可支援資產頁面、儀表板小工具、查詢等的效能監控、以及管理效能原則和違規。

- 計畫

  「規劃」授權可支援規劃功能、包括資源使用量和配置。

- 主機使用率套件

  主機使用率授權可支援主機和虛擬機器上的檔案系統使用率。

- 報告製作

  「報告撰寫」授權可支援其他作者進行報告。此授權需要Plan授權。

下列各項均獲授權以供每年或永久使用OnCommand Insight ：

- 受監控容量TB、可用於探索、保證、規劃、執行模組
- 依主機使用率套件的主機數
- 依「報告撰寫」所需的Cognos專業作者額外單位數

授權金鑰是為每位客戶產生的一組獨特字串。您可以向OnCommand Insight 您的銷售代表取得授權金鑰。

您安裝的授權可控制軟體提供的下列選項：

- 探索

  取得及管理庫存（基礎）

監控變更並管理庫存原則

- 保證

  檢視及管理SAN路徑原則與違規

  檢視及管理弱點

  檢視及管理工作與移轉

- 計畫

  檢視及管理要求

  檢視及管理擱置的工作

  檢視及管理違反預約的情況

  檢視及管理連接埠平衡違規

- 執行

  監控效能資料、包括儀表板小工具、資產頁面和查詢中的資料

  檢視及管理效能原則與違規行為

下表提供管理使用者和非管理員使用者執行授權時及不含執行授權的功能詳細資料。

功能（管理員）	含Perform授權	不含執行授權
應用程式	是的	無效能資料或圖表
虛擬機器	是的	無效能資料或圖表
Hypervisor	是的	無效能資料或圖表
主機	是的	無效能資料或圖表
資料存放區	是的	無效能資料或圖表
VMDK	是的	無效能資料或圖表
內部Volume	是的	無效能資料或圖表
Volume	是的	無效能資料或圖表
儲存資源池	是的	無效能資料或圖表

磁碟	是的	無效能資料或圖表
儲存設備	是的	無效能資料或圖表
儲存節點	是的	無效能資料或圖表
網路	是的	無效能資料或圖表
交換器連接埠	是的	無效能資料或圖表；「Port Errors」（連接埠錯誤）顯示「'N/A'」
儲存連接埠	是的	是的
NPV連接埠	是的	無效能資料或圖表
交換器	是的	無效能資料或圖表
NPV交換器	是的	無效能資料或圖表
qtree	是的	無效能資料或圖表
配額	是的	無效能資料或圖表
路徑	是的	無效能資料或圖表
區域	是的	無效能資料或圖表
區域成員	是的	無效能資料或圖表
一般裝置	是的	無效能資料或圖表
磁帶	是的	無效能資料或圖表
遮罩	是的	無效能資料或圖表
iSCSI工作階段	是的	無效能資料或圖表
ICSI網路入口網站	是的	無效能資料或圖表
搜尋	是的	是的

管理	是的	是的
儀表板	是的	是的
小工具	是的	部分可用（僅提供資產、查詢和管理小工具）
違規儀表板	是的	隱藏
資產儀表板	是的	部分可用（隱藏儲存IOPS和VM IOPS小工具）
管理效能原則	是的	隱藏
管理註釋	是的	是的
管理註釋規則	是的	是的
管理應用程式	是的	是的
查詢	是的	是的
管理企業實體	是的	是的

功能	使用者：含Perform授權	來賓-含執行授權	使用者-不含執行授權	來賓-不含執行授權
資產儀表板	是的	是的	部分可用（隱藏儲存IOPS和VM IOPS小工具）	部分可用（隱藏儲存IOPS和VM IOPS小工具）
自訂儀表板	僅檢視（不建立、編輯或儲存選項）	僅檢視（不建立、編輯或儲存選項）	僅檢視（不建立、編輯或儲存選項）	僅檢視（不建立、編輯或儲存選項）
管理效能原則	是的	隱藏	隱藏	隱藏
管理註釋	是的	隱藏	是的	隱藏
管理應用程式	是的	隱藏	是的	隱藏
管理企業實體	是的	隱藏	是的	隱藏

查詢	是的	僅限檢視與編輯（無儲存選項）	是的	僅限檢視與編輯（無儲存選項）

設定及管理使用者帳戶

使用者帳戶、使用者驗證和使用者授權、可透過兩種方式加以定義和管理：在Microsoft Active Directory（第2版或第3版）LDAP（輕量型目錄存取傳輸協定）伺服器、OnCommand Insight 或是在內部的非功能性使用者資料庫中。為每個人設定不同的使用者帳戶、可讓您控制存取權限、個人偏好設定和責任歸屬。請使用具有此作業管理員權限的帳戶。

開始之前

您必須完成下列工作：

- 安裝OnCommand Insight 您的不一樣授權。
- 為每位使用者分配唯一的使用者名稱。
- 確定要使用的密碼。
- 指派正確的使用者角色。

> 安全性最佳實務做法要求系統管理員設定主機作業系統、以防止非系統管理員/標準使用者互動登入。

步驟

1. 在瀏覽器中開啟Insight。
2. 在Insight工具列上、按一下*管理*。
3. 按一下*設定*。
4. 選取「**使用者」索引標籤。
5. 若要建立新的使用者、請按一下*「Actions」（動作）按鈕、然後選取「Add user*」（新增使用者*）。

   您可以輸入*姓名*、密碼、*電子郵件*地址、然後選取其中一個使用者*角色*做為系統管理員、使用者或訪客。

6. 若要變更使用者資訊、請從清單中選取使用者、然後按一下使用者說明右側的*編輯使用者帳戶*符號。
7. 若要從OnCommand Insight 這個系統移除使用者、請從清單中選取使用者、然後按一下使用者說明右側的*刪除使用者帳戶*。

結果

當使用者登入OnCommand Insight 到NetApp時、伺服器會先嘗試透過LDAP驗證（如果已啟用LDAP）。如果OnCommand Insight 無法在LDAP伺服器上找到使用者、則會在本機Insight資料庫中搜尋。

Insight使用者角色

每個使用者帳戶都會被指派三種可能的權限等級之一。

- Guest可讓您登入Insight並檢視各種頁面。
- 使用者允許所有來賓層級權限、以及存取Insight作業、例如定義原則和識別一般裝置。使用者帳戶類型不允許您執行資料來源作業、也不允許新增或編輯您自己以外的任何使用者帳戶。
- 系統管理員可讓您執行任何作業、包括新增使用者及管理資料來源。

*最佳實務做法：*為使用者或訪客建立大多數帳戶、以限制擁有系統管理員權限的使用者人數。

設定LDAP的Insight

必須在公司LDAP網域中設定使用輕量型目錄存取傳輸協定（LDAP）設定OnCommand Insight 。

在將Insight設定為搭配LDAP或安全LDAP（LDAPS）使用之前、請先記下公司環境中的Active Directory組態。Insight設定必須符合貴組織LDAP網域組態中的設定。在設定Insight與LDAP搭配使用之前、請先檢閱下列概念、並洽詢您的LDAP網域管理員、以瞭解您環境中要使用的適當屬性。

對於所有安全的Active Directory（即LDAPS）使用者、您必須使用與憑證中定義完全相同的AD伺服器名稱。您無法使用IP位址進行安全的AD登入。

> 支援透過Microsoft Active Directory伺服器或Azure AD的LDAP和LDAPS OnCommand Insight 。其他LDAP實作可能仍可運作、但尚未符合Insight資格。本指南中的程序假設您使用的是Microsoft Active Directory版本2或3 LDAP（輕量型目錄存取傳輸協定）。

使用者主要名稱屬性：

LDAP使用者主要名稱屬性（userPrincipalName）是Insight做為使用者名稱屬性的用途。使用者主要名稱保證在Active Directory（AD）樹系中具有全域唯一性、但在許多大型組織中、使用者的主要名稱可能並不立即顯而易見或已知。您的組織可能會針對主要使用者名稱使用User Principal Name屬性以外的其他選項。

以下是使用者主要名稱屬性欄位的一些替代值：

- * sAMAccountName*

  此使用者屬性是舊版Windows 2000 NT使用者名稱、這是大多數使用者習慣登入其個人Windows機器的方式。這在整個AD樹系中並不保證是全域唯一的。

  > SamAccountName對User主體名稱屬性區分大小寫。

- 郵件

  在使用MS Exchange的AD環境中、此屬性是終端使用者的主要電子郵件地址。這應該在整個AD樹系中具有全域唯一性（也適用於終端使用者）、不同於其userPrincipalName屬性。郵件屬性不存在於大多數非MS Exchange環境中。

- 推薦

LDAP參照是網域控制器向用戶端應用程式指出它沒有所要求物件的複本（或更精確地說、 它不會保留目錄樹狀結構中該物件所在的區段（如果實際上存在）、並提供用戶端較有可能保留該物件的位置。用戶端會使用參照做為DNS搜尋網域控制器的基礎。理想情況下、參照一律會參照確實包含物件的網域控制器。不過、雖然通常不會花很長時間來發現物件不存在、並通知用戶端、但參照網域控制器仍有可能產生另一個參照。

SamAccountName通常比使用者主要名稱更受歡迎。SamAccountName在網域中是唯一的（雖然在網域樹系中可能不是唯一的）、但它是使用者通常用於登入的字串網域（例如、*NetApp\username*）。辨別名稱是樹系中的唯一名稱、但使用者通常不知道。

在同一個網域的Windows系統部分、您可以隨時開啟命令提示字元、然後輸入set以尋找適當的網域名稱（USERDOMAIN=）。然後OCI登入名稱將會是 `USERDOMAIN\sAMAccountName`。

如需網域名稱* mydomain.x.y.z.com、請使用 `DC=x,DC=y,DC=z,DC=com` 在Insight的Domain（網域）欄位中。

連接埠：

LDAP的預設連接埠為389、LDAPS的預設連接埠為636

LDAPS的一般URL： `ldaps://<ldap_server_host_name>:636`

記錄位於：`\\<install directory>\SANscreen\wildfly\standalone\log\ldap.log`

根據預設、Insight會預期下列欄位中所註明的值。如果Active Directory環境中有這些變更、請務必在Insight LDAP組態中加以變更。

角色屬性
成員
郵件屬性
郵件
辨別名稱屬性
區分名稱
推薦
追蹤

群組：

若要驗證OnCommand Insight 使用者在支援對象架構和DWH伺服器中具有不同存取角色、您必須在Active Directory中建立群組、並在OnCommand Insight 支援對象架構和DWH伺服器中輸入這些群組名稱。下列群組名

稱僅為範例、您在Insight中為LDAP設定的名稱必須符合為Active Directory環境設定的名稱。

Insight Group	範例
Insight伺服器管理員群組	insight.server.admins
Insight系統管理員群組	Insight。管理員
Insight使用者群組	insight.users
Insight Guest群組	Insight、訪客
報告管理員群組	INSIGHT。report.管理員
報告專業作者群組	insight.report.proauthors
報告作者群組	insight.report.business.authors
報告使用者群組	INSIGHT。report.business。消費者
報告收件者群組	INSIGHT。report.Recipients

使用**LDAP**設定使用者定義

若要從OnCommand Insight LDAP伺服器設定使用者驗證和授權的功能（OCI）、您必須在LDAP伺服器中定義OnCommand Insight 為「支援伺服器管理員」。

開始之前

您必須知道已在LDAP網域中針對Insight設定的使用者和群組屬性。

對於所有安全的Active Directory（即LDAPS）使用者、您必須使用與憑證中定義完全相同的AD伺服器名稱。您無法使用IP位址進行安全的AD登入。

關於這項工作

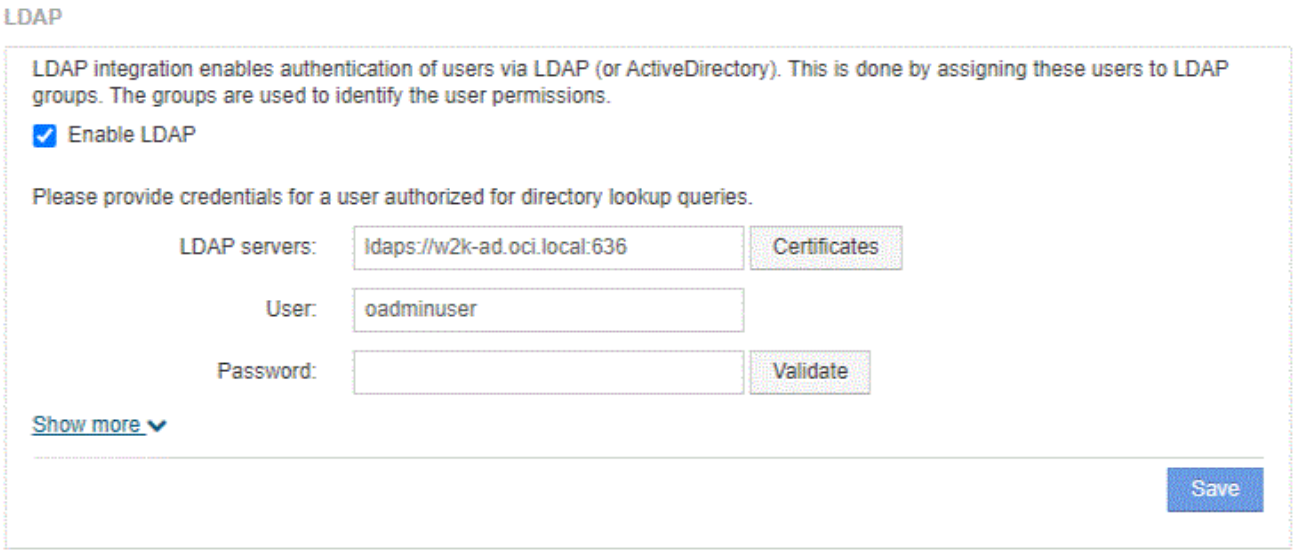
支援透過Microsoft Active Directory伺服器的LDAP和LDAPS OnCommand Insight 。其他LDAP實作可能仍可運作、但尚未符合Insight資格。此程序假設您使用的是Microsoft Active Directory版本2或3 LDAP（輕量型目錄存取傳輸協定）。

LDAP使用者與本機定義的使用者一起顯示在*管理*>功能表：設定[使用者]清單中。

步驟

1. 在Insight工具列上、按一下*管理*。
2. 按一下*設定*。
3. 按一下「使用者」索引標籤。

4. 捲動至LDAP區段、如下所示。



5. 按一下*「啟用LDAP*」以允許LDAP使用者驗證與授權。
6. 填寫欄位：

   - `LDAP servers`：Insight接受以逗號分隔的LDAP URL列表。Insight會嘗試連線至提供的URL、但不驗證LDAP傳輸協定。

     若要匯入LDAP憑證、請按一下*憑證*、然後自動匯入或手動尋找憑證檔案。

     用於識別LDAP伺服器的IP位址或DNS名稱通常是以下列格式輸入：

     ```
     ldap://<ldap-server-address>:port
     ```

     或者、如果使用預設連接埠：

     ```
     ldap://<ldap-server-address>
     ```

   + 在此欄位中輸入多個LDAP伺服器時、請確定每個項目都使用正確的連接埠號碼。

   - `User name`：輸入授權用於LDAP伺服器上目錄查詢的使用者認證。
   - `Password`：輸入上述使用者的密碼。若要在LDAP伺服器上確認此密碼、請按一下*驗證*。

7. 如果您想更精確地定義此LDAP使用者、請按一下*顯示更多*、然後填入所列屬性的欄位。

   這些設定必須符合LDAP網域中設定的屬性。如果您不確定要輸入這些欄位的值、請洽詢Active Directory管理員。

   - 管理員群組

     LDAP群組、適用於具有Insight Administrator權限的使用者。預設為 `insight.admins`。

- 使用者群組

  LDAP群組、適用於具有Insight使用者權限的使用者。預設為 `insight.users`。

- 來賓群組

  LDAP群組、適用於具有Insight Guest權限的使用者。預設為 `insight.guests`。

- 伺服器管理員群組

  LDAP群組、適用於具有Insight Server Administrator權限的使用者。預設為 `insight.server.admins`。

- 超時

  在逾時之前等待LDAP伺服器回應的時間長度（以毫秒為單位）。預設值為2、000、在所有情況下都足夠、不應修改。

- 網域

  應從LDAP節點OnCommand Insight 開始尋找LDAP使用者。通常這是組織的頂層網域。例如：

  ```
  DC=<enterprise>,DC=com
  ```

- 使用者主要名稱屬性

  用於識別LDAP伺服器中每個使用者的屬性。預設為 `userPrincipalName`是全球獨一無二的。嘗試將此屬性的內容與上述提供的使用者名稱配對OnCommand Insight 。

- 角色屬性

  可識別使用者符合指定群組的LDAP屬性。預設為 `memberOf`。

- 郵件屬性

  用於識別使用者電子郵件地址的LDAP屬性。預設為 `mail`。如果您想訂閱OnCommand Insight 可從下列網站取得的報告、此功能非常實用：Insight會在每位使用者第一次登入時取回使用者的電子郵件地址、之後不會再尋找。

  > 如果使用者的電子郵件地址在LDAP伺服器上變更、請務必在Insight中更新。

- 辨別名稱屬性

  識別使用者辨別名稱的LDAP屬性。預設為 `distinguishedName`。

8. 按一下「 * 儲存 * 」。

變更使用者密碼

擁有系統管理員權限的使用者可以變更OnCommand Insight 本機伺服器上所定義之任何使

用者帳戶的密碼。

開始之前

下列項目必須已完成：

- 通知所有登入您正在修改之使用者帳戶的人員。
- 此變更之後要使用的新密碼。

關於這項工作

使用此方法時、您無法變更透過LDAP驗證的使用者密碼。

步驟

1. 以系統管理員權限登入。
2. 在Insight工具列上、按一下*管理*。
3. 按一下*設定*。
4. 按一下「使用者」索引標籤。
5. 找出顯示您要修改之使用者帳戶的列。
6. 按一下使用者資訊右側的*編輯使用者帳戶*。
7. 輸入新的*密碼*、然後在驗證欄位中再次輸入。
8. 按一下「 * 儲存 * 」。

編輯使用者定義

擁有系統管理員權限的使用者可以編輯使用者帳戶、以變更OnCommand Insight 電子郵件地址或角色、以利執行功能、包括功能更新或報告功能。

開始之前

判斷OnCommand Insight 需要變更的使用者帳戶類型（例如、DWH或組合）。

關於這項工作

對於LDAP使用者、您只能使用此方法修改電子郵件地址。

步驟

1. 以系統管理員權限登入。
2. 在Insight工具列上、按一下*管理*。
3. 按一下*設定*。
4. 按一下「使用者」索引標籤。
5. 找出顯示您要修改之使用者帳戶的列。

6. 在使用者資訊的右側、按一下*編輯使用者帳戶*圖示。
7. 進行必要的變更。
8. 按一下「 * 儲存 * 」。

刪除使用者帳戶

任何擁有系統管理員權限的使用者都可以刪除使用者帳戶、無論是不再使用（用於本機使用者定義）、或是強制OnCommand Insight 下次使用者登入（用於LDAP使用者）時重新探索使用者資訊。

步驟

1. 以系統管理員權限登入OnCommand Insight 支援功能。
2. 在Insight工具列上、按一下*管理*。
3. 按一下*設定*。
4. 按一下「使用者」索引標籤。
5. 找出顯示您要刪除之使用者帳戶的列。
6. 在使用者資訊右側、按一下*刪除使用者帳戶*「* x *」圖示。
7. 按一下「 * 儲存 * 」。

設定登入警告訊息

支援系統管理員設定自訂文字訊息、供使用者登入時顯示OnCommand Insight 。

步驟

1. 若要在OnCommand Insight The傳達訊息的伺服器中設定訊息：
   a. 瀏覽至選單：管理[疑難排解>進階疑難排解>進階設定]。
   b. 在文字區域輸入您的登入訊息。
   c. 按一下*用戶端顯示登入警告訊息*核取方塊。
   d. 按一下「 * 儲存 * 」。

      所有使用者登入時都會顯示此訊息。
2. 若要在資料倉儲（DWH）和報告（Cognos）中設定訊息：
   a. 瀏覽至*系統資訊*、然後按一下*登入警告*索引標籤。
   b. 在文字區域輸入您的登入訊息。
   c. 按一下「 * 儲存 * 」。

      此訊息會在DWH和Cognos報告登入時顯示給所有使用者。

Insight Security

7.3.1版OnCommand Insight 的功能介紹安全功能、可讓Insight環境以增強的安全性運作。這些功能包括加密、密碼雜湊、以及變更加密和解密密碼的內部使用者密碼和金鑰配對的能力。您可以在Insight環境中的所有伺服器上管理這些功能。

Insight的預設安裝包括安全性組態、讓您環境中的所有站台共用相同的金鑰和相同的預設密碼。為了保護敏感資料、NetApp建議您在安裝或升級後變更預設金鑰和擷取使用者密碼。

資料來源加密密碼儲存在Insight Server資料庫中。伺服器具有公開金鑰、當使用者在WebUI資料來源組態頁面中輸入密碼時、會加密這些密碼。伺服器沒有解密儲存在伺服器資料庫中的資料來源密碼所需的私密金鑰。只有擷取單位（Lau、Rau）擁有解密資料來源密碼所需的資料來源私密金鑰。

重新輸入伺服器金鑰

使用預設金鑰會在您的環境中引進安全性弱點。根據預設、資料來源密碼會加密儲存在Insight資料庫中。加密時會使用所有Insight安裝通用的金鑰。在預設組態中、傳送至NetApp的Insight資料庫包含理論上可由NetApp解密的密碼。

變更擷取使用者密碼

使用預設的「擷取」使用者密碼會在您的環境中引入安全性弱點。所有擷取設備都會使用「擷取」使用者與伺服器通訊。使用預設密碼的Raus理論上可以使用預設密碼連線至任何Insight伺服器。

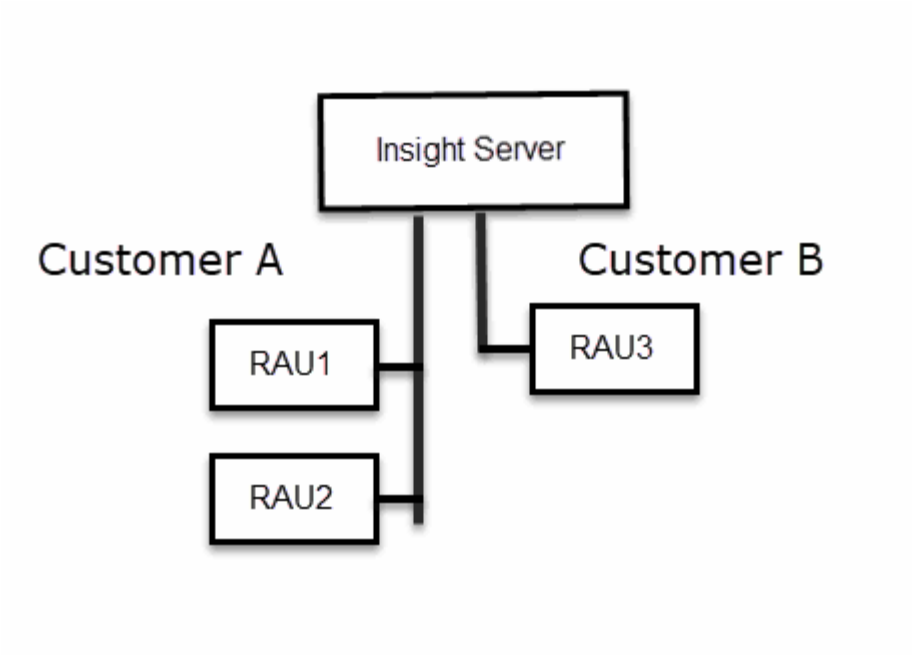
升級與安裝考量

如果Insight系統包含非預設的安全性組態（您已重新輸入或變更密碼）、則必須備份安全性組態。安裝新軟體、或在某些情況下升級軟體、會將系統還原為預設的安全組態。當系統恢復為預設組態時、您必須還原非預設組態、系統才能正常運作。

在複雜的服務供應商環境中管理金鑰

服務供應商可以託管OnCommand Insight 多個收集資料的客戶。這些金鑰可防止Insight伺服器上的多個客戶未經授權存取客戶資料。每位客戶的資料都受到其特定金鑰配對的保護。

Insight實作可設定如下圖所示。



您需要在此組態中為每位客戶建立個別的金鑰。客戶A需要兩個Raus相同的金鑰。客戶B需要一組金鑰。

您將採取哪些步驟來變更客戶A的加密金鑰：

1. 遠端登入裝載RAU1的伺服器。
2. 啟動安全性管理工具。
3. 選取變更加密金鑰以取代預設金鑰。
4. 選取備份以建立安全性組態的備份壓縮檔。
5. 遠端登入裝載RAU2的伺服器。
6. 將安全組態的備份壓縮檔複製到RAU2。
7. 啟動安全性管理工具。
8. 將安全備份從RAU1還原至目前的伺服器。

變更客戶B加密金鑰的步驟：

1. 遠端登入裝載RAU3的伺服器。
2. 啟動安全性管理工具。
3. 選取變更加密金鑰以取代預設金鑰。
4. 選取備份以建立安全性組態的備份壓縮檔。

管理**Insight**伺服器上的安全性

。 `securityadmin` 工具可讓您管理Insight伺服器上的安全選項。安全管理包括變更密碼、產生新金鑰、儲存及還原您建立的安全組態、或將組態還原為預設設定。

關於這項工作

您可以使用 `securityadmin` 管理安全性的工具：

- Windows - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat`
- Linux - `/bin/oci-securityadmin.sh`

步驟

1. 遠端登入Insight伺服器。
2. 以互動模式啟動安全管理工具：
   - Windows - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i`
   - Linux - `/bin/oci-securityadmin.sh -i`

     系統會要求登入認證資料。
3. 輸入具有「admin」認證的帳戶使用者名稱和密碼。
4. 選取*伺服器*。

   提供下列伺服器組態選項：

   - 備份

     建立包含所有密碼和金鑰的資料保險箱備份壓縮檔、並將檔案放置在使用者指定的位置、或是下列預設位置：

     - Windows - `C:\Program Files\SANscreen\backup\vault`
     - Linux - `/var/log/netapp/oci/backup/vault`
   - 還原

     還原所建立之資料保存庫的壓縮備份。還原之後、所有密碼和金鑰都會還原為建立備份時的現有值。

     > 還原可用於同步多個伺服器上的密碼和金鑰、例如：-變更單一伺服器上的伺服器加密金鑰-建立資料庫備份-將資料庫備份還原至第二個伺服器
   - 變更加密金鑰

     變更用來加密或解密Proxy使用者密碼、SMTP使用者密碼、LDAP使用者密碼等的伺服器加密金鑰。

     > 變更加密金鑰時、您應該備份新的安全性組態、以便在升級或安裝之後還原。
   - 更新密碼

     變更Insight使用的內部帳戶密碼。畫面會顯示下列選項：

     - 內部_
     - 併購

- Cogns_admin
- dwh_internal
- 主機
- 庫存
- 根

> 有些帳戶需要在密碼變更時進行同步處理。例如、如果您變更伺服器上「擷取」使用者的密碼、則需要變更劉、Rau和DWH上「擷取」使用者的密碼以進行比對。此外、當您變更密碼時、也應該備份新的安全組態、以便在升級或安裝之後還原。

- 重設為預設值

  將金鑰和密碼重設為預設值。預設值為安裝期間提供的值。

- 退出

  結束 `securityadmin` 工具：

  a. 選擇您要變更的選項、然後依照提示進行。

管理本地採購單位的安全性

。 `securityadmin` 此工具可讓您管理本機擷取使用者（Lau）的安全選項。安全管理包括管理金鑰和密碼、儲存及還原您建立的安全組態、或將組態還原為預設設定。

開始之前

您必須擁有 `admin` 執行安全組態工作的權限。

關於這項工作

您可以使用 `securityadmin` 管理安全性的工具：

- Windows - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat`
- Linux - `/bin/oci-securityadmin.sh`

步驟

1. 遠端登入Insight伺服器。
2. 以互動模式啟動安全管理工具：
   - Windows - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i`
   - Linux - `/bin/oci-securityadmin.sh -i`

     系統會要求登入認證資料。
3. 輸入具有「admin」認證的帳戶使用者名稱和密碼。

4. 選取*本機擷取單位*以重新設定本機擷取單位安全性組態。

   畫面會顯示下列選項：

   - 備份

     建立包含所有密碼和金鑰的資料保險箱備份壓縮檔、並將檔案放置在使用者指定的位置、或是下列預設位置：

     - Windows - `C:\Program Files\SANscreen\backup\vault`
     - Linux - `/var/log/netapp/oci/backup/vault`

   - 還原

     還原所建立之資料保存庫的壓縮備份。還原之後、所有密碼和金鑰都會還原為建立備份時的現有值。

     > 還原可用於同步多個伺服器上的密碼和金鑰、例如：-變更Lau上的加密金鑰-建立資料庫備份-將資料庫備份還原至每個Raus

   - 變更加密金鑰

     變更用於加密或解密裝置密碼的AU加密金鑰。

     > 變更加密金鑰時、您應該備份新的安全性組態、以便在升級或安裝之後還原。

   - 更新密碼

     變更「擷取」使用者帳戶的密碼。

     > 有些帳戶需要在密碼變更時進行同步處理。例如、如果您變更伺服器上「擷取」使用者的密碼、則需要變更劉、Rau和DWH上「擷取」使用者的密碼以進行比對。此外、當您變更密碼時、也應該備份新的安全組態、以便在升級或安裝之後還原。

   - 重設為預設值

     將擷取使用者密碼和擷取使用者加密金鑰重設為預設值、預設值為安裝期間提供的值。

   - 退出

     結束 `securityadmin` 工具：

5. 選擇您要設定的選項、然後依照提示進行。

管理Rau的安全性

。 `securityadmin` 工具可讓您管理Rous上的安全選項。您可能需要備份或還原資料保險箱組態、變更加密金鑰、或更新擷取單位的密碼。

關於這項工作

您可以使用 `securityadmin` 管理安全性的工具：

- Windows - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat`
- Linux - `/bin/oci-securityadmin.sh`

更新Lau安全性組態的其中一種案例是、在伺服器上變更該使用者的密碼時、更新「擷取」使用者密碼。所有的Raus和Lau都使用與伺服器「擷取」使用者相同的密碼來與伺服器通訊。

「擷取」使用者僅存在於Insight伺服器上。當Rau或Lau連線至伺服器時、會以該使用者的身分登入。

請使用下列步驟來管理Rau上的安全性選項：

步驟

1. 遠端登入執行Rau的伺服器
2. 以互動模式啟動安全管理工具：
   - Windows - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i`
   - Linux - `/bin/oci-securityadmin.sh -i`

     系統會要求登入認證資料。
3. 輸入具有「admin」認證的帳戶使用者名稱和密碼。

   系統會顯示Rau功能表。

   - 備份

     建立包含所有密碼和金鑰的資料保險箱備份壓縮檔、並將檔案放置在使用者指定的位置、或是下列預設位置：

     - Windows - `C:\Program Files\SANscreen\backup\vault`
     - Linux - `/var/log/netapp/oci/backup/vault`
   - 還原

     還原所建立之資料保存庫的壓縮備份。還原之後、所有密碼和金鑰都會還原為建立備份時的現有值。

     > 還原可用於同步多個伺服器上的密碼和金鑰、例如：-變更一部伺服器上的加密金鑰-建立資料庫備份-將資料庫備份還原至第二部伺服器
   - 變更加密金鑰

     變更用來加密或解密裝置密碼的Rau加密金鑰。

     > 變更加密金鑰時、您應該備份新的安全性組態、以便在升級或安裝之後還原。
   - 更新密碼

變更「擷取」使用者帳戶的密碼。

> 有些帳戶需要在密碼變更時進行同步處理。例如、如果您變更伺服器上「擷取」使用者的密碼、則需要變更劉、Rau和DWH上「擷取」使用者的密碼以進行比對。此外、當您變更密碼時、也應該備份新的安全組態、以便在升級或安裝之後還原。

- 重設為預設值

  將加密金鑰和密碼重設為預設值。預設值為安裝期間提供的值。

- 退出

  結束 `securityadmin` 工具：

管理資料倉儲的安全性

。 `securityadmin` 工具可讓您管理資料倉儲伺服器上的安全選項。安全管理包括更新DWH伺服器上內部使用者的內部密碼、建立安全組態備份、或將組態還原為預設設定。

關於這項工作

您可以使用 `securityadmin` 管理安全性的工具：

- Windows - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat`
- Linux - `/bin/oci-securityadmin.sh`

步驟

1. 遠端登入資料倉儲伺服器。
2. 以互動模式啟動安全管理工具：
   - Windows - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i`
   - Linux - `/bin/oci-securityadmin.sh -i`

     系統會要求登入認證資料。
3. 輸入具有「admin」認證的帳戶使用者名稱和密碼。

   系統會顯示資料倉儲的安全管理功能表：

   - 備份

     建立包含所有密碼和金鑰的資料保險箱備份壓縮檔、並將檔案放置在使用者指定的位置、或是預設位置：

     - Windows - `C:\Program Files\SANscreen\backup\vault`
     - Linux - `/var/log/netapp/oci/backup/vault`
   - 還原

還原所建立之資料保存庫的壓縮備份。還原之後、所有密碼和金鑰都會還原為建立備份時的現有值。

> 還原可用於同步多個伺服器上的密碼和金鑰、例如：-變更一部伺服器上的加密金鑰-建立資料庫備份-將資料庫備份還原至第二部伺服器
>
> +

- 變更加密金鑰

  變更用於加密或解密密碼的DWH加密金鑰、例如連接器密碼和SMPT密碼。

- 更新密碼

  變更特定使用者帳戶的密碼。

  - 內部_
  - 併購
  - Cogns_admin
  - dwh
  - dwh_internal
  - dwhuser
  - 主機
  - 庫存
  - 根

> 當您變更dwhuser、hosts、inventory或root密碼時、您可以選擇使用SHA-256密碼雜湊。此選項需要所有存取帳戶的用戶端都使用SSL連線。

+

- 重設為預設值

  將加密金鑰和密碼重設為預設值。預設值為安裝期間提供的值。

- 退出

  結束 `securityadmin` 工具：

變更**OnCommand Insight** 內部使用者密碼

安全性原則可能需要您在OnCommand Insight 您的環境中變更密碼。某部伺服器上的某些密碼存在於環境中的不同伺服器上、需要您變更兩部伺服器上的密碼。例如、當您變更Insight Server上的「Inventory」使用者密碼時、您必須符合Data倉儲伺服器Connector上針對該Insight Server所設定的「Inventory」使用者密碼。

開始之前

> 變更密碼之前、您應該先瞭解使用者帳戶的相依性。若未更新所有必要伺服器上的密碼、Insight元件之間的通訊將會失敗。

關於這項工作

下表列出Insight Server的內部使用者密碼、並列出具有相依密碼的Insight元件、這些元件必須符合新密碼。

Insight Server密碼	必要變更
內部_	
併購	劉羅
dwh_internal	資料倉儲
主機	
庫存	資料倉儲
根	

下表列出Data倉儲的內部使用者密碼、並列出Insight元件、這些元件的相依密碼必須與新密碼相符。

資料倉儲密碼	必要變更
Cogns_admin	
dwh	
Dwh_internal（使用伺服器連接器組態UI變更）	Insight伺服器
dwhuser	
主機	
庫存（使用伺服器連接器組態UI變更）	Insight伺服器
根	

*變更DWH伺服器連線組態Ui*中的密碼

下表列出了劉的使用者密碼、並列出了Insight元件、這些元件的相依密碼必須與新密碼相符。

劉密碼	必要變更
併購	Insight Server、Rau

使用伺服器連線組態**UI**變更「庫存」和「**dwh_internal**」密碼

如果您需要變更「Inventory」或「dwh_internal」密碼、以符合Insight伺服器上的密碼、請使用Data倉儲UI。

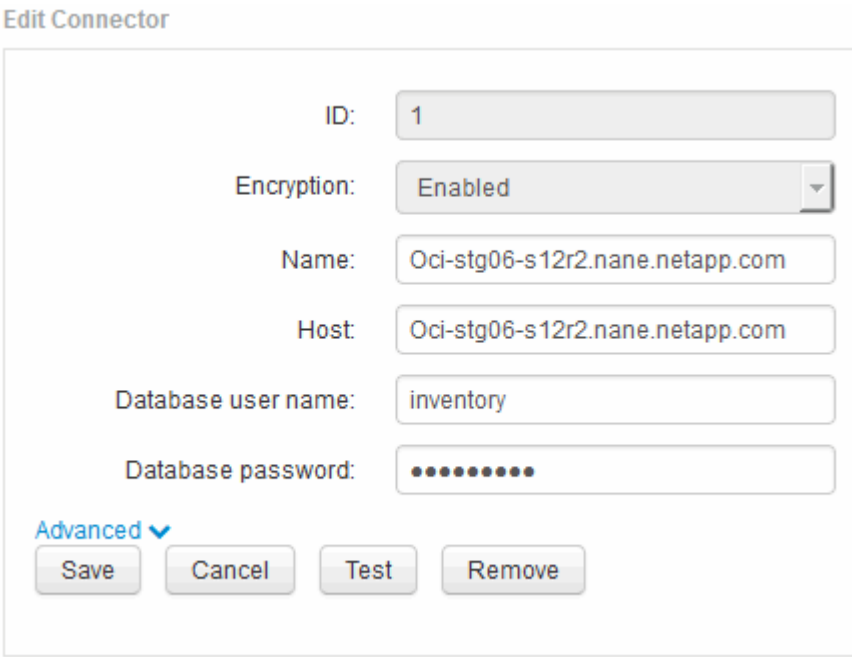
開始之前

您必須以系統管理員身分登入才能執行此工作。

步驟

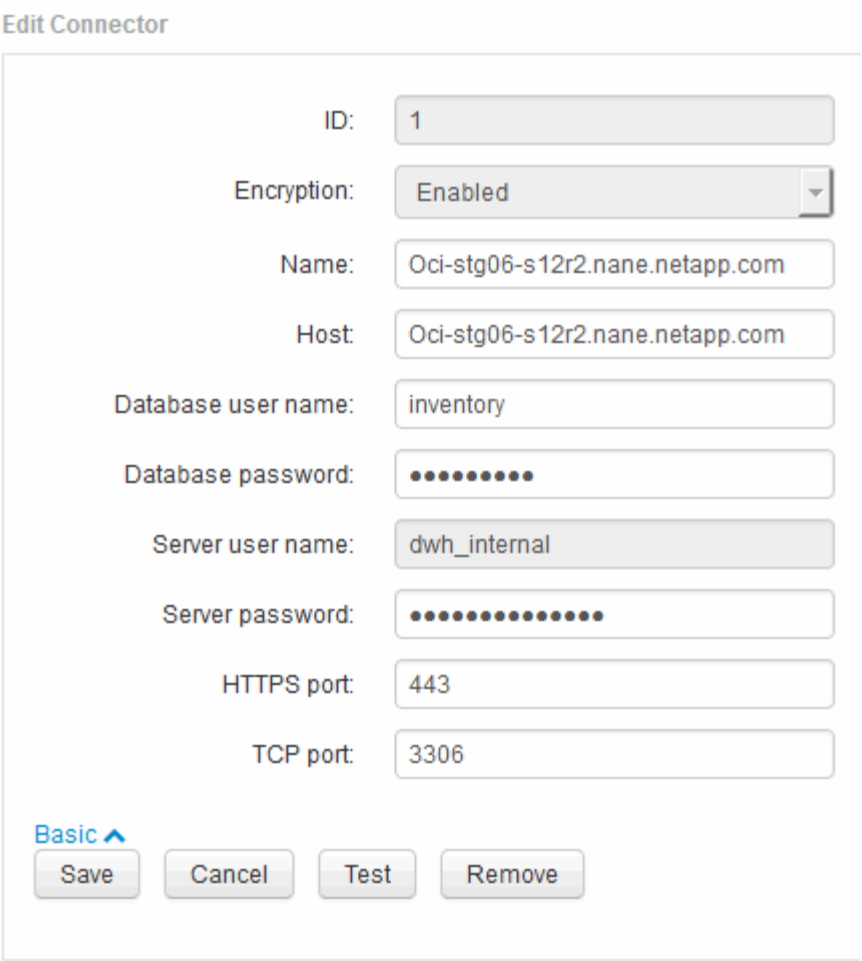
1. 登入資料倉儲入口網站： https://hostname/dwh、其中、主機名稱是OnCommand Insight 安裝了「IsorData倉儲」的系統名稱。
2. 在左側的導覽窗格中、按一下* Connectors *。

   此時將顯示*編輯連接器*畫面。



3. 在「資料庫密碼」欄位中輸入新的「'inventory'」密碼。
4. 按一下「儲存」
5. 若要變更「dwh_internal」密碼、請按一下*進階。*

   此時會顯示Edit Connector Advanced（編輯連接器進階）畫面。



6. 在*伺服器密碼*欄位中輸入新密碼：
7. 按一下儲存。

使用「**ODBC**管理」工具變更**dwh**密碼

當您在Insight伺服器上變更dwh使用者的密碼時、也必須在Data倉儲伺服器上變更密碼。您可以使用「ODBC資料來源管理員」工具來變更資料倉儲上的密碼。

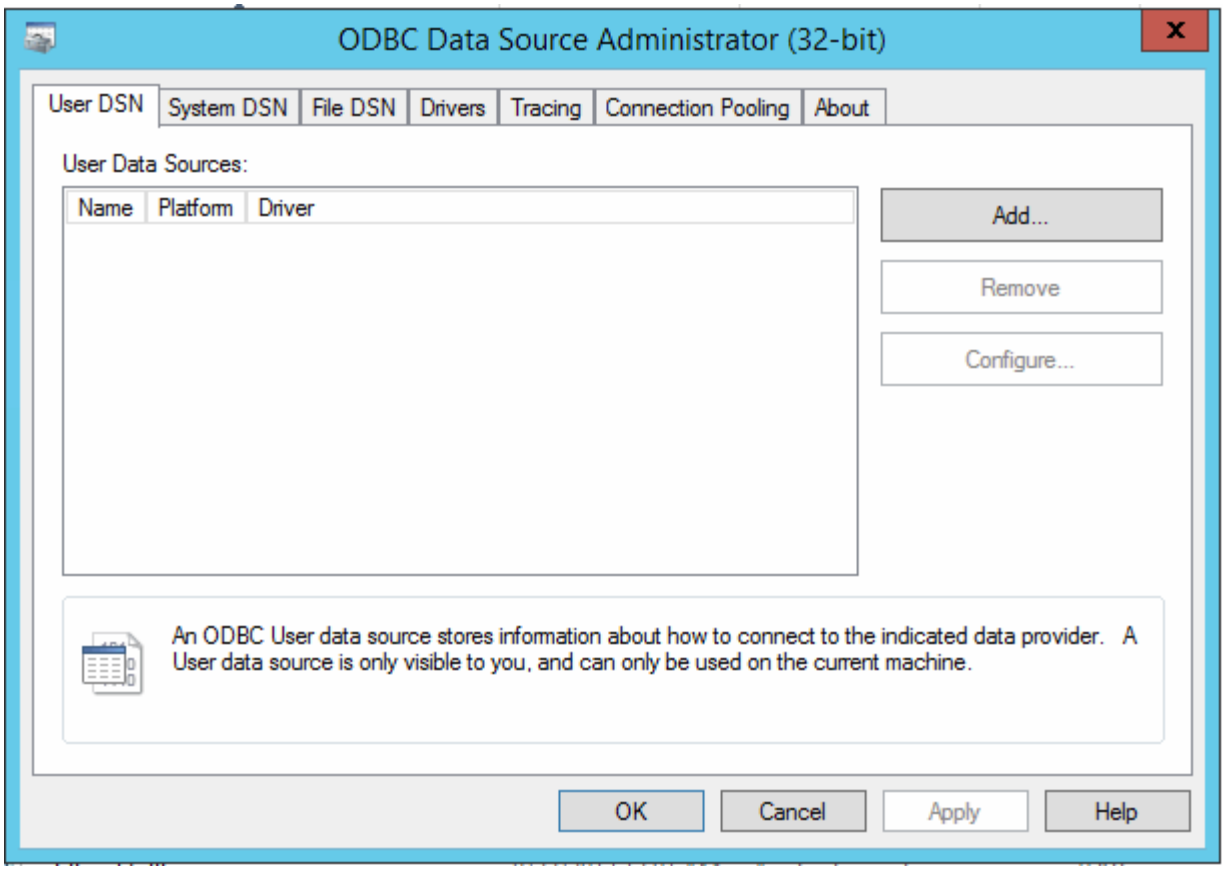
開始之前

您必須使用具有系統管理員權限的帳戶、遠端登入Data倉儲伺服器。

步驟

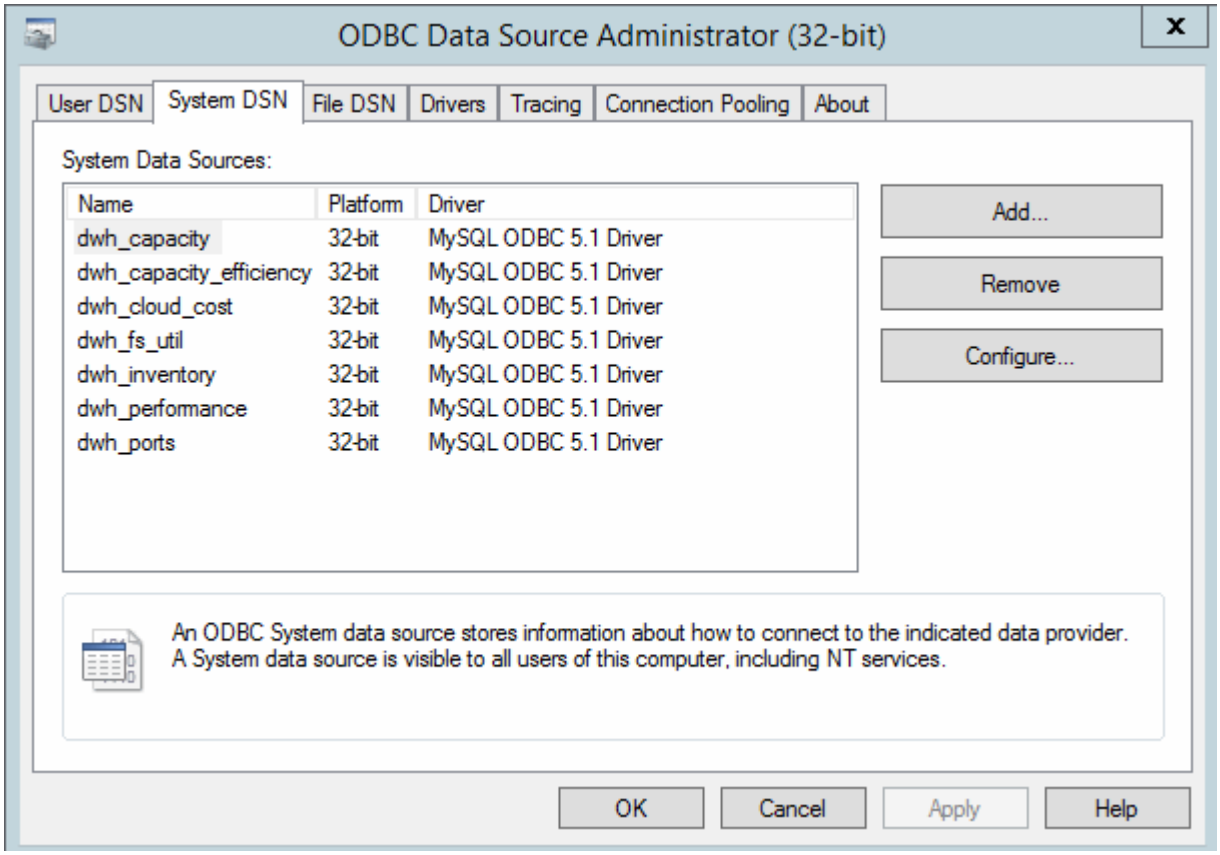
1. 遠端登入裝載該資料倉儲的伺服器。
2. 存取位於的「ODBC行政」工具 `C:\Windows\SysWOW64\odbcad32.exe`

   系統會顯示「ODBC資料來源管理員」畫面。



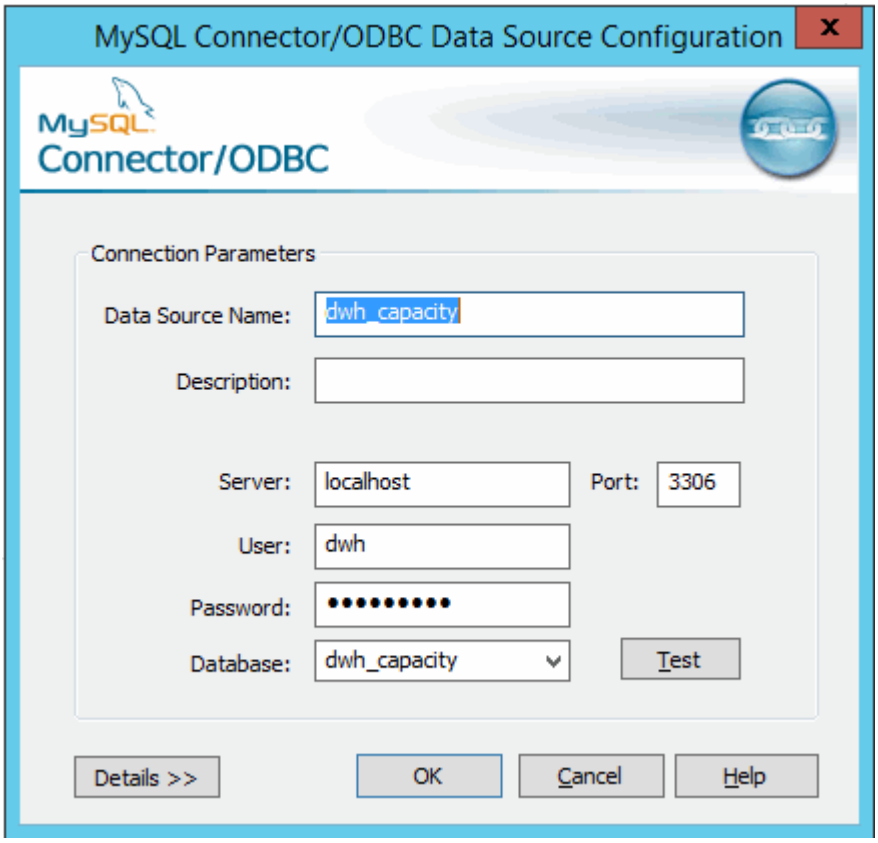
3. 單擊*系統DSN*

系統資料來源隨即顯示。



4. 從OnCommand Insight 清單中選取一個「支援資料來源」。
5. 按一下「設定」

   此時會顯示「Data來源組態」畫面。



6. 在*密碼*欄位中輸入新密碼。

智慧卡與憑證登入支援

支援使用智慧卡（CAC）和憑證來驗證登入Insight伺服器的使用者OnCommand Insight 。您必須設定系統才能啟用這些功能。

設定系統以支援CAC和憑證之後、瀏覽OnCommand Insight 至新的階段作業時、瀏覽器會顯示原生對話方塊、提供使用者可選擇的個人憑證清單。這些憑證會根據OnCommand Insight 由受到該伺服器信任的CA所發行的一組個人憑證進行篩選。通常只有單一選擇。根據預設、如果只有一個選項、Internet Explorer就會跳過此對話方塊。

> 對於CAC使用者、智慧卡包含多個憑證、其中只有一個可與信任的CA相符。的CAC憑證 `identification` 應使用。

如需最新的CAC和憑證指示、請參閱下列知識庫文章（需要支援登入）：

- "如何設定OnCommand Insight 通用存取卡（CAC）驗證以供使用"
- "如何設定OnCommand Insight 適用於《支援不支援資料倉儲》的通用存取卡（CAC）驗證"
- "如何建立及匯入已簽署的憑證授權單位（CA）憑證至OnComand Insight及OnCommand Insight 《Data Warehouse 7.3.x》"
- "如何在OnCommand Insight 安裝在Windows主機上的Se.7.3.x內建立自我簽署的憑證"
- "如何將Cognos憑證授權單位（CA）簽署的憑證匯入OnCommand 到EWdatawarehouse 7.3.3及更新版本"

設定主機以進行智慧卡和憑證登入

您必須修改OnCommand Insight 支援Smart Card（CAC）和憑證登入的整套主機組態。

開始之前

- 必須在系統上啟用LDAP。
- LDAP `User principal account name` 屬性必須符合包含使用者ID的LDAP欄位。

如需最新的CAC和憑證指示、請參閱下列知識庫文章（需要支援登入）：

- "如何設定OnCommand Insight 通用存取卡（CAC）驗證以供使用"
- "如何設定OnCommand Insight 適用於《支援不支援資料倉儲》的通用存取卡（CAC）驗證"
- "如何建立及匯入已簽署的憑證授權單位（CA）憑證至OnComand Insight及OnCommand Insight 《Data Warehouse 7.3.x》"
- "如何在OnCommand Insight 安裝在Windows主機上的Se.7.3.x內建立自我簽署的憑證"
- "如何將Cognos憑證授權單位（CA）簽署的憑證匯入OnCommand 到EWdatawarehouse 7.3.3及更新版本"

步驟

1. 使用 `regedit` 用於修改中登錄值的公用程式 `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun2.0\SANscreen Server\Parameters\Java`：
   a. 變更JVM_Option `DclientAuth=false` 至 `DclientAuth=true.`
2. 備份Keystore檔案： `C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
3. 開啟命令提示字元以指定 `Run as administrator`
4. 刪除自行產生的憑證： `C:\Program Files\SANscreen\java64\bin\keytool.exe -delete -alias "ssl certificate" -keystore C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
5. 產生新的憑證： `C:\Program Files\SANscreen\java64\bin\keytool.exe -genkey -alias "alias_name" -keyalg RSA -sigalg SHA1withRSA -keysize 2048 -validity 365`

```
-keystore "C:\Program
Files\SANscreen\wildfly\standalone\configuration\server.keystore" -dname
"CN=commonName,OU=orgUnit,O=orgName,L=localityNameI,S=stateName,C=countryName"
```

6. 產生憑證簽署要求（CSR）：`C:\Program Files\SANscreen\java64\bin\keytool.exe -certreq -sigalg SHA1withRSA -alias "alias_name" -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -file C:\temp\server.csr"`
7. 在步驟6中傳回CSR之後、匯入憑證、然後以Base -64格式匯出憑證、並將其放入其中 `"C:\temp" named servername.cer`。
8. 從Keystore擷取憑證：`C:\Program Files\SANscreen\java64\bin\keytool.exe -v -importkeystore -srckeystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -srcalias "alias_name" -destkeystore "C:\temp\file.p12" -deststoretype PKCS12`
9. 從p12檔案擷取私密金鑰：`openssl pkcs12 -in "C:\temp\file.p12" -out "C:\temp\servername.private.pem"`
10. 將您在步驟7中匯出的Base 64憑證與私密金鑰合併：`openssl pkcs12 -export -in "<folder>\<certificate>.cer" -inkey "C:\temp\servername.private.pem" -out "C:\temp\servername.new.p12" -name "servername.abc.123.yyy.zzz"`
11. 將合併的憑證匯入Keystore：`C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -destkeystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -srckeystore "C:\temp\servername.new.p12" -srcstoretype PKCS12 -alias "alias_name"`
12. 匯入根憑證：`C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -file "C:\<root_certificate>.cer" -trustcacerts -alias "alias_name"`
13. 將根憑證匯入server.trustore：`C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.trustore" -file "C:\<email_certificate>.cer" -trustcacerts -alias "alias_name"`
14. 匯入中繼憑證：`C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.trustore" -file "C:\<intermediate_certificate>.cer" -trustcacerts -alias "alias_name"`

    對所有中繼憑證重複此步驟。

15. 在LDAP中指定與此範例相符的網域。
16. 重新啟動伺服器。

設定用戶端以支援智慧卡和憑證登入

用戶端機器需要中介軟體和瀏覽器修改、才能使用智慧卡和登入憑證。已使用智慧卡的客戶不應要求對其用戶端機器進行額外的修改。

開始之前

如需最新的CAC和憑證指示、請參閱下列知識庫文章（需要支援登入）：

- "如何設定OnCommand Insight 通用存取卡（CAC）驗證以供使用"
- "如何設定OnCommand Insight 適用於《支援不支援資料倉儲》的通用存取卡（CAC）驗證"
- "如何建立及匯入已簽署的憑證授權單位（CA）憑證至OnComand Insight及OnCommand Insight 《Data Warehouse 7.3.x》"
- "如何在OnCommand Insight 安裝在Windows主機上的Se.7.3.x內建立自我簽署的憑證"
- "如何將Cognos憑證授權單位（CA）簽署的憑證匯入OnCommand 到EWdatawarehouse 7.3.3及更新版本"

關於這項工作

以下是一般用戶端組態需求：

- 安裝Smart Card中介軟體、例如ActivClient（請參閱
- 修改IE瀏覽器（請參閱
- 修改Firefox瀏覽器（請參閱

在**Linux**伺服器上啟用**CAC**

在Linux OnCommand Insight 支援伺服器上啟用CAC需要進行一些修改。

步驟

1. 瀏覽至 `/opt/netapp/oci/conf/`
2. 編輯 `wildfly.properties` 並變更的值 `CLIENT_AUTH_ENABLED` 至「真」
3. 匯入下的「root憑證」 `/opt/netapp/oci/wildfly/standalone/configuration/server.keystore`
4. 重新啟動伺服器

設定資料倉儲以進行智慧卡和憑證登入

您必須修改OnCommand Insight 「支援智慧卡（CAC）」和「憑證登入」的「支援資料倉儲」組態。

開始之前

- 必須在系統上啟用LDAP。
- LDAP `User principal account name` 屬性必須符合包含使用者政府ID號碼的LDAP欄位。

  儲存在政府核發之CAC上的一般名稱（CN）通常採用下列格式： `first.last.ID`。對於某些LDAP欄位、例如 `sAMAccountName`、格式太長。對於這些欄位OnCommand Insight 、只會從CNS擷取ID號碼。

如需最新的CAC和憑證指示、請參閱下列知識庫文章（需要支援登入）：

- "如何設定OnCommand Insight 通用存取卡（CAC）驗證以供使用"
- "如何設定OnCommand Insight 適用於《支援不支援資料倉儲》的通用存取卡（CAC）驗證"
- "如何建立及匯入已簽署的憑證授權單位（CA）憑證至OnComand Insight及OnCommand Insight 《Data Warehouse 7.3.x》"
- "如何在OnCommand Insight 安裝在Windows主機上的Se.7.3.x內建立自我簽署的憑證"
- "如何將Cognos憑證授權單位（CA）簽署的憑證匯入OnCommand 到EWdatawarehouse 7.3.3及更新版本"

步驟

1. 使用RegEdit修改中的登錄值 `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun2.0\SANscreen Server\Parameters\Java`

   a. 變更JVM_Option `-DclientAuth=false` 至 `-DclientAuth=true`。

   若為Linux、請修改 `clientAuth` 參數輸入 `/opt/netapp/oci/scripts/wildfly.server`

2. 將憑證授權單位（CA）新增至資料倉儲信任庫：

   a. 在命令視窗中、前往 `..\SANscreen\wildfly\standalone\configuration`。

   b. 使用 `keytool` 列出信任CA的公用程式： `C:\Program Files\SANscreen\java64\bin\keytool.exe -list -keystore server.trustore -storepass changeit`

      每行的第一個字表示CA別名。

   c. 如有必要、請提供CA憑證檔案、通常是 `.pem` 檔案：若要將客戶的CA納入資料倉儲信任的CA、請前往 `..\SANscreen\wildfly\standalone\configuration` 並使用 `keytool` 匯入命令： `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore server.trustore -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

      my_alias通常是容易識別中CA的別名`keytool -list` 營運。

3. 在伺服器上OnCommand Insight `wildfly/standalone/configuration/standalone-full.xml` 檔案必須透過將驗證用戶端更新為中的「要求的」來修改 `/subsystem=undertow/server=default-server/https-listener=default-https`以啟用CAC。登入Insight伺服器並執行適當的命令：

作業系統	指令碼
Windows	wildfly \bin\enableCACforRemoteEJB.bat <install dir>
Linux	/opp/NetApp/OCI /萬用里/賓/enableCACforRemoteEJB.sh

執行指令碼之後、請等到重新載入wildfly伺服器完成之後、再繼續下一步。

4. 重新啟動OnCommand Insight 伺服器。

設定Cognos以登入智慧卡和憑證（OnCommand Insight 從版本號到版本號7.3.9）

您必須修改OnCommand Insight 「支援Cognos伺服器的智慧卡（CAC）和憑證登入」的「資料倉儲」組態。

開始之前

此程序適用於執行OnCommand Insight VMware 7.3.5到7.3.9的系統。

> 如需最新的CAC和憑證指示、請參閱下列知識庫文章（需要支援登入）：
>
> - "如何設定OnCommand Insight 通用存取卡（CAC）驗證以供使用"
> - "如何設定OnCommand Insight 適用於《支援不支援資料倉儲》的通用存取卡（CAC）驗證"
> - "如何建立及匯入已簽署的憑證授權單位（CA）憑證至OnComand Insight及OnCommand Insight 《Data Warehouse 7.3.x》"
> - "如何在OnCommand Insight 安裝在Windows主機上的Se.7.3.x內建立自我簽署的憑證"
> - "如何將Cognos憑證授權單位（CA）簽署的憑證匯入OnCommand 到EWdatawarehouse 7.3.3及更新版本"

步驟

1. 將憑證授權單位（CA）新增至Cognos受託者。
   a. 在命令視窗中、前往 `..\SANscreen\cognos\analytics\configuration\certs\`
   b. 使用 `keytool` 列出信任CA的公用程式： `..\..\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass NoPassWordSet`

      每行的第一個字表示CA別名。

   c. 如果不存在適當的檔案、請提供CA憑證檔案、通常是 `.pem` 檔案：
   d. 若要將客戶的CA納入OnCommand Insight 可靠的可靠CA、請前往 `..\SANscreen\cognos\analytics\configuration\certs\`。
   e. 使用 `keytool` 匯入的公用程式 `.pem` 檔案： `..\..\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

      `my_alias` 通常是容易識別中CA的別名`keytool -list` 營運。

   f. 當系統提示輸入密碼時、請輸入 `NoPassWordSet`。
   g. 答 `yes` 當系統提示您信任憑證時。
2. 若要啟用CAC模式、請執行 `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`
3. 若要停用CAC模式、請執行 `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`

設定Cognos以登入智慧卡和憑證（OnCommand Insight 更新版本：

您必須修改OnCommand Insight 「支援Cognos伺服器的智慧卡（CAC）和憑證登入」的「資料倉儲」組態。

開始之前

此程序適用於執行OnCommand Insight 支援更新版本的系統。

> 如需最新的CAC和憑證指示、請參閱下列知識庫文章（需要支援登入）：
>
> - "如何設定OnCommand Insight 通用存取卡（CAC）驗證以供使用"
> - "如何設定OnCommand Insight 適用於《支援不支援資料倉儲》的通用存取卡（CAC）驗證"
> - "如何建立及匯入已簽署的憑證授權單位（CA）憑證至OnComand Insight及OnCommand Insight 《Data Warehouse 7.3.x》"
> - "如何在OnCommand Insight 安裝在Windows主機上的Se.7.3.x內建立自我簽署的憑證"
> - "如何將Cognos憑證授權單位（CA）簽署的憑證匯入OnCommand 到EWdatawarehouse 7.3.3及更新版本"

步驟

1. 將憑證授權單位（CA）新增至Cognos受託者。
   a. 在命令視窗中、前往 `..\SANscreen\cognos\analytics\configuration\certs\`
   b. 使用 `keytool` 列出信任CA的公用程式： `..\..\ibm-jre\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass NoPassWordSet`

      每行的第一個字表示CA別名。

   c. 如果不存在適當的檔案、請提供CA憑證檔案、通常是 `.pem` 檔案：
   d. 若要將客戶的CA納入OnCommand Insight 可靠的可靠CA、請前往 `..\SANscreen\cognos\analytics\configuration\certs\`。
   e. 使用 `keytool` 匯入的公用程式 `.pem` 檔案： `..\..\ibm-jre\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

      `my_alias` 通常是容易識別中CA的別名`keytool -list` 營運。

   f. 當系統提示輸入密碼時、請輸入 `NoPassWordSet`。
   g. 答 `yes` 當系統提示您信任憑證時。
2. 若要啟用CAC模式、請執行下列步驟：
   a. 使用下列步驟設定CAC登出頁面：
      - 登入Cognos入口網站（使用者必須是系統管理員群組的一部分、例如Cogns_admin）
      - （僅適用於7.3.10和7.3.11）按一下「管理」（Manage）「組態」（Configuration）「系統」（System）「安全性」（Security）

- （僅適用於7.3.10和7.3.11）在登出重新導向URL →套用下輸入cacLogout.html
- 關閉瀏覽器。

b. 執行 `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`

c. 啟動IBM Cognos服務。等待Cognos服務啟動。

3. 若要停用CAC模式、請執行下列步驟：

a. 執行 `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`

b. 啟動IBM Cognos服務。等待Cognos服務啟動。

c. （僅適用於7.3.10和7.3.11）使用下列步驟取消設定CAC登出頁面：

- 登入Cognos入口網站（使用者必須是系統管理員群組的一部分、例如Cogns_admin）
- 按一下「管理」→「組態」→「系統」→「安全性」
- 在「登出重新導向URL」→「套用」下輸入cacLogout.html
- 關閉瀏覽器。

匯入Cognos和DWH的CA簽署SSL憑證（Insight 7.3.5至7.3.9）

您可以新增SSL憑證、為Data倉儲和Cognos環境啟用增強的驗證和加密功能。

開始之前

此程序適用於執行OnCommnand Insight 7.3.5到7.3.9的系統。

> 如需最新的CAC和憑證指示、請參閱下列知識庫文章（需要支援登入）：
>
> - "如何設定OnCommand Insight 通用存取卡（CAC）驗證以供使用"
> - "如何設定OnCommand Insight 適用於《支援不支援資料倉儲》的通用存取卡（CAC）驗證"
> - "如何建立及匯入已簽署的憑證授權單位（CA）憑證至OnComand Insight及OnCommand Insight 《Data Warehouse 7.3.x》"
> - "如何在OnCommand Insight 安裝在Windows主機上的Se.7.3.x內建立自我簽署的憑證"
> - "如何將Cognos憑證授權單位（CA）簽署的憑證匯入OnCommand 到EWdatawarehouse 7.3.3及更新版本"

關於這項工作

您必須擁有管理權限才能執行此程序。

步驟

1. 建立的備份 `..\SANScreen\cognos\analytics\configuration\cogstartup.xml`。
2. 在下建立「certs」和「'csk'」資料夾的備份 `..\ SANScreen\cognos\analytics\configuration`。
3. 從Cognos產生憑證加密要求。在管理CMD視窗中、執行：

a. CD “`\Program Files\sanscreen\cognos\analytics\bin`”

b. `ThirdPartyCertificateTool.bat -java:local -c -e -p NoPassWordSet -a RSA -d “CN=FQDN,O=orgname,C=US” -r c:\temp\encryptRequest.csr`

4. 開啟 `c:\temp\encryptRequest.csr` 歸檔並複製產生的內容。
5. 將加密Request。CSR傳送至憑證授權單位（CA）以取得SSL憑證。

   請務必新增其他屬性、例如「「：DNS = FQDN」（例如、hostname.netapp.com)`"以新增SubjectAltName。Google Chrome 58版及更新版本會抱怨憑證中是否遺漏SubjectAltName。

6. 使用PKCS7格式加入根憑證、即可下載鏈結憑證

   這會下載FQDN。p7b檔案

7. 從CA取得.p7b格式的憑證。使用名稱將其標示為Cognos Webserver的憑證。
8. ThirdPartyCertificateTool.bat無法匯入整個鏈結、因此匯出所有憑證需要執行多個步驟。請依照下列步驟個別匯出鏈結：
   a. 在「加密Shell Extensions」中開啟.p7b憑證。
   b. 在左窗格中瀏覽至「憑證」。
   c. 在根CA上按一下滑鼠右鍵>「All Tasks（所有工作）」>「Export（匯出
   d. 選取Base64輸出。
   e. 輸入檔案名稱、將其識別為根憑證。
   f. 重複步驟8a到8c、分別將所有憑證匯出至.cer檔案。
   g. 將檔案命名為merginate.cer和Cogns.cer。
9. 如果您只有一個CA憑證、請忽略此步驟、否則請將root.cer和merinateX.cer合併成一個檔案。
   a. 使用「記事本」開啟mintermed.cer並複製內容。
   b. 使用「記事本」開啟root.cer、並儲存9a的內容。
   c. 將檔案另存為CA.cer。
10. 使用管理CMD提示將憑證匯入Cognos Keystore：
    a. CD「Program Files\SANSANSANSANSANSANPC\Cognos /分析\BIN'」
    b. ThirdPartyCertificateTool.bat -Java:local -I -T -r c：\temp\ca.cer

       這會將CA.cer設為根憑證授權單位。

    c. ThirdPartyCertificateTool.bat -Java:local -i -e -r c：\emp\Cogns.cer -t c：\emp\ca.cer

       這會將Cogns.cer設為由CA.cer簽署的加密憑證。

11. 開啟IBM Cognos組態。
    a. 選取「本機組態」→「安全性」→「密碼編譯」→「Cognos」
    b. 變更「Use third party CA？」 為真。
    c. 儲存組態。
    d. 重新啟動Cognos

12. 使用管理CMD提示字元、將最新的Cognos憑證匯出至Cognos。CRT：
    a. 「d:\Program Files\SANSANSANSANSANP\Java\BIN\keytool.exe」-exportcert -file 「'c:\temp\Cogns.crt」-keystore「d:\Program Files\SANSANSANSANSANsce\Cognos \analystation\configuration \certs\CAMKeystore」-storeetype PKCS12 -storeNoPassSet Word-alias加密
13. 使用管理CMD提示視窗、將「'c:\emp\Cognes.crt」匯入DWh信任區、以建立Cognos與DWH之間的SSL通訊。
    a. "d:\Program Files\SANSANSANSANSANSANp\Java\BIN\keytool.exe"-importcert -file ""c:\emp\Cognos.crt"-keystore "D:\Program Files\SANSANscove\wildfly\sonsolation\configuration \server.trustore"-storeepass changit -alias cognoscert
14. 重新啟動SANscreen 此服務。
15. 執行DWH備份、確保DWH與Cognos通訊。

匯入Cognos和DWH的CA簽署SSL憑證（Insight 7.3.10及更新版本）

您可以新增SSL憑證、為Data倉儲和Cognos環境啟用增強的驗證和加密功能。

開始之前

此程序適用於執行OnCommand Insight 支援更新版本的系統。

> 如需最新的CAC和憑證指示、請參閱下列知識庫文章（需要支援登入）：
>
> - "如何設定OnCommand Insight 通用存取卡（CAC）驗證以供使用"
> - "如何設定OnCommand Insight 適用於《支援不支援資料倉儲》的通用存取卡（CAC）驗證"
> - "如何建立及匯入已簽署的憑證授權單位（CA）憑證至OnComand Insight及OnCommand Insight 《Data Warehouse 7.3.x》"
> - "如何在OnCommand Insight 安裝在Windows主機上的Se.7.3.x內建立自我簽署的憑證"
> - "如何將Cognos憑證授權單位（CA）簽署的憑證匯入OnCommand 到EWdatawarehouse 7.3.3及更新版本"

關於這項工作

您必須擁有管理權限才能執行此程序。

步驟

1. 使用IBM Cognos組態工具來停止Cognos。關閉Cognos。
2. 建立的備份 `..\SANScreen\cognos\analytics\configuration` 和 `..\SANScreen\cognos\analytics\temp\cam\freshness` 資料夾：
3. 從Cognos產生憑證加密要求。在管理CMD視窗中、執行：
    a. CD “`\Program Files\sanscreen\cognos\analytics\bin`”
    b. `ThirdPartyCertificateTool.bat -java:local -c -e -p NoPassWordSet -a RSA -r c:\temp\encryptRequest.csr -d “CN=server.domain.com,O=NETAPP,C=US” -H`

`“server.domain.com” -I “ipaddress”`。附註：此處-H和-I是新增subectAltNames、例如DNS和IP地址。

4. 開啟 `c:\temp\encryptRequest.csr` 歸檔並複製產生的內容。
5. 輸入加密Request。CSR內容、並使用CA簽署入口網站產生憑證。
6. 使用PKCS7格式加入根憑證、即可下載鏈結憑證

   這會下載FQDN。p7b檔案

7. 從CA取得.p7b格式的憑證。使用名稱將其標示為Cognos Webserver的憑證。
8. ThirdPartyCertificateTool.bat無法匯入整個鏈結、因此匯出所有憑證需要執行多個步驟。請依照下列步驟個別匯出鏈結：
   a. 在「加密Shell Extensions」中開啟.p7b憑證。
   b. 在左窗格中瀏覽至「憑證」。
   c. 在根CA上按一下滑鼠右鍵>「All Tasks（所有工作）」>「Export（匯出
   d. 選取Base64輸出。
   e. 輸入檔案名稱、將其識別為根憑證。
   f. 重複步驟8a到8e、分別將所有憑證匯出至.cer檔案。
   g. 將檔案命名為merginate.cer和Cogns.cer。
9. 如果您只有一個CA憑證、請忽略此步驟、否則請將root.cer和merinateX.cer合併成一個檔案。
   a. 使用「記事本」開啟root.cer並複製內容。
   b. 使用「記事本」開啟mender.cer、然後附加9a的內容（中間第一和下一）。
   c. 將檔案另存為chain .cer。
10. 使用管理CMD提示將憑證匯入Cognos Keystore：
    a. CD「Program Files\SANSANSANSANSANSANPC\Cognos /分析\BIN'」
    b. ThirdPartyCertificateTool.bat -Java:local -I -t-r c：\temp\root.cer
    c. ThirdPartyCertificateTool.bat -Java:local -I -T -r c：\temp\minter.cer
    d. ThirdPartyCertificateTool.bat -Java:local -i -e -r c：\emp\Cogns.cer -t c：\emp\chain .cer
11. 開啟IBM Cognos組態。
    a. 選取「本機組態」→「安全性」→「密碼編譯」→「Cognos」
    b. 變更「Use third party CA？」 為真。
    c. 儲存組態。
    d. 重新啟動Cognos
12. 使用管理CMD提示字元、將最新的Cognos憑證匯出至Cognos。CRT：
    a. CD「'C:\Program Files\SANSANSANSANSAND"
    b. Java\BIN\keytool.exe -exportcert -file c：\temp\Cogns.crt -keystore Cognos \分析\組態\certs\CAMKeystore -storetype PKCS12 -storepass NoPassWordSet -alias加密
13. 備份DWH伺服器信任資

源`..\SANscreen\wildfly\standalone\configuration\server.trustore`

14. 使用管理CMD提示視窗、將「'c:\emp\Cognes.crt'」匯入DWH信任區、以建立Cognos與DWH之間的SSL通訊。
    a. CD「'C:\Program Files\SANSANSANSANSAND"
    b. Java\BIN\keytool.exe -importcert -file c:\emp\Cognos.crt -keystore wildfly\sisonal\configuration \server.trustore -storepass changit -alias cognos3rca
15. 重新啟動SANscreen 此服務。
16. 執行DWH備份、確保DWH與Cognos通訊。
17. 即使只變更「sSL憑證」、而且預設的Cognos憑證保持不變、仍應執行下列步驟。否則、Cognos可能會抱怨新SANscreen 的不合格證書、或無法建立DWH備份。
    a. `cd "%SANSCREEN_HOME%cognos\analytics\bin\"`
    b. `"%SANSCREEN_HOME%java64\bin\keytool.exe" -exportcert -file "c:\temp\sanscreen.cer" -keystore "%SANSCREEN_HOME%wildfly\standalone\configuration\server.keystore" -storepass changeit -alias "ssl certificate"`
    c. `ThirdPartyCertificateTool.bat -java:local -i -T -r "c:\temp\sanscreen.cer"`

    這些步驟通常是在中所述的Cognos憑證匯入程序中執行 "如何將Cognos憑證授權單位（CA）簽署的憑證匯入OnCommand 到EWdatawarehouse 7.3.3及更新版本"

設定資料倉儲以進行智慧卡和憑證登入

您必須修改OnCommand Insight 「支援智慧卡（CAC）」和「憑證登入」的「支援資料倉儲」組態。

開始之前

- 必須在系統上啟用LDAP。
- LDAP `User principal account name` 屬性必須符合包含使用者政府ID號碼的LDAP欄位。

  儲存在政府核發之CAC上的一般名稱（CN）通常採用下列格式： `first.last.ID`。對於某些LDAP欄位、例如 `sAMAccountName`、格式太長。對於這些欄位OnCommand Insight 、只會從CNS擷取ID號碼。

> 如需最新的CAC和憑證指示、請參閱下列知識庫文章（需要支援登入）：
>
> - "如何設定OnCommand Insight 通用存取卡（CAC）驗證以供使用"
> - "如何設定OnCommand Insight 適用於《支援不支援資料倉儲》的通用存取卡（CAC）驗證"
> - "如何建立及匯入已簽署的憑證授權單位（CA）憑證至OnComand Insight及OnCommand Insight 《Data Warehouse 7.3.x》"
> - "如何在OnCommand Insight 安裝在Windows主機上的Se.7.3.x內建立自我簽署的憑證"
> - "如何將Cognos憑證授權單位（CA）簽署的憑證匯入OnCommand 到EWdatawarehouse 7.3.3及更新版本"

步驟

1. 使用RegEdit修改中的登錄值 `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun2.0\SANscreen Server\Parameters\Java`

   a. 變更JVM_Option `-DclientAuth=false` 至 `-DclientAuth=true`。

   若為Linux、請修改 `clientAuth` 參數輸入 `/opt/netapp/oci/scripts/wildfly.server`

2. 將憑證授權單位（CA）新增至資料倉儲信任庫：

   a. 在命令視窗中、前往 `..\SANscreen\wildfly\standalone\configuration`。

   b. 使用 `keytool` 列出信任CA的公用程式： `C:\Program Files\SANscreen\java64\bin\keytool.exe -list -keystore server.trustore -storepass changeit`

      每行的第一個字表示CA別名。

   c. 如有必要、請提供CA憑證檔案、通常是 `.pem` 檔案：若要將客戶的CA納入資料倉儲信任的CA、請前往 `..\SANscreen\wildfly\standalone\configuration` 並使用 `keytool` 匯入命令： `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore server.trustore -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

      my_alias通常是容易識別中CA的別名`keytool -list` 營運。

3. 在伺服器上OnCommand Insight `wildfly/standalone/configuration/standalone-full.xml` 檔案必須透過將驗證用戶端更新為中的「要求的」來修改 `/subsystem=undertow/server=default-server/https-listener=default-https`以啟用CAC。登入Insight伺服器並執行適當的命令：

作業系統	指令碼
Windows	wildfly \bin\enableCACforRemoteEJB.bat <install dir>
Linux	/opp/NetApp/OCI /萬用里/賓/enableCACforRemoteEJB.sh

   執行指令碼之後、請等到重新載入wildfly伺服器完成之後、再繼續下一步。

4. 重新啟動OnCommand Insight 伺服器。

設定Cognos以登入智慧卡和憑證（OnCommand Insight 從版本號到版本號7.3.9）

您必須修改OnCommand Insight 「支援Cognos伺服器的智慧卡（CAC）和憑證登入」的「資料倉儲」組態。

開始之前

此程序適用於執行OnCommand Insight VMware 7.3.5到7.3.9的系統。

> 如需最新的CAC和憑證指示、請參閱下列知識庫文章（需要支援登入）：
>
> - "如何設定OnCommand Insight 通用存取卡（CAC）驗證以供使用"
> - "如何設定OnCommand Insight 適用於《支援不支援資料倉儲》的通用存取卡（CAC）驗證"
> - "如何建立及匯入已簽署的憑證授權單位（CA）憑證至OnComand Insight及OnCommand Insight 《Data Warehouse 7.3.x》"
> - "如何在OnCommand Insight 安裝在Windows主機上的Se.7.3.x內建立自我簽署的憑證"
> - "如何將Cognos憑證授權單位（CA）簽署的憑證匯入OnCommand 到EWdatawarehouse 7.3.3及更新版本"

步驟

1. 將憑證授權單位（CA）新增至Cognos受託者。
   a. 在命令視窗中、前往 `..\SANscreen\cognos\analytics\configuration\certs\`
   b. 使用 `keytool` 列出信任CA的公用程式： `..\..\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass NoPassWordSet`

      每行的第一個字表示CA別名。

   c. 如果不存在適當的檔案、請提供CA憑證檔案、通常是 `.pem` 檔案：
   d. 若要將客戶的CA納入OnCommand Insight 可靠的可靠CA、請前往 `..\SANscreen\cognos\analytics\configuration\certs\`。
   e. 使用 `keytool` 匯入的公用程式 `.pem` 檔案： `..\..\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

      `my_alias` 通常是容易識別中CA的別名`keytool -list` 營運。

   f. 當系統提示輸入密碼時、請輸入 `NoPassWordSet`。
   g. 答 `yes` 當系統提示您信任憑證時。
2. 若要啟用CAC模式、請執行 `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`
3. 若要停用CAC模式、請執行 `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`

設定Cognos以登入智慧卡和憑證（OnCommand Insight 更新版本：

您必須修改OnCommand Insight 「支援Cognos伺服器的智慧卡（CAC）和憑證登入」的「資料倉儲」組態。

開始之前

此程序適用於執行OnCommand Insight 支援更新版本的系統。

> 如需最新的CAC和憑證指示、請參閱下列知識庫文章（需要支援登入）：
>
> - "如何設定OnCommand Insight 通用存取卡（CAC）驗證以供使用"
> - "如何設定OnCommand Insight 適用於《支援不支援資料倉儲》的通用存取卡（CAC）驗證"
> - "如何建立及匯入已簽署的憑證授權單位（CA）憑證至OnComand Insight及OnCommand Insight 《Data Warehouse 7.3.x》"
> - "如何在OnCommand Insight 安裝在Windows主機上的Se.7.3.x內建立自我簽署的憑證"
> - "如何將Cognos憑證授權單位（CA）簽署的憑證匯入OnCommand 到EWdatawarehouse 7.3.3及更新版本"

步驟

1. 將憑證授權單位（CA）新增至Cognos受託者。
   a. 在命令視窗中、前往 `..\SANscreen\cognos\analytics\configuration\certs\`
   b. 使用 `keytool` 列出信任CA的公用程式： `..\..\ibm-jre\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass NoPassWordSet`

      每行的第一個字表示CA別名。

   c. 如果不存在適當的檔案、請提供CA憑證檔案、通常是 `.pem` 檔案：
   d. 若要將客戶的CA納入OnCommand Insight 可靠的可靠CA、請前往 `..\SANscreen\cognos\analytics\configuration\certs\`。
   e. 使用 `keytool` 匯入的公用程式 `.pem` 檔案： `..\..\ibm-jre\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

      `my_alias` 通常是容易識別中CA的別名`keytool -list` 營運。

   f. 當系統提示輸入密碼時、請輸入 `NoPassWordSet`。
   g. 答 `yes` 當系統提示您信任憑證時。
2. 若要啟用CAC模式、請執行下列步驟：
   a. 使用下列步驟設定CAC登出頁面：
      - 登入Cognos入口網站（使用者必須是系統管理員群組的一部分、例如Cogns_admin）
      - （僅適用於7.3.10和7.3.11）按一下「管理」（Manage）「組態」（Configuration）「系統」（System）「安全性」（Security）
      - （僅適用於7.3.10和7.3.11）在登出重新導向URL →套用下輸入cacLogout.html
      - 關閉瀏覽器。
   b. 執行 `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`

c. 啟動IBM Cognos服務。等待Cognos服務啟動。

3. 若要停用CAC模式、請執行下列步驟：
   a. 執行 `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`
   b. 啟動IBM Cognos服務。等待Cognos服務啟動。
   c. （僅適用於7.3.10和7.3.11）使用下列步驟取消設定CAC登出頁面：
      - 登入Cognos入口網站（使用者必須是系統管理員群組的一部分、例如Cogns_admin）
      - 按一下「管理」→「組態」→「系統」→「安全性」
      - 在「登出重新導向URL」→「套用」下輸入cacLogout.html
      - 關閉瀏覽器。

匯入Cognos和DWH的CA簽署SSL憑證（Insight 7.3.5至7.3.9）

您可以新增SSL憑證、為Data倉儲和Cognos環境啟用增強的驗證和加密功能。

開始之前

此程序適用於執行OnCommnand Insight 7.3.5到7.3.9的系統。

> 如需最新的CAC和憑證指示、請參閱下列知識庫文章（需要支援登入）：
>
> - "如何設定OnCommand Insight 通用存取卡（CAC）驗證以供使用"
> - "如何設定OnCommand Insight 適用於《支援不支援資料倉儲》的通用存取卡（CAC）驗證"
> - "如何建立及匯入已簽署的憑證授權單位（CA）憑證至OnComand Insight及OnCommand Insight 《Data Warehouse 7.3.x》"
> - "如何在OnCommand Insight 安裝在Windows主機上的Se.7.3.x內建立自我簽署的憑證"
> - "如何將Cognos憑證授權單位（CA）簽署的憑證匯入OnCommand 到EWdatawarehouse 7.3.3及更新版本"

關於這項工作

您必須擁有管理權限才能執行此程序。

步驟

1. 建立的備份 `..\SANScreen\cognos\analytics\configuration\cogstartup.xml`。
2. 在下建立「certs」和「'csk'」資料夾的備份 `..\ SANScreen\cognos\analytics\configuration`。
3. 從Cognos產生憑證加密要求。在管理CMD視窗中、執行：
   a. CD `"\Program Files\sanscreen\cognos\analytics\bin"`
   b. `ThirdPartyCertificateTool.bat -java:local -c -e -p NoPassWordSet -a RSA -d "CN=FQDN,O=orgname,C=US" -r c:\temp\encryptRequest.csr`

4. 開啟 `c:\temp\encryptRequest.csr` 歸檔並複製產生的內容。
5. 將加密Request。CSR傳送至憑證授權單位（CA）以取得SSL憑證。

   請務必新增其他屬性、例如「「：DNS = FQDN」（例如、hostname.netapp.com)`"以新增SubjectAltName。Google Chrome 58版及更新版本會抱怨憑證中是否遺漏SubjectAltName。

6. 使用PKCS7格式加入根憑證、即可下載鏈結憑證

   這會下載FQDN。p7b檔案

7. 從CA取得.p7b格式的憑證。使用名稱將其標示為Cognos Webserver的憑證。
8. ThirdPartyCertificateTool.bat無法匯入整個鏈結、因此匯出所有憑證需要執行多個步驟。請依照下列步驟個別匯出鏈結：
   a. 在「加密Shell Extensions」中開啟.p7b憑證。
   b. 在左窗格中瀏覽至「憑證」。
   c. 在根CA上按一下滑鼠右鍵>「All Tasks（所有工作）」>「Export（匯出
   d. 選取Base64輸出。
   e. 輸入檔案名稱、將其識別為根憑證。
   f. 重複步驟8a到8c、分別將所有憑證匯出至.cer檔案。
   g. 將檔案命名為merginate.cer和Cogns.cer。
9. 如果您只有一個CA憑證、請忽略此步驟、否則請將root.cer和merinateX.cer合併成一個檔案。
   a. 使用「記事本」開啟mintermed.cer並複製內容。
   b. 使用「記事本」開啟root.cer、並儲存9a的內容。
   c. 將檔案另存為CA.cer。
10. 使用管理CMD提示將憑證匯入Cognos Keystore：
    a. CD「Program Files\SANSANSANSANSANSANPC\Cognos /分析\BIN'」
    b. ThirdPartyCertificateTool.bat -Java:local -I -T -r c：\temp\ca.cer

       這會將CA.cer設為根憑證授權單位。

    c. ThirdPartyCertificateTool.bat -Java:local -i -e -r c：\emp\Cogns.cer -t c：\emp\ca.cer

       這會將Cogns.cer設為由CA.cer簽署的加密憑證。

11. 開啟IBM Cognos組態。
    a. 選取「本機組態」→「安全性」→「密碼編譯」→「Cognos」
    b. 變更「Use third party CA？」 為真。
    c. 儲存組態。
    d. 重新啟動Cognos
12. 使用管理CMD提示字元、將最新的Cognos憑證匯出至Cognos。CRT：
    a. 「d:\Program Files\SANSANSANSANSANP\Java\BIN\keytool.exe」-exportcert -file

「'c:\temp\Cogns.crt」-keystore「d:\Program Files\SANSANSANSANSANsce\Cognos \analystation\configuration \certs\CAMKeystore」-storeetype PKCS12 -storeNoPassSet Word-alias加密

13. 使用管理CMD提示視窗、將「'c:\emp\Cognes.crt」匯入DWh信任區、以建立Cognos與DWH之間的SSL通訊。
    a. "d:\Program Files\SANSANSANSANSANSANp\Java\BIN\keytool.exe"-importcert -file ""c:\emp\Cognos.crt"-keystore "D:\Program Files\SANSANscove\wildfly\sonsolation\configuration \server.trustore"-storeepass changit -alias cognoscert
14. 重新啟動SANscreen 此服務。
15. 執行DWH備份、確保DWH與Cognos通訊。

匯入Cognos和DWH的CA簽署SSL憑證（Insight 7.3.10及更新版本）

您可以新增SSL憑證、為Data倉儲和Cognos環境啟用增強的驗證和加密功能。

開始之前

此程序適用於執行OnCommand Insight 支援更新版本的系統。

> 如需最新的CAC和憑證指示、請參閱下列知識庫文章（需要支援登入）：
>
> - "如何設定OnCommand Insight 通用存取卡（CAC）驗證以供使用"
> - "如何設定OnCommand Insight 適用於《支援不支援資料倉儲》的通用存取卡（CAC）驗證"
> - "如何建立及匯入已簽署的憑證授權單位（CA）憑證至OnComand Insight及OnCommand Insight 《Data Warehouse 7.3.x》"
> - "如何在OnCommand Insight 安裝在Windows主機上的Se.7.3.x內建立自我簽署的憑證"
> - "如何將Cognos憑證授權單位（CA）簽署的憑證匯入OnCommand 到EWdatawarehouse 7.3.3及更新版本"

關於這項工作

您必須擁有管理權限才能執行此程序。

步驟

1. 使用IBM Cognos組態工具來停止Cognos。關閉Cognos。
2. 建立的備份 `..\SANScreen\cognos\analytics\configuration` 和 `..\SANScreen\cognos\analytics\temp\cam\freshness` 資料夾：
3. 從Cognos產生憑證加密要求。在管理CMD視窗中、執行：
    a. CD “`\Program Files\sanscreen\cognos\analytics\bin`”
    b. `ThirdPartyCertificateTool.bat -java:local -c -e -p NoPassWordSet -a RSA -r c:\temp\encryptRequest.csr -d “CN=server.domain.com,O=NETAPP,C=US” -H “server.domain.com” -I “ipaddress”`。附註：此處-H和-I是新增subectAltNames、例如DNS

和IP地址。

4. 開啟 `c:\temp\encryptRequest.csr` 歸檔並複製產生的內容。
5. 輸入加密Request。CSR內容、並使用CA簽署入口網站產生憑證。
6. 使用PKCS7格式加入根憑證、即可下載鏈結憑證

   這會下載FQDN。p7b檔案

7. 從CA取得.p7b格式的憑證。使用名稱將其標示為Cognos Webserver的憑證。
8. ThirdPartyCertificateTool.bat無法匯入整個鏈結、因此匯出所有憑證需要執行多個步驟。請依照下列步驟個別匯出鏈結：
   a. 在「加密Shell Extensions」中開啟.p7b憑證。
   b. 在左窗格中瀏覽至「憑證」。
   c. 在根CA上按一下滑鼠右鍵>「All Tasks（所有工作）」>「Export（匯出
   d. 選取Base64輸出。
   e. 輸入檔案名稱、將其識別為根憑證。
   f. 重複步驟8a到8e、分別將所有憑證匯出至.cer檔案。
   g. 將檔案命名為merginate.cer和Cogns.cer。
9. 如果您只有一個CA憑證、請忽略此步驟、否則請將root.cer和merinateX.cer合併成一個檔案。
   a. 使用「記事本」開啟root.cer並複製內容。
   b. 使用「記事本」開啟mender.cer、然後附加9a的內容（中間第一和下一）。
   c. 將檔案另存為chain .cer。
10. 使用管理CMD提示將憑證匯入Cognos Keystore：
    a. CD「Program Files\SANSANSANSANSANSANPC\Cognos /分析\BIN'」
    b. ThirdPartyCertificateTool.bat -Java:local -I -t-r c：\temp\root.cer
    c. ThirdPartyCertificateTool.bat -Java:local -I -T -r c：\temp\minter.cer
    d. ThirdPartyCertificateTool.bat -Java:local -i -e -r c：\emp\Cogns.cer -t c：\emp\chain .cer
11. 開啟IBM Cognos組態。
    a. 選取「本機組態」→「安全性」→「密碼編譯」→「Cognos」
    b. 變更「Use third party CA？」 為真。
    c. 儲存組態。
    d. 重新啟動Cognos
12. 使用管理CMD提示字元、將最新的Cognos憑證匯出至Cognos。CRT：
    a. CD「'C:\Program Files\SANSANSANSANSAND"
    b. Java\BIN\keytool.exe -exportcert -file c：\temp\Cogns.crt -keystore Cognos \分析\組態\certs\CAMKeystore -storetype PKCS12 -storepass NoPassWordSet -alias加密
13. 備份DWH伺服器信任資源`..\SANscreen\wildfly\standalone\configuration\server.trustore`

14. 使用管理CMD提示視窗、將「'c:\emp\Cognes.crt'」匯入DWH信任區、以建立Cognos與DWH之間的SSL通訊。
    a. CD「'C:\Program Files\SANSANSANSANSAND"
    b. Java\BIN\keytool.exe -importcert -file c:\emp\Cognos.crt -keystore wildfly\sisonal\configuration \server.trustore -storepass changit -alias cognos3rca
15. 重新啟動SANscreen 此服務。
16. 執行DWH備份、確保DWH與Cognos通訊。
17. 即使只變更「sSL憑證」、而且預設的Cognos憑證保持不變、仍應執行下列步驟。否則、Cognos可能會抱怨新SANscreen 的不合格證書、或無法建立DWH備份。
    a. `cd "%SANSCREEN_HOME%cognos\analytics\bin\"`
    b. `"%SANSCREEN_HOME%java64\bin\keytool.exe" -exportcert -file "c:\temp\sanscreen.cer" -keystore "%SANSCREEN_HOME%wildfly\standalone\configuration\server.keystore" -storepass changeit -alias "ssl certificate"`
    c. `ThirdPartyCertificateTool.bat -java:local -i -T -r "c:\temp\sanscreen.cer"`

    這些步驟通常是在中所述的Cognos憑證匯入程序中執行 "如何將Cognos憑證授權單位（CA）簽署的憑證匯入OnCommand 到EWdatawarehouse 7.3.3及更新版本"

匯入SSL憑證

您可以新增SSL憑證來啟用增強的驗證和加密功能、以增強OnCommand Insight 您的支援環境的安全性。

開始之前

您必須確保系統符合所需的最低位元層級（1024位元）。

關於這項工作

> 在嘗試執行此程序之前、您應該先備份現有的 `server.keystore` 檔案、並命名備份 `server.keystore.old`。毀損或毀損 `server.keystore` 重新啟動Insight伺服器後、檔案可能導致Insight伺服器無法運作。如果您建立備份、當發生問題時、可以還原至舊檔案。

步驟

1. 建立原始Keystore檔案的複本： `cp c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore.old`
2. 列出Keystore的內容： `C:\Program Files\SANscreen\java64\bin\keytool.exe -list -v -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore"`
    a. 當系統提示輸入密碼時、請輸入 `changeit`。

系統會顯示Keystore的內容。金鑰庫中至少應有一個憑證、 `"ssl certificate"`。

3. 刪除 `"ssl certificate"`： `keytool -delete -alias "ssl certificate" -keystore c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
4. 產生新金鑰： `C:\Program Files\SANscreen\java64\bin\keytool.exe -genkey -alias "ssl certificate" -keyalg RSA -keysize 2048 -validity 365 -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore"`
   a. 當系統提示輸入名字和姓氏時、請輸入您要使用的完整網域名稱（FQDN）。
   b. 提供下列組織與組織架構的相關資訊：
      - 國家/地區：您所在國家/地區的雙字母ISO縮寫（例如美國）
      - 州或省：貴組織總公司所在州或省的名稱（例如、麻塞諸塞州）
      - 地區：貴組織總公司所在城市的名稱（例如Waltham）
      - 組織名稱：擁有網域名稱的組織名稱（例如NetApp）
      - 組織單位名稱：將使用憑證的部門或群組名稱（例如Support）
      - 網域名稱/一般名稱：用於伺服器DNS查詢的FQDN（例如www.example.com）系統會以類似下列的資訊回應： `Is CN=www.example.com, OU=support, O=NetApp, L=Waltham, ST=MA, C=US correct?`
   c. 輸入 `Yes` 當「Common Name（CN）（一般名稱（CN））」等於FQDN時。
   d. 當系統提示輸入金鑰密碼時、請輸入密碼、或按Enter鍵以使用現有的金鑰庫密碼。
5. 產生憑證要求檔案： `C:\Program Files\SANscreen\java64\bin\keytool.exe -certreq -alias "ssl certificate" -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -file c:\localhost.csr`

   - `c:\localhost.csr` 檔案是新產生的憑證要求檔案。
6. 提交 `c:\localhost.csr` 歸檔至您的憑證授權單位（CA）以供核准。

   一旦憑證要求檔案獲得核准、您就會想要在中傳回憑證給您 `.der` 格式。檔案可能會傳回、也可能不會傳回 `.der` 檔案：預設檔案格式為 `.cer` 適用於Microsoft CA服務。

   大多數組織的CA都使用信任鏈模式、包括通常離線的根CA。它只簽署了少數子CA的憑證、稱為中繼CA。

   您必須取得整個信任鏈的公開金鑰（憑證）、即簽署OnCommand Insight 該伺服器憑證的CA憑證、以及該CA與組織根CA之間的所有憑證。

   在某些組織中、當您提交簽署要求時、可能會收到下列其中一項：

   - 包含您簽署的憑證及信任鏈中所有公開憑證的PKCS12檔案
   - 答 `.zip` 包含個別檔案（包括您簽署的憑證）和信任鏈中所有公開憑證的檔案
   - 只有您簽署的憑證

     您必須取得公開憑證。

7. 匯入伺服器.keystore的核准憑證： `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -alias OCI.hostname.com -file c:\localhost2.DER -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore"`

   a. 出現提示時、請輸入Keystore密碼。

      畫面會顯示下列訊息： `Certificate reply was installed in keystore`

8. 匯入伺服器的核准憑證.trustore： `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -alias OCI.hostname.com -file c:\localhost2.DER -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.trustore"`

   a. 出現提示時、請輸入信任密碼。

      畫面會顯示下列訊息： `Certificate reply was installed in trustore`

9. 編輯 `SANscreen\wildfly\standalone\configuration\standalone-full.xml` 檔案：

   替換下列別名字串： `alias="cbc-oci-02.muccbc.hq.netapp.com"`。例如：

   ```
   <keystore path="server.keystore" relative-to="jboss.server.config.dir" keystore-password="${VAULT::HttpsRealm::keystore_password::1}" alias="cbc-oci-02.muccbc.hq.netapp.com" key-password="${VAULT::HttpsRealm::key_password::1}"/>
   ```

10. 重新啟動SANscreen 伺服器服務。

    執行Insight之後、您可以按一下掛鎖圖示來檢視系統上安裝的憑證。

    如果您看到的憑證包含「核發給」資訊、且該資訊符合「核發者」資訊、您仍安裝自我簽署的憑證。Insight安裝程式產生的自我簽署憑證已過期100年。

    NetApp無法保證此程序會移除數位憑證警告。NetApp無法控制終端使用者工作站的設定方式。請考慮下列案例：

    - Microsoft Internet Explorer和Google Chrome都使用Microsoft在Windows上的原生憑證功能。

      這表示、如果Active Directory管理員將組織的CA憑證推入終端使用者的憑證信任器、則OnCommand Insight 當以內部CA基礎架構簽署的更新版本取代自我簽署的憑證時、這些瀏覽器的使用者將會看到憑證警告消失。

    - Java和Mozilla Firefox都有自己的憑證存放區。

      如果系統管理員未將 CA 憑證自動擷取至這些應用程式的信任憑證存放區、則使用 Firefox 瀏覽器可能會因為不受信任的憑證而持續產生憑證警告、即使自行簽署的憑證已被取代。將組織的憑證鏈結安裝到信任關係中、是另一項需求。

為Insight資料庫設定每週備份

您可能想要為Insight資料庫設定每週自動備份、以保護資料。這些自動備份會覆寫指定備份目錄中的檔案。

關於這項工作

最佳實務做法：當您設定OCI資料庫的每週備份時、必須將備份儲存在Insight所使用的不同伺服器上、以防伺服器故障。請勿在每週備份目錄中儲存任何手動備份、因為每週備份會覆寫目錄中的檔案。

備份檔案將包含下列項目：

- 庫存資料
- 高達7天的效能資料

步驟

1. 在Insight工具列上、按一下*管理*>*設定*。
2. 按一下*備份與歸檔*索引標籤。
3. 在「每週備份」區段中、選取*「啟用每週備份」*。
4. 輸入*備份位置*的路徑。這可以位於本機Insight伺服器上、或位於可從Insight伺服器存取的遠端伺服器上。

> 備份位置設定包含在備份本身中、因此如果您在其他系統上還原備份、請注意新系統上的備份資料夾位置可能無效。還原備份後、請再次檢查備份位置設定。

5. 選擇*清理*選項以保留最後兩個或最後五個備份。
6. 按一下「 * 儲存 * 」。

結果

您也可以前往*管理*>*疑難排解*建立隨需備份。

備份內容

每週和隨需備份可用於疑難排解或移轉。

每週或隨需備份包括下列項目：

- 庫存資料
- 效能資料（若已選擇納入備份）
- 資料來源和資料來源設定
- 整合套件
- 遠端擷取單元
- ASUP/ Proxy設定
- 備份位置設定
- 歸檔位置設定
- 通知設定
- 使用者

- 效能原則
- 企業實體與應用程式
- 裝置解析度規則與設定
- 儀表板與小工具
- 自訂的資產頁面儀表板和小工具
- 查詢
- 註釋和註釋規則

每週備份不包括：

- 安全工具設定/資料保存資訊（透過獨立的CLI程序備份）
- 記錄（可視需要儲存至.Zip檔案）
- 效能資料（若未選擇納入備份）
- 授權

> 如果您選擇在備份中加入效能資料、則會備份最近七天的資料。如果啟用了該功能、其餘資料將會儲存在歸檔中。

效能資料歸檔

介紹能夠每日歸檔效能資料的功能OnCommand Insight 。這是對組態和有限效能資料備份的補充。

支援多達90天的效能和違規資料OnCommand Insight 。不過、建立該資料的備份時、備份中只會包含最新的資訊。歸檔可讓您儲存其餘的效能資料、並視需要載入。

設定歸檔位置並啟動歸檔之後、Insight會每天將所有物件的前一天效能資料歸檔到歸檔位置。每天的歸檔資料都會保留在個別檔案的歸檔資料夾中。歸檔會在背景中進行、只要Insight正在執行、就會繼續進行。

系統會保留最近90天的歸檔資料；在建立較新的歸檔資料時、會刪除90天之前的歸檔檔案。

實現效能歸檔

若要啟用效能資料歸檔、請遵循下列步驟。

步驟

1. 在工具列上、按一下*管理*>*設定*。
2. 選取*備份與歸檔*索引標籤。
3. 在「效能歸檔」區段中、確認已勾選「啟用效能歸檔」。
4. 指定有效的歸檔位置。

   您無法在Insight安裝資料夾下指定資料夾。

最佳實務做法：請勿指定與Insight備份位置相同的歸檔資料夾。

5. 按一下「 * 儲存 * 」。

   歸檔程序會在背景中處理、不會干擾其他Insight活動。

正在載入效能歸檔

若要載入效能資料歸檔、請依照下列步驟進行。

開始之前

在載入效能資料歸檔之前、您必須先還原有效的每週或手動備份。

步驟

1. 在工具列上、按一下*管理*>*疑難排解*。
2. 在「還原」區段的「載入效能歸檔」下、按一下「載入」。

> 歸檔載入會在背景中處理。載入完整歸檔可能需要很長時間、因為每天的歸檔效能資料都會填入Insight中。歸檔載入的狀態會顯示在此頁面的歸檔區段中。

設定您的電子郵件

您必須設定OnCommand Insight 支援以存取電子郵件系統、OnCommand Insight Server 才能使用您的電子郵件來傳送報告（您訂閱的報告）、並將疑難排解支援資訊傳送給NetApp技術支援部門。

電子郵件組態先決條件

在設定OnCommand Insight 支援存取電子郵件系統的功能之前、您必須先探索主機名稱或IP位址、以識別（SMTP或Exchange）郵件伺服器、並為OnCommand Insight 其分配電子郵件帳戶以供提交靜態報告。

請您的電子郵件管理員建立OnCommand Insight 一個電子郵件帳戶以供使用。您需要下列資訊：

- 用於識別組織所使用（SMTP或Exchange）郵件伺服器的主機名稱或IP位址。您可以透過用來讀取電子郵件的應用程式來尋找此資訊。例如、在Microsoft Outlook中、您可以檢視帳戶組態來尋找伺服器名稱：工具-電子郵件帳戶-檢視或變更現有的電子郵件帳戶。
- 電子郵件帳戶名稱OnCommand Insight 、透過此電子郵件帳戶、即可寄送定期報告。帳戶必須是貴組織中有效的電子郵件地址。（除非訊息是由有效使用者傳送、否則大部分的郵件系統都不會傳送訊息。） 如果電子郵件伺服器需要使用者名稱和密碼才能傳送郵件、請向系統管理員索取此資訊。

設定**Insight**電子郵件

如果使用者想要在電子郵件帳戶中接收Insight報告、您必須設定電子郵件伺服器才能啟用

此功能。

步驟

1. 在Insight工具列上、按一下*管理*、然後選取*通知*。
2. 向下捲動至頁面的*電子郵件*區段。
3. 在「伺服器」方塊中、輸入您組織中的SMTP伺服器名稱、此名稱是使用主機名稱或IP位址（_nn.n.n.n.nn.nnn_格式）來識別。

   如果您指定主機名稱、請確定名稱可以透過DNS解析。

4. 在*使用者名稱*方塊中、輸入您的使用者名稱。
5. 在「密碼」方塊中、輸入存取電子郵件伺服器的密碼、僅當您的SMTP伺服器受密碼保護時才需要輸入密碼。這是您用來登入應用程式的相同密碼、可讓您讀取電子郵件。如果需要密碼、您必須再次輸入密碼進行驗證。
6. 在「寄件者電子郵件」方塊中、輸入在所有OnCommand Insight 的報告中、將被識別為寄件者的寄件者電子郵件帳戶。

   此帳戶必須是貴組織內有效的電子郵件帳戶。

7. 在「電子郵件簽名」方塊中、輸入您要插入每封電子郵件的文字。
8. 在「收件者」方塊中、按一下 ✚輸入電子郵件地址、然後按一下*確定*。

   若要編輯電子郵件地址、請選取地址、然後按一下 。若要刪除電子郵件地址、請選取地址、然後按一下 ✖。

9. 若要傳送測試電子郵件給指定的收件者、請按一下 ✔。
10. 按一下「 * 儲存 * 」。

設定SNMP通知

支援SNMP通知、以進行組態和全域路徑原則變更、以及違規OnCommand Insight 。例如、當超過資料來源臨界值時、就會傳送SNMP通知。

開始之前

下列項目必須已完成：

- 識別伺服器的IP位址、以整合每種事件類型的陷阱。

  您可能必須諮詢系統管理員以取得此資訊。

- 識別指定機器取得每種事件類型SNMP設陷的連接埠號碼。

  SNMP設陷的預設連接埠為162。

- 在您的站台上編譯mib。

專屬的mib隨附安裝軟體、可支援OnCommand Insight 各種不必要的功能。NetApp MIB與所有標準SNMP管理軟體相容、可在的Insight伺服器上找到 `<install dir>\SANscreen\MIBS\sanscreen.mib`。

步驟

1. 按一下「管理」、然後選取「通知」。
2. 向下捲動至頁面的「* SNMP *」區段。
3. 按一下「動作」、然後選取「新增設陷來源」。
4. 在「新增**SNMP**設陷收件者」對話方塊中、輸入下列值：
   - * IP*

     將SNMP設陷訊息傳送至OnCommand Insight 哪個IP位址。

   - 連接埠

     將SNMP設陷訊息傳送至OnCommand Insight 哪個連接埠號碼。

   - 社群字串

     使用「'public'」來顯示SNMP設陷訊息。
5. 按一下「 * 儲存 * 」。

啟用syslog工具

您可以識別OnCommand Insight 記錄不符合資訊的事件、效能警示及稽核訊息的位置、並啟動記錄程序。

開始之前

- 您必須擁有儲存系統記錄的伺服器IP位址。
- 您必須知道與記錄訊息的程式類型相對應的設施層級、例如：LOCAL2或使用者。

關於這項工作

系統記錄包括下列類型的資訊：

- 違規訊息
- 效能警示
- 也可以選擇稽核記錄訊息

系統記錄中使用下列單位：

- 使用率指標：百分比
- 流量指標：MB

- 流量：MB/s

步驟

1. 在Insight工具列上、按一下*管理*、然後選取*通知*。
2. 向下捲動至頁面的「系統記錄」區段。
3. 選取*啟用SysLog *核取方塊。
4. 如有需要、請選取*傳送稽核*核取方塊。除了顯示在「稽核」頁面之外、新的稽核記錄訊息也會傳送至syslog。請注意、現有的稽核記錄訊息將不會傳送至syslog、只會傳送新產生的記錄訊息。
5. 在*伺服器*欄位中、輸入記錄伺服器的IP位址。

   您可以在伺服器IP結尾加上一個分號（例如伺服器：連接埠）、以指定自訂連接埠。如果未指定連接埠、則會使用預設的syslog連接埠：514。

6. 在* Facility *欄位中、選取與記錄訊息之程式類型相對應的設施層級。
7. 按一下「 * 儲存 * 」。

Insight syslog內容

您可以在伺服器上啟用syslog、以收集Insight違規和效能警示訊息、包括使用率和流量資料。

訊息類型

Insight syslog列出三種類型的訊息：

- SAN路徑違規
- 一般違規
- 效能警示

提供的資料

違規說明包括所涉及的元素、事件時間、以及違規的相對嚴重性或優先順序。

效能警示包括下列資料：

- 使用率百分比
- 流量類型
- 流量以MB為單位

設定效能並確保違規通知

支援效能通知、確保違規OnCommand Insight 。根據預設、Insight不會針對這些違規事件傳送通知；您必須設定Insight以傳送電子郵件、傳送系統記錄訊息至系統記錄伺服器、或在發生違規時傳送SNMP通知。

開始之前

您必須已設定電子郵件、系統記錄和SNMP傳送方法、以處理違規事件。

步驟

1. 按一下*管理*>*通知*。
2. 按一下「事件」。
3. 在「效能違規事件」或「保證違規事件」區段中、按一下您要的通知方法（電子郵件、系統日誌*或 SNMP）清單、然後針對違規選取嚴重性等級（*警告及以上*或*嚴重）。
4. 按一下「 * 儲存 * 」。

設定系統層級的事件通知

支援系統層級事件的通知、例如擷取單元故障或資料來源錯誤OnCommand Insight 。若要接收通知、您必須設定Insight在發生一或多個事件時傳送電子郵件。

開始之前

您必須在*管理*>*通知*>*傳送方法*中設定接收通知的電子郵件收件者。

步驟

1. 按一下*管理*>*通知*。
2. 按一下「事件」。
3. 在「系統警示事件*電子郵件」區段中、選取通知的嚴重性等級（*警告及以上*或*嚴重）、或如果您不想收到系統層級事件的通知、請選擇*不要傳送*。
4. 按一下「 * 儲存 * 」。
5. 按一下*管理*>*系統警示*以自行設定警示。
6. 若要新增警示、請按一下「**+**新增」、然後為警示提供唯一的*名稱*。您也可以按一下右側圖示*編輯*現有警示。
7. 選擇要警示的*事件類型*、例如_擷取單位故障_。
8. 選擇* Snooze *時間間隔、可在所選時間間隔內、針對所選類型的重複事件、隱藏通知。如果您選取「_Never」、則每分鐘會收到一次重複通知、直到事件不再發生為止。
9. 選擇*嚴重性*（警告或嚴重）作為事件通知。
10. 依預設、電子郵件通知會傳送至全域電子郵件收件者清單、您也可以按一下提供的連結來覆寫全域清單、並傳送通知給特定的收件者。
11. 按一下「儲存」以新增警示。

設定**ASUP**處理

所有NetApp產品均具備自動化功能、可為客戶提供最佳支援。自動化支援（ASUP）會定

期傳送預先定義的特定資訊給客戶支援部門。您可以控制要轉送給NetApp的資訊、以及傳送的頻率。

開始之前

您必須先設定OnCommand Insight 支援功能、才能在傳送任何資料之前轉寄資料。

關於這項工作

ASUP資料會使用HTTPS傳輸協定進行轉送。

步驟

1. 在Insight工具列上、按一下*管理*。
2. 按一下*設定*。
3. 按一下「* ASUP & Proxy*」標籤。
4. 在「* ASUP*」區段中、選取「啟用**ASUP**」以啟動ASUP功能。
5. 如果您想要變更公司資訊、請更新下列欄位：
   - 公司名稱
   - 站台名稱
   - 要傳送的內容：記錄、組態資料、效能資料
6. 按一下「測試連線」以確保您指定的連線正常運作。
7. 按一下「 * 儲存 * 」。
8. 在* Proxy*區段中、選擇是否要*啟用Proxy*、然後指定您的Proxy 主機、*連接埠*和*使用者*資訊。
9. 按一下「測試連線」以確保您指定的Proxy正常運作。
10. 按一下「 * 儲存 * 」。

包含在**S**甚麼（**ASUP**）套件中**AutoSupport**

此支援包含資料庫備份及延伸資訊AutoSupport 。

此套件包含下列項目AutoSupport ：

- 庫存資料
- 效能資料（若已選取納入ASUP）
- 資料來源和資料來源設定
- 整合套件
- 遠端擷取單元
- ASUP/ Proxy設定
- 備份位置設定

- 歸檔位置設定
- 通知設定
- 使用者
- 效能原則
- 企業實體與應用程式
- 裝置解析度規則與設定
- 儀表板與小工具
- 自訂的資產頁面儀表板和小工具
- 查詢
- 註釋和註釋規則
- 記錄
- 授權
- 擷取/資料來源狀態
- MySQL狀態
- 系統資訊

此套件不包括AutoSupport ：

- 安全工具設定/資料保存資訊（透過獨立的CLI程序備份）
- 效能資料（若未選擇納入ASUP）

> 如果您選擇在ASUP中包含效能資料、則會包含最近七天的資料。如果啟用了該功能、其餘資料將會儲存在歸檔中。ASUP不包含歸檔資料。

定義應用程式

如果您想要追蹤與環境中執行之特定應用程式相關的資料、則必須定義這些應用程式。

開始之前

如果您想要將應用程式與企業實體建立關聯、您必須已經建立企業實體。

關於這項工作

您可以將應用程式與下列資產建立關聯：主機、虛擬機器、磁碟區、內部磁碟區、qtree、 共享區和Hypervisor。

步驟

1. 登入OnCommand Insight 到The W不明 網路UI。
2. 單擊*管理*並選擇*應用程序*。

定義應用程式之後、「應用程式」頁面會顯示應用程式的名稱、優先順序、以及與應用程式相關聯的企業實體（若適用）。

3. 按一下「 * 新增 * 」。

   此時會顯示「新增應用程式」對話方塊。

4. 在「名稱」方塊中輸入應用程式的唯一名稱。
5. 按一下*優先順序*、然後選取您環境中應用程式的優先順序（嚴重、高、中或低）。
6. 如果您打算將此應用程式與企業實體搭配使用、請按一下*商業實體*、然後從清單中選取實體。
7. 選用：如果您不使用磁碟區共用、請按一下以清除*驗證磁碟區共用*方塊。

   這需要保證授權。若要確保每個主機都能存取叢集中的相同磁碟區、請設定此選項。例如、高可用度叢集中的主機通常需要遮罩至相同的磁碟區、才能進行容錯移轉；不過、不相關應用程式中的主機通常不需要存取相同的實體磁碟區。此外、為了安全起見、法規原則可能會要求您明確禁止不相關的應用程式存取相同的實體磁碟區。

8. 按一下「 * 儲存 * 」。

   應用程式會出現在「應用程式」頁面中。如果按一下應用程式名稱、Insight會顯示應用程式的資產頁面。

完成後

定義應用程式之後、您可以前往主機、虛擬機器、Volume、內部Volume或Hypervisor的資產頁面、將應用程式指派給資產。

將應用程式指派給資產

定義應用程式之後、無論是否有商業實體、您都可以將應用程式與資產建立關聯。

步驟

1. 登入OnCommand Insight 到The W不明 網路UI。
2. 執行下列其中一項動作、找出您要套用應用程式的資產（主機、虛擬機器、Volume或內部Volume）：
   - 按一下*儀表板*、選取*資產儀表板*、然後按一下資產。
   - 按一下 在工具列上顯示*搜尋資產*方塊、輸入資產名稱、然後從清單中選取資產。
3. 在資產頁面的「使用者資料」區段中、將游標放在目前指派給資產的應用程式名稱上（如果未指派應用程式、則會顯示*「無」*）、然後按一下 （編輯應用程式）。

   所選資產顯示的可用應用程式清單。目前與資產相關聯的應用程式前面會有核取符號。

4. 您可以在「搜尋」方塊中輸入以篩選應用程式名稱、也可以向下捲動清單。
5. 選取您要與資產建立關聯的應用程式。

   您可以將多個應用程式指派給主機、虛擬機器和內部磁碟區、但是您只能將一個應用程式指派給磁碟區。

6.

按一下 ✓ 可將選定的應用程序或應用程序分配給資產。

應用程式名稱會顯示在「使用者資料」區段中；如果應用程式與企業實體相關聯、則該企業實體的名稱也會顯示在此區段中。

編輯應用程式

您可能想要變更應用程式的優先順序、與應用程式相關聯的商業實體、或磁碟區共用的狀態。

步驟

1. 登入OnCommand Insight 到The W不明 網路UI。
2. 單擊*管理*並選擇*應用程序*。
3. 將游標放在您要編輯的應用程式上、然後按一下 ✎ 。

   隨即顯示「編輯應用程式」對話方塊。

4. 執行下列任一項：
   - 按一下*優先順序*、然後選取不同的優先順序。

     ⓘ 您無法變更應用程式的名稱。

   - 按一下「商業實體」、然後選取要與應用程式建立關聯的不同企業實體、或選取「無」以移除應用程式與企業實體之間的關聯。
   - 按一下以清除或選取*驗證磁碟區共用*。

     ⓘ 此選項僅在您擁有Assure授權時可用。

5. 按一下「 * 儲存 * 」。

刪除應用程式

當應用程式不再滿足您環境中的需求時、您可能會想要刪除它。

步驟

1. 登入Insight Web UI。
2. 單擊*管理*並選擇*應用程序*。
3. 將游標放在您要刪除的應用程式上、然後按一下 🗑 。

   隨即顯示確認對話方塊、詢問您是否要刪除應用程式。

4. 按一下「確定」。

您的企業實體階層架構

您可以定義企業實體、以更精細的層級追蹤及報告環境資料。

在這個結構中、企業實體階層包含下列層級OnCommand Insight ：

- *租戶*主要由服務供應商用來將資源與客戶建立關聯、例如NetApp。
- *業務線（LOB）*是公司內部的業務線或產品線、例如資料儲存設備。
- *業務單位*代表傳統業務單位、例如法務或行銷部門。
- *專案*通常用於識別業務單位內您想要容量計費的特定專案。例如、「專利」可能是法律業務單位的專案名稱、而「銷售活動」可能是行銷業務單位的專案名稱。請注意、層級名稱可能包含空格。

您不需要使用公司階層架構設計中的所有層級。

設計企業實體階層架構

您必須瞭解企業架構的要素、以及企業實體中需要呈現的內容、因為這些要素已成為OnCommand Insight 您的一套完整的還原資料庫結構。您可以使用下列資訊來設定企業實體。請記住、您不需要使用所有階層層級來收集這些類別中的資料。

步驟

1. 檢查各個層級的企業實體階層、以判斷該層級是否應納入貴公司的企業實體階層：
   - *如果您的公司是ISP、而且您想要追蹤客戶的資源使用量、則需要租戶*層級。
   - 如果需要追蹤不同產品線的資料、則階層架構中需要使用業務線（**LOB**）。
   - 如果您需要追蹤不同部門的資料、則需要業務單位。在分隔某個部門使用的資源（其他部門不使用的資源）時、這種階層層級通常非常重要。
   - *專案層級可用於部門內的專業工作。相較於公司或部門的其他專案、此資料可能有助於找出、定義及監控個別專案的技術需求。
2. 建立圖表、顯示實體內所有層級的每個企業實體名稱。
3. 檢查階層中的名稱、以確保OnCommand Insight 它們在「景點」和「報告」中能夠自我解釋。
4. 識別與每個企業實體相關的所有應用程式。

建立商業實體

為貴公司設計企業實體階層之後、您可以設定應用程式、然後將商業實體與應用程式建立關聯。此程序可在OnCommand Insight 您的資料庫中建立業務實體架構。

關於這項工作

將應用程式與商業實體建立關聯是選擇性的、不過這是最佳實務做法。

步驟

1. 登入Insight Web UI。
2. 按一下「管理」、然後選取「商業實體」。

   隨即顯示「商業實體」頁面。

3. 按一下 ✚Add 開始建立新的實體。

   此時將顯示「新增營業實體」對話方塊。

4. 對於每個實體層級（租戶、業務單位、業務單位和專案）、您可以執行下列任一項：
   - 按一下實體層級清單、然後選取一個值。
   - 輸入新值、然後按Enter。
   - 如果您不想將實體層級用於企業實體、請將實體層級值保留為N/A。
5. 按一下「 * 儲存 * 」。

將企業實體指派給資產

您可以將企業實體指派給資產（主機、連接埠、儲存設備、交換器、虛擬機器、 qtree、共享區、Volume或內部Volume）、但不需將企業實體與應用程式建立關聯；不過、如果該資產與與企業實體相關的應用程式相關聯、則會自動將企業實體指派給該資產。

開始之前

您必須已建立企業實體。

關於這項工作

雖然您可以將業務實體直接指派給資產、但建議您將應用程式指派給資產、然後將業務實體指派給資產。

步驟

1. 登入OnCommand Insight 到The W不明 網路UI。
2. 執行下列其中一項操作、找出您要套用商業實體的資產：
   - 按一下資產儀表板中的資產。
   - 按一下 在工具列上顯示*搜尋資產*方塊、輸入資產名稱、然後從清單中選取資產。
3. 在資產頁面的「使用者資料」區段中、將游標放在「商業實體」旁邊的「*無」*上、然後按一下 。

   此時會顯示可用的商業實體清單。

4. 輸入*搜尋*方塊以篩選特定實體的清單、或向下捲動清單；從清單中選取企業實體。

   如果您選擇的企業實體與應用程式相關聯、則會顯示應用程式名稱。在這種情況下、企業實體名稱旁會出現「已導入」一詞。如果您只想維護資產的實體、而不想維護相關應用程式、您可以手動覆寫應用程式的指派。

5. 若要覆寫衍生自企業實體的應用程式、請將游標放在應用程式名稱上、然後按一下 🗑 、選取其他企業實體、然後從清單中選取其他應用程式。

將企業實體指派給多個資產、或是從多個資產中移除企業實體

您可以使用查詢來指派或移除多個資產中的商業實體、而不必手動指派或移除這些實體。

開始之前

您必須已經建立要新增至所需資產的商業實體。

步驟

1. 建立新的查詢、或開啟現有的查詢。
2. 如果需要、請篩選您要新增商業實體的資產。
3. 在清單中選取所需的資產、或按一下 ☐ ▾ 選擇*全部*。

   將顯示* Actions （操作）按鈕。

4. 若要將企業實體新增至所選資產、請按一下 Actions ▾ 。如果所選的資產類型可以指派給商業實體、您會看到選單選項*新增商業實體*。選取此選項。
5. 從清單中選取所需的企業實體、然後按一下「儲存」。

   您指派的任何新企業實體、都會優先於已指派給該資產的任何企業實體。將應用程式指派給資產、也會以相同方式覆寫指派給企業實體。將業務實體指派給AS資產、也可能會覆寫指派給該資產的任何應用程式。

6. 若要移除指派給資產的企業實體、請按一下 Actions ▾ 然後選取*移除商業實體*。
7. 從清單中選取所需的企業實體、然後按一下*刪除*。

定義註釋

自訂OnCommand Insight 功能以追蹤資料以符合企業需求時、您可以定義所需的任何專業註釋、以便提供完整的資料圖片：例如資產生命週期結束、資料中心、建置位置、儲存層或磁碟區、 和內部Volume服務層級。

步驟

1. 列出環境資料必須關聯的任何產業術語。
2. 列出環境資料必須關聯的企業術語、但尚未使用商業實體來追蹤這些術語。
3. 找出您可以使用的任何預設註釋類型。
4. 找出您需要建立的自訂附註。

使用註釋來監控環境

自訂OnCommand Insight 功能時、若要根據公司需求追蹤資料、您可以定義專業的附註、

稱為_annotations、然後將其指派給您的資產。例如、您可以使用資產生命週期結束、資料中心、建置位置、儲存層級或Volume服務層級等資訊來為資產加上註釋。

使用註釋來協助監控環境、包括下列高層級工作：

- 建立或編輯所有註釋類型的定義。
- 顯示資產頁面、並將每項資產與一或多個附註建立關聯。

  例如、如果某項資產正在租賃、而租賃在兩個月內到期、您可能會想要在該資產上套用生命週期結束附註。這有助於防止其他人長期使用該資產。

- 建立規則以自動將註釋套用至同一類型的多個資產。
- 使用註釋匯入公用程式匯入註釋。
- 依資產附註篩選資產。
- 根據附註將報告中的資料分組、然後產生這些報告。

  如OnCommand Insight 需報告的詳細資訊、請參閱《_此報告指南》。

管理註釋類型

提供一些預設的註釋類型、例如資產生命週期（生日或生命週期結束）、建置或資料中心位置、以及階層、您可以自訂以顯示在報告中OnCommand Insight 。您可以定義預設註釋類型的值、或建立自己的自訂註釋類型。您稍後可以編輯這些值。

預設註釋類型

OnCommandInsight提供一些預設註釋類型。這些附註可用來篩選或分組資料、以及篩選資料報告。

您可以將資產與預設註釋類型建立關聯、例如：

- 資產生命週期、例如生日、日出或生命週期結束
- 裝置的位置資訊、例如資料中心、建築物或樓層
- 資產分類、例如依品質（階層）、依連線裝置（交換器層級）或依服務層級分類
- 狀態、例如Hot（高使用率）

下表列出預設的註釋類型。您可以根據自己的需求、編輯這些註釋名稱中的任何一個。

註釋類型	說明	類型
別名	資源的使用者易記名稱。	文字
生日	裝置上線或即將上線的日期。	日期

建置	主機、儲存設備、交換器和磁帶資源的實體位置。	清單
城市	主機、儲存設備、交換器和磁帶資源的市位置。	清單
運算資源群組	主機和VM檔案系統資料來源所使用的群組指派。	清單
大陸	主機、儲存設備、交換器和磁帶資源的地理位置。	清單
國家/地區	主機、儲存設備、交換器和磁帶資源的國家位置。	清單
資料中心	資源的實體位置、可用於主機、儲存陣列、交換器和磁帶。	清單
直接附加	表示（是或否）儲存資源是否直接連線至主機。	布林值
生命週期終止	裝置離線的日期、例如當租約過期或硬體即將淘汰時。	日期
網路別名	使用者易記的Fabric名稱。	文字
現場	裝置在建築物地板上的位置。可針對主機、儲存陣列、交換器和磁帶進行設定。	清單
熱	已定期或在容量臨界值時大量使用的裝置。	布林值
附註	您想要與資源相關聯的註解。	文字
機架	資源所在的機架。	文字
空間	在建築物內或主機、儲存設備、交換器和磁帶資源的其他位置。	清單
SAN	網路的邏輯分割區。可用於主機、儲存陣列、磁帶、交換器及應用程式。	清單

服務層級	一組可指派給資源的支援服務層級。提供內部磁碟區、qtree和磁碟區的排序選項清單。編輯服務層級以設定不同層級的效能原則。	清單
州/省	資源所在的州或省。	清單
日落後	設定的臨界值、在此之後無法對該裝置進行新的配置。適用於計畫性移轉和其他擱置中的網路變更。	日期
交換器層級	包含預先定義的選項、可設定交換器類別。一般而言、這些名稱會保留在裝置的使用壽命內、但您可以視需要加以編輯。僅適用於交換器。	清單
層級	可用於定義環境中的不同服務層級。階層可以定義層級類型、例如所需的速度（例如金級或銀級）。此功能僅適用於內部磁碟區、qtree、儲存陣列、儲存資源池和磁碟區。	清單
違規嚴重性	在最高至最低重要性的階層中、排列違規（例如遺失主機連接埠或缺少備援）的等級（例如MAJOR）。	清單

別名、資料中心、Hot、服務層級、 交換器層級、服務層級、層級和違規嚴重性為系統層級的附註、您無法刪除或重新命名；您只能變更其指派的值。

註釋的指派方式

您可以手動或使用註釋規則自動指派註釋。此外、還會自動指派一些資產取得和繼承的附註OnCommand Insight 。您指派給資產的任何附註都會顯示在資產頁面的「使用者資料」區段中。

註釋的指派方式如下：

- 您可以手動指派附註給資產。

  如果評註是直接指派給資產、評註會在資產頁面上顯示為一般文字。手動指派的註釋一律優先於註釋規則所繼承或指派的註釋。

- 您可以建立附註規則、自動將附註指派給相同類型的資產。

  如果評註是根據規則指派、Insight會在資產頁面上的評註名稱旁顯示規則名稱。

- Insight會自動將層級與儲存層模型建立關聯、以加速在取得資產時、將儲存註釋指派給資源。

  某些儲存資源會自動與預先定義的層（層級1和層級2）建立關聯。例如、Symmetrix儲存層是以Symmetrix和VMAX系列為基礎、並與層級1相關聯。您可以變更預設值以符合層級要求。如果評註是由Insight指派（例如層級）、當您將游標放在資產頁面上的評註名稱上時、您會看到「系統定義」。

- 少數資源（資產子項）可從其資產（父項）衍生預先定義的層級附註。

  例如、如果您指派附註給儲存設備、則層級附註會衍生自屬於儲存設備的所有儲存資源池、內部磁碟區、磁碟區、qtree及共用區。如果將不同的註釋套用至儲存設備的內部磁碟區、則註釋會隨後衍生至所有磁碟區、qtree和共用區。「已導出」會出現在資產頁面上的註釋名稱旁。

將成本與附註建立關聯

在執行成本相關報告之前、您應該先將成本與服務層級、交換器層級及層級系統層級的註釋建立關聯、以便根據儲存使用者實際使用的正式作業量和複寫容量來進行計費。例如、對於階層層級、您可能有黃金和銀層值、並將較高的成本指派給金層、而非銀層。

步驟

1. 登入InsightWeb UI。
2. 按一下「Manage（管理）」、然後選取「* annotation

   此時會顯示「附註」頁面。

3. 將游標放在「服務層級」、「交換器層級」或「層級」註釋上、然後按一下 。

   隨即顯示「編輯附註」對話方塊。

4. 在「成本」欄位中輸入任何現有層級的值。

   層級和服務層級附註分別具有自動層級和物件儲存值、您無法移除這些值。

5. 按一下 ✚Add 以新增其他層級。
6. 完成後單擊*保存*。

建立自訂註釋

使用註釋、您可以新增符合業務需求的自訂業務專屬資料至資產。雖然提供一組預設附註、但您可能會發現您想要以其他方式檢視資料OnCommand Insight 。自訂附註中的資料可補充已收集的裝置資料、例如交換器製造商、連接埠數量和效能統計資料。Insight不會探索您使用附註新增的資料。

步驟

1. 登入Insight Web UI。
2. 按一下「管理」、然後選取「註釋」。

「附註」頁面會顯示附註清單。

3. 按一下 ✚ Add 。

   此時將顯示* Add Annotation*（添加註釋*）對話框。

4. 在*名稱*和*說明*欄位中輸入名稱和說明。

   您可以在這些欄位中輸入最多255個字元。

   > 以點開頭或結尾的註釋名稱。 不受支援。

5. 按一下「類型」、然後選取下列其中一個選項、代表此註釋所允許的資料類型：

   - 布林值

     這會建立下拉式清單、其中包含「是」和「否」選項例如、「直接附加」註釋為布林型。

   - 日期

     這會建立一個保留日期的欄位。例如、如果註釋是日期、請選取此選項。

   - 清單

     這可能會產生下列任一項目：

     - 下拉式固定清單

       當其他人在裝置上指派此註釋類型時、他們無法新增更多值至清單。

     - 下拉式彈性清單

       如果您在建立此清單時選取*「即時新增值*」選項、當其他人在裝置上指派此註釋類型時、他們可以將更多值新增至清單。

   - 數量

     這會建立一個欄位、讓指派附註的使用者可以輸入一個數字。例如、如果註釋類型為「Floor」、則使用者可以選取「'number'」的值類型、然後輸入樓層編號。

   - 文字

     這會建立允許自由格式文字的欄位。例如、您可以輸入「'Language」作為註釋類型、選取「'Text」作為值類型、然後輸入語言作為值。

   > 設定類型並儲存變更後、便無法變更註釋類型。如果您需要變更類型、則必須刪除註釋並建立新的註釋。

6. 如果您選取「**清單」作為註釋類型、請執行下列動作：

   a. 如果您想要在資產頁面上新增更多值至註釋、請選取*「即時新增值」*、以建立彈性清單。

例如、假設您在資產頁面上、資產的「城市」註釋會顯示值為「底特律」、「坦帕」和「波士頓」。如果您選取*「即時新增值」選項、您可以直接在資產頁面上新增城市（例如舊金山和芝加哥）的其他值、而不必前往「附註」頁面新增這些值。如果您未選擇此選項、則在套用註釋時、將無法新增註釋值；這會建立固定清單。

b. 在*值*和*說明*欄位中輸入值和名稱。

c. 按一下 ✚Add 以新增其他值。

d. 按一下 移除值。

7. 按一下「 * 儲存 * 」。

   您的註釋會出現在「註釋」頁面的清單中。

相關資訊

"匯入及匯出使用者資料"

手動指派資產附註

指派資產附註有助於您以與業務相關的方式來排序、分組及報告資產。雖然您可以使用註釋規則、自動將註釋指派給特定類型的資產、但您可以使用資產頁面、將註釋指派給個別資產。

開始之前

您必須已建立要指派的附註。

步驟

1. 登入OnCommand Insight 到The W不明 網路UI。
2. 執行下列其中一項操作、找出您要套用註釋的資產：
   - 按一下資產儀表板中的資產。
   - 按一下 在工具列上顯示「搜尋資產」方塊、輸入資產的類型或名稱、然後從顯示的清單中選取資產。

     隨即顯示「資產」頁面。
3. 在資產頁面的*使用者資料*區段中、按一下 ✚Add。

   此時會顯示「新增附註」對話方塊。
4. 按一下*註釋*、然後從清單中選取註釋。
5. 按一下*值*、然後根據您選取的註釋類型執行下列任一項：
   - 如果註釋類型為清單、日期或布林值、請從清單中選取一個值。
   - 如果註釋類型為文字、請輸入一個值。
6. 按一下「 * 儲存 * 」。

7. 如果您要在指派註釋後變更其值、請按一下 並選取不同的值。

   如果註釋屬於清單類型、且已選取「在註釋指派時動態新增值」選項、則除了選取現有值之外、您也可以輸入新值。

修改註釋

您可能想要變更註釋的名稱、說明或值、或是刪除不想再使用的註釋。

步驟

1. 登入OnCommand 到「無法使用者介面」。
2. 按一下「管理」、然後選取「註釋」。

   此時會顯示「附註」頁面。

3. 將游標放在您要編輯的附註上、然後按一下 。

   此時將顯示*編輯註釋*對話框。

4. 您可以對附註進行下列修改：

   a. 變更名稱、說明或兩者。

      不過、請注意、您最多可以輸入255個字元做為名稱和說明、而且無法變更任何附註的類型。此外、對於系統層級的註釋、您無法變更名稱或說明；不過、如果註釋是清單類型、您可以新增或移除值。

      > 如果自訂附註已發佈至資料倉儲並重新命名、您將會遺失歷史資料。

   a. 若要在清單類型的註釋中新增其他值、請按一下 Add 。
   b. 若要從清單類型的附註中移除值、請按一下 。

      如果註釋值與註釋規則、查詢或效能原則中包含的註釋相關聯、則無法刪除該註釋值。

5. 完成後單擊*保存*。

完成後

如果您要在資料倉儲中使用註釋、則必須強制更新資料倉儲中的註釋。請參閱《_ OnCommand Insight 資料倉儲管理指南_》。

刪除註釋

您可能想要刪除不再使用的註釋。您無法刪除註釋規則、查詢或效能原則中使用的系統層級註釋或註釋。

步驟

1. 登入OnCommand Insight 到The W不明 網路UI。

2. 按一下「管理」、然後選取「註釋」。

   此時會顯示「附註」頁面。

3. 將游標放在您要刪除的附註上、然後按一下 🗑 。

   隨即顯示確認對話方塊。

4. 按一下「確定」。

使用註釋規則指派註釋給資產

若要根據您定義的準則自動指派資產附註、請設定附註規則。根據這些規則、將註釋指派給資產OnCommand Insight 。Insight也提供兩種預設註釋規則、您可以根據需求進行修改、或是在不想使用時加以移除。

預設儲存附註規則

為了加速將儲存附註指派給資源、OnCommand Insight 包含21項預設附註規則、可將層級與儲存層模式建立關聯。在您的環境中擷取資產時、所有的儲存資源都會自動與某個層級建立關聯。

預設的附註規則會以下列方式套用階層附註：

- 第1層、儲存品質層

  第1層註釋適用於下列廠商及其指定系列：EMC（Symmetrix）、HDS（HDS9500V、HDS9900V、HDS9900V、R600、 R700、USP r、USP V）、IBM（DS8000）、NetApp（FAS6000或FAS6200）及Violin（記憶體）。

- 第2層、儲存品質層

  第2層註釋適用於下列廠商及其指定系列：HP（3PAR StoreServ或Eva）、EMC（CLARiiON）、HDS（AMS或D800）、IBM（XIV）及NetApp（FAS3000、FAS3100及FAS3200）。

您可以編輯這些規則的預設設定、以符合您的層級要求、也可以在不需要時移除這些設定。

建立註釋規則

您可以使用註釋規則、自動將註釋套用至多個資產、作為手動套用註釋至個別資產的替代方法。Insight評估註釋規則時、在個別資產頁面上手動設定的註釋優先於規則型註釋。

開始之前

您必須已建立註釋規則的查詢。

關於這項工作

雖然您可以在建立規則時編輯註釋類型、但應該事先定義類型。

步驟

1. 登入OnCommand Insight 到The W不明 網路UI。
2. 按一下「管理」、然後選取「註釋規則」。

   「附註規則」頁面會顯示現有附註規則的清單。

3. 按一下 ✚ Add 。

   此時會顯示「新增規則」對話方塊。

4. 請執行下列動作：
   a. 在*名稱*方塊中、輸入描述規則的唯一名稱。

      此名稱會顯示在「註釋規則」頁面中。

   b. 按一下「查詢」、然後選取OnCommand Insight 查詢、以便將評註套用至資產。
   c. 按一下*註釋*、然後選取您要套用的註釋。
   d. 按一下*值*、然後選取註釋的值。

      例如、如果您選擇「Birthday」做為註釋、則需指定值的日期。

5. 按一下「 * 儲存 * 」。
6. 如果您要立即執行所有規則、請按一下*執行所有規則*；否則、規則會以定期排程的時間間隔執行。

設定註釋規則優先順序

根據預設OnCommand Insight 、如果OnCommand Insight 您想讓Insight以特定順序評估規則、則可以依序評估附註規則、但是您可以設定以什麼順序來評估附註規則。

步驟

1. 登入InsightWeb UI。
2. 按一下「管理」、然後選取「註釋規則」。

   「附註規則」頁面會顯示現有附註規則的清單。

3. 將游標放在註釋規則上。

   優先順序箭頭會出現在規則的右側。

4. 若要在清單中上下移動規則、請按一下向上箭頭或向下箭頭。

   根據預設、新規則會依序新增至規則清單。Insight評估註釋規則時、在個別資產頁面上手動設定的註釋優先於規則型註釋。

修改註釋規則

您可以修改附註規則、以變更規則名稱、其附註、附註值或與規則相關的查詢。

步驟

1. 登入OnCommand 到「無法使用者介面」。
2. 按一下「管理」、然後選取「註釋規則」。

   「附註規則」頁面會顯示現有附註規則的清單。

3. 找出您要修改的規則：
   - 在「附註規則」頁面上、您可以在篩選方塊中輸入值來篩選附註規則。
   - 如果頁面上有超出頁面大小的規則、請按一下頁碼、逐頁瀏覽註釋規則。
4. 執行下列其中一項以顯示「編輯規則」對話方塊：
   - 如果您在「附註規則」頁面上、請將游標放在附註規則上、然後按一下 。
   - 如果您在資產頁面上、請將游標放在與規則相關的註釋上、並在顯示規則名稱時將游標放在規則名稱上、然後按一下規則名稱。
5. 進行必要的變更、然後按一下*「Save（儲存）」*。

刪除註釋規則

當不再需要規則來監控網路中的物件時、您可以刪除註釋規則。

步驟

1. 登入OnCommand 到「無法使用者介面」。
2. 按一下*管理*、然後選取*註釋規則*。

   「附註規則」頁面會顯示現有附註規則的清單。

3. 找出您要刪除的規則：
   - 在「附註規則」頁面上、您可以在篩選方塊中輸入值來篩選附註規則。
   - 如果單一頁面上的規則超過頁面大小、請按一下頁碼、逐頁瀏覽註釋規則。
4. 將游標指向您要刪除的規則、然後按一下 。

   隨即顯示確認訊息、提示您是否要刪除規則。

5. 按一下「確定」。

匯入註釋值

如果您在CSV檔案中保留SAN物件（例如儲存設備、主機和虛擬機器）的附註、您可以將該資訊匯入OnCommand Insight 到VMware。您可以匯入應用程式、商業實體或註釋、例如階層和建置。

關於這項工作

適用下列規則：

- 如果註釋值為空白、則該註釋會從物件中移除。
- 在註釋磁碟區或內部磁碟區時、物件名稱是使用破折號和箭頭（->）分隔符號的儲存名稱和磁碟區名稱組合：

```
<storage_name>-><volume_name>
```

- 儲存設備、交換器或連接埠註解時、應用程式欄會被忽略。
- 租戶、Line__of_Business、Business_Unit和Project等欄位組成企業實體。

  任何值都可以保留空白。如果應用程式已與不同於輸入值的企業實體相關、則應用程式會指派給新的企業實體。

匯入公用程式支援下列物件類型和金鑰：

類型	金鑰
主機	id-><id> 或 <Name> 或 <IP>
VM	id-><id> 或 <Name>
儲存資源池	id-><id> 或 <Storage_name>-><Storage_Pool_name>
內部Volume	id-><id> 或 <Storage_name>-><Internal_volume_name>
Volume	id-><id> 或 <Storage_name>-><Volume_name>
儲存設備	id-><id> 或 <Name> 或 <IP>
交換器	id-><id> 或 <Name> 或 <IP>
連接埠	id-><id> 或 <WWN>
分享	id-><id> 或 <Storage Name>-><Internal Volume Name>-><Share Name>-><Protocol><Qtree> 如果有預設qtree、則為選用。
qtree	id-><id> 或 <Storage Name>-><Internal Volume Name>-><Qtree Name>

CSV檔案應使用下列格式：

```
, , <Annotation Type> [, <Annotation Type> ...]
[, Application] [, Tenant] [, Line_Of_Business] [,
Business_Unit] [, Project]

<Object Type Value 1>, <Object Key 1>, <Annotation Value> [,
<Annotation Value> ...] [, <Application>] [, <Tenant>] [,
<Line_Of_Business>] [, <Business_Unit>] [, <Project>]

...

<Object Type Value N>, <Object Key N>, <Annotation Value> [,
<Annotation Value> ...] [, <Application>] [, <Tenant>] [,
<Line_Of_Business>] [, <Business_Unit>] [, <Project>]
```

步驟

1. 登入Insight Web UI。
2. 單擊*管理*並選擇*疑難排解*。

   隨即顯示「疑難排解」頁面。

3. 在頁面的*其他工作區段*中、按一下* OnCommand Insight 《Portal》*連結。
4. 按一下「* Insight Connect API*」。
5. 登入入口網站。
6. 按一下*註釋匯入公用程式*。
7. 儲存 `.zip` 將檔案解壓縮、然後讀取 `readme.txt` 檔案以取得更多資訊和範例。
8. 將CSV檔案放在與相同的資料夾中 `.zip` 檔案：
9. 在命令列視窗中、輸入下列命令：

   ```
   java -jar rest-import-utility.jar [-uusername] [-ppassword]
   [-aserver name or IP address] [-bbatch size] [-ccase
   sensitive:true/false]
   [-lextra logging:true/false] csv filename
   ```

   啟用額外記錄的-l選項和啟用區分大小寫的-c選項預設為假。因此、您只能在想要使用這些功能時才指定這些功能。

   > 選項與其值之間沒有空格。

下列關鍵字會保留、並防止使用者將其指定為註釋名稱：-應用程式- Application_Priority -租戶- Line__of_Business - Business_Unit -如果您嘗試使用其中一個保留關鍵字匯入註釋類型、就會產生專案錯誤。如果您已使用這些關鍵字建立註釋名稱、則必須加以修改、以便匯入公用程式工具能夠正常運作。

註釋匯入公用程式需要 Java 8 或 Java 11 。在執行匯入公用程式之前、請先確定已安裝其中一項。建議使用最新的 OpenJDK 11 。

使用查詢指派附註給多個資產

將註釋指派給一組資產、有助於更輕鬆地識別或使用查詢或儀表板中的相關資產。

開始之前

您想要指派給資產的附註必須是先前建立的。

關於這項工作

您可以使用查詢來簡化指派附註給多個資產的工作。例如、如果您想要將自訂位址附註指派給位於特定資料中心位置的所有陣列。

步驟

1. 建立新的查詢、以識別您要指派附註的資產。按一下*查詢*>*+新查詢*。
2. 在「搜尋...」下拉式清單中、選擇「儲存設備」。您可以設定篩選條件、進一步縮小所顯示的儲存清單範圍。
3. 在顯示的儲存清單中、按一下儲存名稱旁的核取方塊、選取一或多個儲存區。您也可以按一下清單頂端的主核取方塊、選取所有顯示的儲存。
4. 選取所有想要的儲存後、請按一下「動作」>「編輯註釋」。

   系統會顯示「新增附註」對話方塊。

5. 選擇要指派給儲存體的*註釋*和*值*、然後按一下*儲存*。

   如果您要顯示該註釋的欄位、該欄位會顯示在所有選取的儲存區上。

6. 您現在可以使用附註來篩選小工具或查詢中的儲存。在小工具中、您可以執行下列動作：

   a. 建立儀表板或開啟現有儀表板。新增*變數*、然後選擇您在上述儲存區上設定的註釋。變數隨即新增至儀表板。
   b. 在您剛新增的變數欄位中、按一下*任一*、然後輸入適當的篩選值。按一下核取標記以儲存變數值。
   c. 新增小工具。在小工具的查詢中、按一下「**篩選依據」（0+）按鈕、然後從清單中選取適當的註釋。
   d. 按一下*任一*、然後選取您在上方新增的註釋變數。您建立的變數以「$$」開頭、並顯示在下拉式清單中。
   e. 設定您想要的任何其他篩選器或欄位、然後在您想要自訂小工具時按一下*「儲存」*。

   儀表板上的小工具只會顯示您指派附註的儲存設備資料。

查詢資產

查詢可讓您根據使用者選擇的條件（註釋和效能指標）、以精細的層級搜尋環境中的資產、藉此監控和疑難排解網路。此外、註釋規則會自動指派註釋給資產、因此需要查詢。

用於查詢和儀表板的資產

Insight查詢和儀表板小工具可搭配各種資產類型使用

下列資產類型可用於查詢、儀表板小工具和自訂資產頁面。篩選器、運算式和顯示可用的欄位和計數器會因資產類型而異。並非所有資產都可用於所有小工具類型。

- 應用程式
- 資料存放區
- 磁碟
- 網路
- 一般裝置
- 主機
- 內部Volume
- iSCSI工作階段
- iSCSI網路入口網站
- 路徑
- 連接埠
- qtree
- 配額
- 分享
- 儲存設備
- 儲存節點
- 儲存資源池
- 交換器
- 磁帶
- VMDK
- 虛擬機器
- Volume
- 區域
- 區域成員

建立查詢

您可以建立查詢、讓您以精細的層級搜尋環境中的資產。查詢可讓您新增篩選條件、然後排序結果、以便在單一檢視畫面中檢視庫存和效能資料、藉此分割資料。

關於這項工作

例如、您可以建立磁碟區查詢、新增篩選器以尋找與所選磁碟區相關的特定儲存區、新增篩選器以尋找所選儲存區上的特定附註、例如層級1、 最後新增另一個篩選器、找出IOPS大於25的所有儲存區。顯示結果時、您可以依遞增或遞減順序排序與查詢相關的資訊欄。

新增的資料來源會擷取資產、或是進行任何註釋或應用程式指派時、您可以在查詢建立索引之後、查詢這些資產、註釋或應用程式、這些資料會在定期排程的時間間隔內發生。

步驟

1. 登入OnCommand Insight 到The W不明 網路UI。
2. 按一下「查詢」、然後選取「**+**新查詢」。
3. 按一下*選取資源類型*、然後選取一種資產類型。

   選取查詢的資源時、會自動顯示許多預設欄位；您可以隨時移除這些欄位或新增欄位。

4. 在*名稱*文字方塊中、輸入資產名稱、或輸入部分文字以篩選資產名稱。

   您可以單獨或合併使用下列任一項目、在「新增查詢」頁面的任何文字方塊中精簡搜尋：

   - 星號可讓您搜尋所有內容。例如、 `vol*rhel` 顯示以「'vol'」開頭並以「'RHEL」結尾的所有資源。
   - 問號可讓您搜尋特定的字元數。例如、 `BOS-PRD??-S12` 顯示BOS-PRD12-S12、BOS-PRD13-S12等。
   - 或運算子可讓您指定多個實體。例如、 `FAS2240 OR CX600 OR FAS3270` 尋找多種儲存模式。
   - Not運算子可讓您從搜尋結果中排除文字。例如、 `NOT EMC*` 找到開頭不是「'eme'」的所有項目。您可以使用 `NOT *` 顯示無值的欄位。

5. 按一下 ✔ 以顯示資產。
6. 若要新增準則、請按一下 More ▾ ，然後執行下列其中一項：

   - 輸入以搜尋特定條件、然後選取該條件。
   - 向下捲動清單、然後選取條件。
   - 如果您選擇IOPS -讀取（IO/s）等效能指標、請輸入一系列值。Insight提供的預設註釋會以表示 🏷 ；註釋可能具有重複的名稱。

   清單中查詢的準則和結果會新增一欄至查詢結果清單。

7. 您也可以按一下 ▦ 可從查詢結果中刪除註釋或性能指標。

   例如、如果您的查詢顯示資料存放區的最大延遲和最大處理量、而您想在查詢結果清單中只顯示最大延遲、請按一下此按鈕、然後清除*處理量-最大*核取方塊。「Throued - Max（MB/s）（處理量-最大（MB/s）

）」欄會從「Query Results（查詢結果）」清單中移除。

> 根據查詢結果表格中顯示的欄數、您可能無法檢視其他新增的欄。您可以移除一或多個欄、直到所需的欄顯示為止。

8. 按一下「儲存」、輸入查詢名稱、然後再按一下「儲存」。

   如果您的帳戶具有系統管理員角色、則可以建立自訂儀表板。自訂儀表板可由Widget程式庫中的任何小工具組成、其中有幾個小工具可讓您在自訂儀表板中呈現查詢結果。如需自訂儀表板的詳細資訊、請參閱《_OnCommand Insight 關於使用入門指南》_。

相關資訊

"匯入及匯出使用者資料"

檢視查詢

您可以檢視查詢來監控資產、並變更查詢顯示資產相關資料的方式。

步驟

1. 登入OnCommand Insight 到The W不明 網路UI。
2. 按一下*查詢*、然後選取*顯示所有查詢*。
3. 您可以執行下列任一動作來變更查詢的顯示方式：
   - 您可以在*篩選*方塊中輸入文字、以搜尋以顯示特定查詢。
   - 您可以按一下欄標題中的箭號、將查詢表中欄的排序順序變更為遞增（向上箭頭）或遞減（向下箭頭）。
   - 若要調整欄位大小、請將滑鼠游標暫留在欄標題上、直到出現藍色列為止。將滑鼠放在長條上、然後左右拖曳。
   - 若要移動欄、請按一下欄標題、然後向右或左拖曳。
   - 捲動查詢結果時、請注意Insight會自動輪詢您的資料來源、結果可能會有所變更。這可能會導致某些項目遺失、或是某些項目出現順序不正常、視其排序方式而定。

將查詢結果匯出至.CSV檔案

您可能想要將查詢結果匯出至.CSV檔案、以便將資料匯入其他應用程式。

步驟

1. 登入OnCommand Insight 到The W不明 網路UI。
2. 按一下*查詢*、然後選取*顯示所有查詢*。

   隨即顯示「查詢」頁面。

3. 按一下查詢。
4. 按一下 ⬆ 將查詢結果匯出至`.CSV` 檔案：

5. 執行下列其中一項：
   - 按一下「開啟方式」、然後按一下「確定」、以Microsoft Excel開啟檔案、並將檔案儲存至特定位置。
   - 按一下*「Save file*（儲存檔案*）」、然後按*「OK*（確定）」將檔案儲存至「Downloads（下載）」資料夾。只會匯出顯示欄的屬性。某些顯示的欄位、尤其是屬於複雜巢狀關係的欄位、不會匯出。

     > 當資產名稱中出現一個逗號時、匯出會以引號括住名稱、並保留資產名稱和適當的.csf格式。

     +匯出查詢結果時、請注意、結果表中的*全部*列將會匯出、而不只是畫面上選取或顯示的列、最多可匯出10、000列。

使用Excel開啟匯出的.CSV檔案時、如果您有NN格式的物件名稱或其他欄位（兩位數加上一個分號、再加上兩位數）、Excel有時會將該名稱解譯為時間格式、而非文字格式。這可能導致Excel在這些欄中顯示不正確的值。例如、在Excel中、名為「81：45」的物件會顯示為「81：45：00」。若要解決此問題、請使用下列步驟將.CSV匯入Excel：

+

```
-   Open a new sheet in Excel.
-   On the "Data" tab, choose "From Text".
-   Locate the desired .CSV file and click "Import".
-   In the Import wizard, choose "Delimited" and click Next.
-   Choose "Comma" for the delimiter and click Next.
-   Select the desired columns and choose "Text" for the column data
format.
-   Click Finish.
Your objects should show in Excel in the proper format.
```

+

修改查詢

當您想要變更查詢資產的搜尋準則時、可以變更與查詢相關的準則。

步驟

1. 登入InsightWeb UI。
2. 按一下*查詢*、然後選取*顯示所有查詢*。

   隨即顯示「查詢」頁面。
3. 按一下查詢名稱。
4. 若要從查詢中移除準則、請按一下 🗑 。
5.

若要新增條件至查詢、請按一下 More ，然後從清單中選取條件。

6. 執行下列其中一項：
   - 按一下「儲存」、以最初使用的名稱儲存查詢。
   - 按一下*「另存新檔」*、以其他名稱儲存查詢。
   - 按一下*重新命名*以變更您最初使用的查詢名稱。
   - 按一下*還原*、將查詢名稱變更回您最初使用的名稱。

刪除查詢

當查詢不再收集有關您資產的實用資訊時、您可以刪除查詢。如果查詢用於註釋規則、則無法刪除查詢。

步驟

1. 登入InsightWeb UI。
2. 按一下*查詢*、然後選取*顯示所有查詢*。

   隨即顯示「查詢」頁面。

3. 將游標放在您要刪除的查詢上、然後按一下 🗑 。

   隨即顯示確認訊息、詢問您是否要刪除查詢。

4. 按一下「確定」。

將多個應用程式指派給資產、或從資產中移除多個應用程式

您可以使用查詢來指派多個應用程式給資產、或是從資產中移除多個應用程式、而不必手動指派或移除這些應用程式。

開始之前

您必須已建立查詢、以尋找所有要編輯的資產。

步驟

1. 按一下*查詢*、然後選取*顯示所有查詢*。

   隨即顯示「查詢」頁面。

2. 按一下尋找資產的查詢名稱。

   隨即顯示與查詢相關的資產清單。

3. 在清單中選取所需的資產、或按一下 ☐ ▾ 選擇*全部*。

   將顯示* Actions （操作）按鈕。

4. 若要將應用程式新增至所選資產、請按一下 Actions ，然後選取*編輯應用程式*。
   a. 按一下*應用程式*、然後選取一或多個應用程式。

      您可以為主機、內部磁碟區和虛擬機器選取多個應用程式、不過、您只能為一個磁碟區選取一個應用程式。

   b. 按一下「 * 儲存 * 」。
5. 若要移除指派給資產的應用程式、請按一下 Actions 然後選取*移除應用程式*。
   a. 選取您要移除的應用程式。
   b. 按一下*刪除*。

   您指派的任何新應用程式、都會覆寫從其他資產衍生的資產上的任何應用程式。例如、磁碟區會從主機繼承應用程式、當新的應用程式指派給磁碟區時、新的應用程式會優先於衍生的應用程式。

編輯或移除資產中的多個附註

您可以使用查詢來編輯資產的多個附註、或是移除資產的多個附註、而不必手動編輯或移除這些附註。

開始之前

您必須已經建立查詢、以尋找您要編輯的所有資產。

步驟

1. 按一下*查詢*、然後選取*顯示所有查詢*。

   隨即顯示「查詢」頁面。

2. 按一下尋找資產的查詢名稱。

   隨即顯示與查詢相關的資產清單。

3. 在清單中選取所需的資產、或按一下 ☐ 選擇*全部*。

   將顯示* Actions （操作）按鈕。

4. 若要新增資產附註或編輯指派給資產的附註值、請按一下 Actions ，然後選取*編輯註釋*。
   a. 按一下*註釋*並選取您要變更值的註釋、或選取新註釋以將其指派給所有資產。
   b. 按一下*值*、然後選取註釋的值。
   c. 按一下「 * 儲存 * 」。
5. 若要移除指派給資產的附註、請按一下 Actions ，然後選取*移除註釋*。
   a. 按一下*註釋*、然後選取您要從資產中移除的註釋。
   b. 按一下*刪除*。

複製表格值

您可以複製表格中的值、以便用於搜尋方塊或其他應用程式。

關於這項工作

您可以使用兩種方法從資料表或查詢結果複製值。

步驟

1. 方法1：使用滑鼠反白所需的文字、複製並貼到搜尋欄位或其他應用程式中。
2. 方法2：對於長度超過表格欄寬（以省略符號（...）表示）的單值欄位、請將游標移到欄位上、然後按一下剪貼簿圖示。此值會複製到剪貼簿、以便用於搜尋欄位或其他應用程式。

   請注意、只能複製資產連結的值。另請注意、只有包含單一值（例如非清單）的欄位才會顯示複本圖示。

管理效能原則

利用此功能、您可以建立效能原則、監控網路的各種臨界值、並在超過臨界值時發出警示OnCommand Insight 。使用效能原則、您可以立即偵測違反臨界值的情況、識別影響、並以能夠快速有效修正的方式分析問題的影響和根本原因。

效能原則可讓您設定任何物件（資料存放區、磁碟、Hypervisor、內部Volume、連接埠、 儲存設備、儲存節點、儲存資源池、VMDK、虛擬機器、 和Volume）、以及報告的效能計數器（例如總IOPS）。發生違反臨界值的情況時、Insight會在相關的資產頁面中偵測並報告臨界值、顯示紅色的實體圓圈、透過電子郵件警示（若已設定）、以及違規儀表板或任何報告違規的自訂儀表板。

Insight針對下列物件提供一些預設效能原則、如果這些原則不適用於您的環境、您可以加以修改或刪除：

- Hypervisor

  有ESX交換和ESX使用率原則。

- 內部Volume與Volume

  每個資源都有兩個延遲原則、一個是層級1的註釋、另一個是層級2的註釋。

- 連接埠

  有一項設定為零寬帶點數的原則。

- 儲存節點

  有一個節點使用率原則。

- 虛擬機器

  有VM交換、ESX CPU和記憶體原則。

- Volume

依層級和未對齊的Volume原則而定、會有延遲。

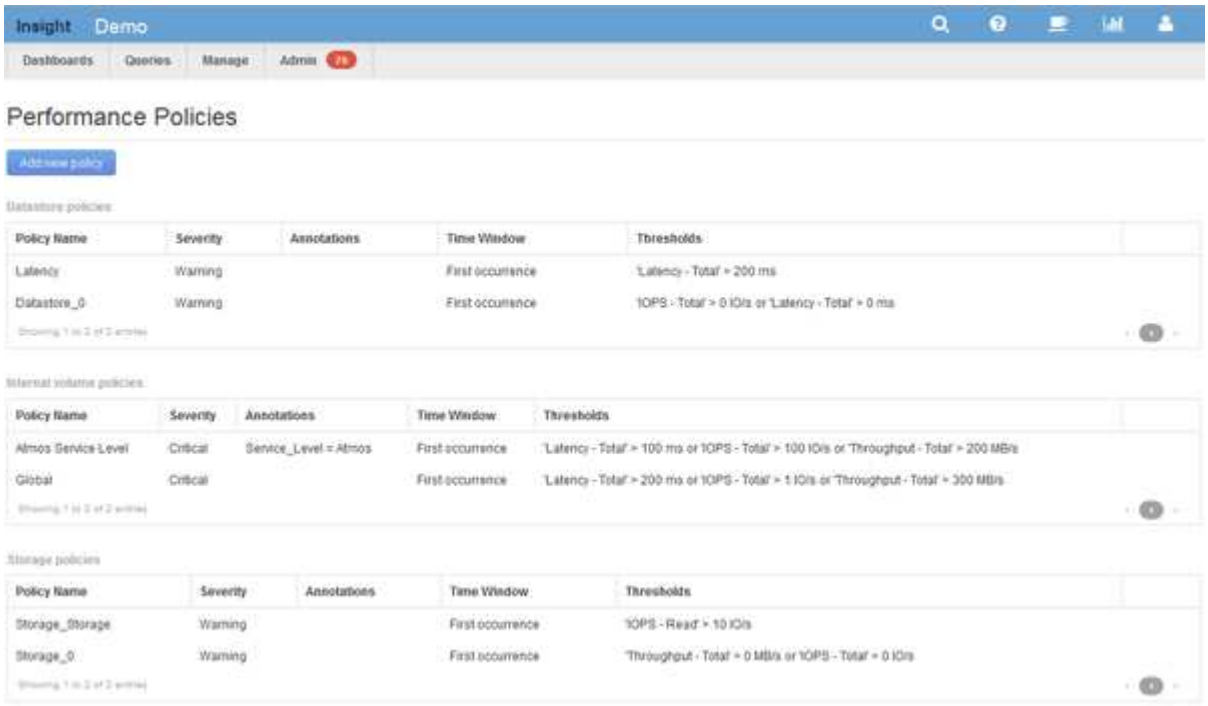
建立效能原則

您可以建立效能原則來設定觸發警示的臨界值、以通知您有關網路資源的問題。例如、您可以建立效能原則、在儲存資源池的總使用率超過60%時發出警示。

步驟

1. 在OnCommand Insight 瀏覽器中開啟
2. 選擇*管理*>*效能原則*。

   隨即顯示「效能原則」頁面。



   原則會依物件組織、並依照原則在清單中出現的順序進行評估。

3. 按一下「新增原則」。

   此時會顯示「新增原則」對話方塊。

4. 在*原則名稱*欄位中、輸入原則的名稱。

   您必須使用不同於物件所有其他原則名稱的名稱。例如、內部磁碟區不能有兩個名為「延遲」的原則、不過內部磁碟區可以有「延遲」原則、而另一個磁碟區則有「延遲」原則。最佳實務做法是永遠為任何原則使用唯一名稱、無論物件類型為何。

5. 從「*套用至類型*的物件」清單中、選取套用原則的物件類型。
6. 從「含註釋」清單中、選取註釋類型（若適用）、然後在「值」方塊中輸入註釋的值、以僅將原則套用至已設定此特定註釋的物件。
7. 如果您選取*連接埠*做為物件類型、請從*連接至*清單中、選取連接埠的連接目標。

8. 從「套用後的時間」清單中、選取警示提出以指出違反臨界值的時間。

   第一次發生選項會在第一次資料樣本超過臨界值時觸發警示。當臨界值超過一次且持續超過指定時間、所有其他選項都會觸發警示。

9. 從「含嚴重性」清單中、選取違規的嚴重性。
10. 根據預設、系統會將違反原則的電子郵件警示傳送給全域電子郵件清單中的收件者。您可以覆寫這些設定、以便將特定原則的警示傳送給特定的收件者。
    - 按一下連結以開啟收件者清單、然後按一下「**+**」按鈕以新增收件者。該原則的違規警示將傳送給清單中的所有收件者。
11. 按一下「*建立警示（如果下列任一項為真）」區段中的*任一*連結、以控制警示的觸發方式：
    - 任何

      這是預設設定、會在超過任何與原則相關的臨界值時建立警示。

    - 全部

      此設定會在超過原則的所有臨界值時建立警示。當您選取*全部*時、您為效能原則建立的第一個臨界值即稱為主要規則。您必須確保主要規則臨界值是您最關心效能原則的違規行為。

12. 在「建立警示條件」區段中、選取效能計數器和運算子、然後輸入值以建立臨界值。
13. 按一下*新增臨界值*以新增更多臨界值。
14. 若要移除臨界值、請按一下垃圾桶圖示。
15. 如果您希望原則在發生警示時停止處理、請選取「如果產生警示、則停止處理其他原則*」核取方塊。

    例如、如果您有四個資料存放區原則、而第二個原則設定為在發生警示時停止處理、則第三個和第四個原則不會在發生違反第二個原則的情況下處理。

16. 按一下「 * 儲存 * 」。

    隨即顯示「效能原則」頁面、且效能原則會出現在物件類型的原則清單中。

效能原則評估優先

「效能原則」頁面會依物件類型將原則分組、而Insight會根據原則在物件效能原則清單中的顯示順序來評估原則。您可以變更Insight評估原則的順序、以顯示網路中最重要的資訊。

Insight會在將效能資料範例帶入系統時、依序評估適用於某個物件的所有原則；不過、根據註釋的不同、並非所有原則都會套用至某個物件群組。例如、假設內部Volume具有下列原則：

- 原則1（Insight提供的預設原則）
- 原則2（附有「服務層級=銀級」註釋、並附有*如果產生警示、請停止處理其他原則*選項
- 政策3（附註「服務層級=金級」）
- 原則4.

對於具有Gold附註的內部磁碟區層、Insight會評估原則1、忽略原則2、然後評估原則3和原則4。對於未註釋的階層、Insight會根據原則的順序進行評估、因此Insight只會評估原則1和原則4。對於具有Silver註釋的內部Volume階層、Insight會評估原則1和原則2； 不過、如果在超過原則臨界值一次且持續超過原則中指定的時間範圍時觸發警示、則Insight將不再評估清單中的其他原則、而會評估物件的目前計數器。當Insight擷取物件的下一組效能範例時、會再次開始依篩選條件評估物件的效能原則、然後再依順序排序。

變更效能原則的優先順序

依預設、Insight會依序評估物件的原則。您可以設定Insight評估效能原則的順序。例如、如果您已設定原則、在Gold層級儲存設備發生違規時停止處理、您可以將該原則放在清單的第一位、避免看到同一儲存資產發生更多一般違規。

步驟

1. 在瀏覽器中開啟Insight。
2. 從*管理*功能表中、選取*效能原則*。

   隨即顯示「效能原則」頁面。

3. 將游標停留在物件類型效能原則清單中的原則名稱上。

   優先順序箭頭會出現在原則右側。

4. 若要在清單中向上移動原則、請按一下向上箭頭；若要在清單中向下移動原則、請按一下向下箭頭。

   根據預設、新原則會依序新增至物件的原則清單。

編輯效能原則

您可以編輯現有和預設的效能原則、以變更Insight監控網路中您感興趣的條件。例如、您可能想要變更原則的臨界值。

步驟

1. 在瀏覽器中開啟Insight。
2. 從*管理*功能表中、選取*效能原則*。

   隨即顯示「效能原則」頁面。

3. 將游標停留在物件效能原則清單中的原則名稱上。
4. 按一下 。

   隨即顯示「編輯原則」對話方塊。

5. 進行必要的變更。

   如果您變更原則名稱以外的任何選項、Insight會刪除該原則的所有現有違規。

6. 按一下「儲存。」

刪除效能原則

如果您認為效能原則不再適用於監控網路中的物件、可以刪除該原則。

步驟

1. 在瀏覽器中開啟Insight。
2. 從*管理*功能表中、選取*效能原則*。

   隨即顯示「效能原則」頁面。

3. 將游標停留在物件效能原則清單中的原則名稱上。
4. 按一下 ✖。

   此時會出現一則訊息、詢問您是否要刪除原則。

5. 按一下「確定」。

匯入及匯出使用者資料

匯入和匯出功能可讓您將註釋、註釋規則、查詢、效能原則和自訂儀表板匯出至一個檔案。此檔案可匯入至不同OnCommand Insight 的伺服器。

只有在執行相同版本OnCommand Insight 的伺服器之間才支援匯出和匯入功能。

若要匯出或匯入使用者資料、請按一下*管理*並選取*設定*、然後選擇*匯入/匯出使用者資料*索引標籤。

在匯入作業期間、會根據匯入的物件和物件類型、新增、合併或取代資料。

- 註釋類型
  - 如果目標系統中不存在名稱相同的註釋、請新增註釋。
  - 如果註釋類型為清單、則會合併註釋、且目標系統中存在名稱相同的註釋。
  - 如果註釋類型不是清單、且目標系統中存在名稱相同的註釋、則會取代註釋。

  > ⓘ 如果目標系統中存在名稱相同但類型不同的附註、則匯入會失敗。如果物件取決於失敗的附註、這些物件可能會顯示不正確或不想要的資訊。匯入作業完成後、您必須檢查所有註釋相依性。

- 註釋規則
  - 如果目標系統中不存在名稱相同的註釋規則、請新增註釋規則。
  - 如果目標系統中存在名稱相同的註釋規則、則會取代註釋規則。

  > ⓘ 註釋規則取決於查詢和註釋。匯入作業完成後、您必須檢查所有註釋規則的準確度。

- 原則

- 如果目標系統中不存在名稱相同的原則、請新增原則。
- 如果目標系統中存在名稱相同的原則、則會取代原則。

> 匯入作業完成後、原則可能會不正常。匯入後、您必須檢查原則順序。如果註釋不正確、則相依於註釋的原則可能會失敗。您必須在匯入後檢查所有註釋相依性。
>
> +

- 查詢
  - 如果目標系統中不存在名稱相同的查詢、則新增查詢。
  - 如果目標系統中存在名稱相同的查詢、即使查詢的資源類型不同、也會取代查詢。

> 如果查詢的資源類型不同、則在匯入之後、使用該查詢的任何儀表板小工具都可能顯示不必要或不正確的結果。匯入後、您必須檢查所有查詢型Widget的準確度。如果註釋不正確、則相依於註釋的查詢可能會失敗。您必須在匯入後檢查所有註釋相依性。
>
> +

- 儀表板
  - 如果目標系統中不存在名稱相同的儀表板、請新增儀表板。
  - 如果目標系統中存在名稱相同的儀表板、即使查詢的資源類型不同、也會取代儀表板。

> 匯入後、您必須檢查儀表板中所有查詢型Widget的準確度。如果來源伺服器有多個名稱相同的儀表板、則會全部匯出。不過、只有第一個會匯入目標伺服器。為了避免在匯入期間發生錯誤、您應該在匯出儀表板之前、先確定其名稱是唯一的。
>
> +