組態與管理
OnCommand Insight

NetApp
October 24, 2024

This PDF was generated from https://docs.netapp.com/zh-tw/oncommand-insight/config-admin/opening-insight.html on October 24, 2024. Always check docs.netapp.com for the latest.

目錄

組態與管理 1
設定Insight 1
Insight Security 88
智慧卡與憑證登入支援 113
設定資料倉儲以進行智慧卡和憑證登入 122
設定Cognos以登入智慧卡和憑證（OnCommand Insight 更新版本： 123
匯入Cognos和DWH的CA簽署SSL憑證（Insight 7.3.10及更新版本） 125
匯入SSL憑證 127
您的企業實體階層架構 129
定義註釋 132
查詢資產 145
Insight資料來源管理 152
裝置解析度 247
維持洞見 264
監控環境 285
OCI 資料收集器支援對照表 311

組態與管理

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：

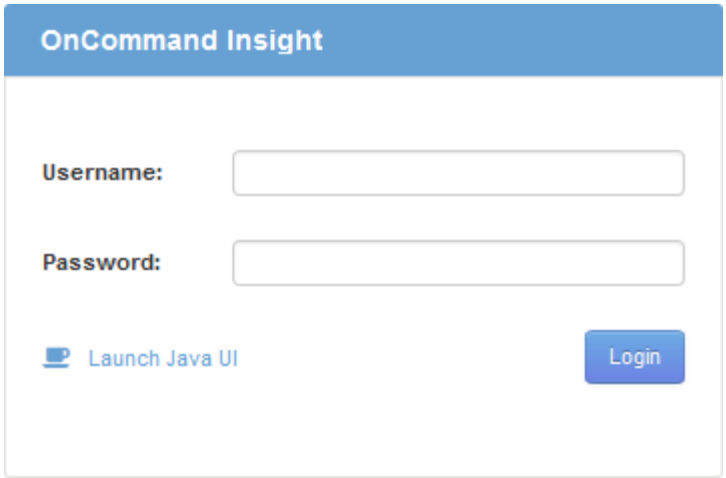
     ```
     https://fqdn
     ```

   - 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。

> 如果您正在匯入 LDAP 憑證、並使用變更 *server.keystore* 和 / 或 *_server.trustore* 密碼"安全性管理"、請 *SANscreen* 在匯入 *LDAP* 憑證之前重新啟動 *_LDAP* 服務。

> 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。

> 如果您使用變更 _server.keystore 和 / 或 _server.trustore 密碼"安全性管理"、請在匯入 LDAP 憑證之前重新啟動 SANscreen 服務。

> 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。

> 如果您使用變更 _server.keystore 和 / 或 _server.trustore 密碼"安全性管理"、請在匯入 LDAP 憑證之前重新啟動 SANscreen 服務。

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。
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。

安全性管理工具

OnCommand Insight 提供的功能可讓 Insight 環境以增強的安全性運作。這些功能包括加密、密碼雜湊、以及變更內部使用者密碼和密碼加密和解密金鑰配對的能力。您可以使用 **securityadmin Tool** 在 Insight 環境中的所有伺服器上管理這些功能。

什麼是安全性管理工具？

安全性管理工具支援變更資料保險箱的內容、以及協調一致地變更 OnCommand Insight 安裝。

安全性管理工具的主要用途是 * 備份 * 和 * 還原 * 安全性組態（即資料保險箱）和密碼。例如、您可以在本機擷取單元上備份資料保險箱、並在遠端擷取單元上還原資料保險箱、確保整個環境都能協調密碼。或者、如果您的環境中有多部 OnCommand Insight 伺服器、您可能需要備份伺服器資料保險箱、並將其還原至其他伺服器、以保持密碼相同。以下只是安全性管理可用於確保環境內凝聚力的兩個範例。

> 強烈建議您在備份 OnCommand Insight 資料庫時 * 備份資料保險箱 * 。否則可能導致存取中斷。

此工具同時提供 * 互動 * 和 * 命令列 * 模式。

許多 securityadmin Tool 作業會變更資料保險箱的內容、也會變更安裝、確保資料保險箱和安裝保持同步。

例如、

- 當您變更 Insight 使用者密碼時、 SANscreen 。 Users 表格中的使用者項目將會以新的雜湊更新。
- 當您變更 MySQL 使用者密碼時、將會執行適當的 SQL 陳述式、以更新 MySQL 執行個體中的使用者密碼。

在某些情況下、會對安裝進行多項變更：

- 修改 dwh MySQL 使用者時、除了更新 MySQL 資料庫中的密碼之外、也會更新多個 ODBC 登錄項目。

在下列各節中、使用「協調式變更」一詞來描述這些變更。

執行模式

- 正常 / 預設操作 - SANscreen 伺服器服務必須執行

  對於默認執行模式， securityadmin Tool 要求 SANscreen 服務器服務 * 正在運行。伺服器用於驗證、許多協調一致的安裝變更都是透過呼叫伺服器來進行。

- 直接操作 - SANscreen 伺服器服務可能正在執行或停止。

  在 OCI 伺服器或 DWH 安裝上執行時、工具也可以在「直接」模式下執行。在此模式中、驗證和協調變更是使用資料庫來執行。未使用伺服器服務。

  操作與一般模式相同、但有下列例外：

- 驗證僅支援非網域管理員使用者。（密碼和角色位於資料庫中的使用者、而非 LDAP ）。
- 不支援「置換金鑰」操作。
- 會略過資料保險箱還原的重新加密步驟。
- 恢復模式即使無法同時存取伺服器和資料庫、也可能執行此工具（例如、因為資料保險箱中的根密碼不正確）。

  在此模式下執行時、無法進行驗證、因此無法執行協調變更安裝的作業。

  恢復模式可用於：

- 判斷哪些資料保險箱項目錯誤（使用驗證作業）
- 請以正確的值取代不正確的根密碼。（這不會變更密碼。使用者必須輸入目前的密碼。）

> 如果資料保險箱中的根密碼不正確、而且密碼未知、而且沒有正確的根密碼備份資料保險箱、則無法使用 securityadmin Tool 還原安裝。恢復安裝的唯一方法是按照中介紹的步驟重置 MySQL 實例的密碼 https://dev.mysql.com/doc/refman/8.4/en/resetting-permissions.html。執行重設程序後、請使用正確的儲存密碼操作、將新密碼輸入資料保險箱。

命令

無限制命令

無限制命令會對安裝進行任何協調的變更（信任存放區除外）。不受限制的命令可在不進行使用者驗證的情況下執行。

命令	說明
備份資料保險箱	建立包含資料保險箱的 zip 檔案。至資料保險箱檔案的相對路徑將與相對於安裝根目錄的資料保險箱路徑相符。 • Wildfly / 獨立 / 組態 / 資料保險箱 / * • ACQ/conf/vVault/* 請注意，強烈建議您在備份 OnCommand Insight 資料庫時備份資料保險箱。
檢查預設金鑰	檢查資料保險箱的金鑰是否與 7.3.16 之前版本中使用的預設資料保險箱金鑰相符。
正確儲存的密碼	以使用者已知的正確密碼取代儲存在資料保險箱中的（不正確）密碼。 當資料保險箱和安裝不一致時、可能會使用此選項。* 請注意、它不會變更安裝中的實際密碼。 *
	change-trust 儲存區密碼變更用於信任儲存區的密碼、並將新密碼儲存在資料保險箱中。信任存放區的目前密碼必須為「已知」。
驗證 Keystore	檢查資料保險箱中的值是否正確： • 對於 OCI 使用者、密碼雜湊是否與資料庫中的值相符 • 對於 MySQL 使用者、可以建立資料庫連線 • 對於 Keystore 、是否可以載入 Keystore 及其金鑰（如果有）讀取
清單鍵	列出資料保險箱中的項目（不顯示儲存的值）

受限命令

任何對安裝進行協調變更的非隱藏命令都需要驗證：

命令	說明
還原資料保險箱備份	以包含在指定資料保險箱備份檔案中的資料保險箱取代目前的資料保險箱。 執行所有協調的動作來更新安裝以符合還原資料保險箱中的密碼： • 更新 OCI 通訊使用者密碼 • 更新 MySQL 使用者密碼、包括 root • 對於每個 Keystore 、如果 Keystore 密碼為「已知」、請使用還原資料保險箱中的密碼來更新 Keystore 。 以正常模式執行時、也會從執行個體讀取每個加密值、使用目前資料保險箱的加密服務將其解密、使用還原的資料保險箱加密服務重新加密、以及儲存重新加密的值。
與資料保險箱同步	執行所有協調的動作來更新安裝，以符合還原資料保險箱中的使用者密碼： • 更新 OCI 通訊使用者密碼 • 更新 MySQL 使用者密碼、包括 root
變更密碼	變更資料保險箱中的密碼並執行協調的動作。
置換鍵	建立新的空資料保險箱（其金鑰與現有的資料保險箱不同）。然後將項目從目前的資料保險箱複製到新的資料保險箱。然後從執行個體讀取每個加密值、使用目前資料保險箱的加密服務將其解密、使用還原的資料保險箱加密服務重新加密、並儲存重新加密的值。

協調行動

伺服器資料保險箱

內部_	更新資料庫中使用者的密碼雜湊
併購	更新資料庫中使用者的密碼雜湊 如果有擷取資料保險箱、請同時更新擷取資料保險箱中的項目
dwh_internal	更新資料庫中使用者的密碼雜湊
Cogns_admin	更新資料庫中使用者的密碼雜湊 如果是 DWH 和 Windows 、請更新 SANscreen / Cognos / 分析 / 組態 / SANscreenAP.properties 、將 Cognos ． admin 屬性設定為密碼。
根	執行 SQL 以更新 MySQL 執行個體中的使用者密碼

庫存	執行 SQL 以更新 MySQL 執行個體中的使用者密碼
dwh	執行 SQL 以更新 MySQL 執行個體中的使用者密碼 如果是 DWH 和 Windows 、請更新 Windows 登錄、將下列與 ODBC 相關的項目設定為新密碼： • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_capies\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_capal_Efficiation\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_FS_util\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_inventory\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_Performance \PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_ports \PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_sa\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_Cloud 成本 \PWD
dwhuser	執行 SQL 以更新 MySQL 執行個體中的使用者密碼
主機	執行 SQL 以更新 MySQL 執行個體中的使用者密碼
Keystore 密碼	使用新密碼重新寫入金鑰儲存區： wildfly/standbed/configuration/server.keystore
truststore_password	使用新密碼重新寫入金鑰儲存區： wildfly/standbed/configuration/server.trustore
key_password	使用新密碼重新寫入金鑰儲存區： wildfly/standbed/configuration/sso.jks
Cognos 歸檔	無

擷取 **Vault**

併購	無
truststore_password	使用新密碼（如果存在）重新寫入密鑰庫 - acq/conf/cert / client.keystore

執行安全管理工具 **-** 命令列

在命令列模式中執行 SA 工具的語法如下：

```
securityadmin [-s | -au] [-db] [-lu <user> [-lp <password>]] <additional-
options>

where

-s                      selects server vault
-au                     selects acquisition vault

-db                     selects direct operation mode

-lu <user>              user for authentication
-lp <password>          password for authentication
<addition-options>      specifies command and command arguments as
described below
```

附註：

- 命令列上可能沒有「 -I 」選項（因為這會選取互動模式）。
- 對於 "-s" 和 "-au" 選項：
  - Rau 不允許使用 "-s"
  - DWH 不允許使用 "-au"
  - 如果兩者都不存在、則
    - 伺服器資料保險箱是在伺服器、 DWH 和雙工上選取
    - 擷取資料保險箱是在 Rau 上選取
- Lu 和 -lp 選項用於使用者驗證。
  - 如果已指定 <user> 且未指定 <password> 、則系統會提示使用者輸入密碼。
  - 如果未提供 <user> 且需要驗證、則系統會提示使用者輸入 <user> 和 <password> 。

命令：

命令	使用量

正確儲存的密碼	`securityadmin [-s`
-au] [-db] -pt <key> [<value>] `where` -pt specifies the command ("put") <key> is the key <value> is the value. If not present, user will be prompted for value	備份資料保險箱
`securityadmin [-s`	-au] [-db] -b [<backup-dir>] where -b specified command <backup-dir> is the output directory. If not present, default location of SANscreen/backup/vault is used The backup file will be named ServerSecurityBackup-yyyy-MM-dd-HH-mm.zip
備份資料保險箱	`securityadmin [-s`
-au] [-db] -ub <backup-file> where -ub specified command ("upgrade-backup") <backup-file> The location to write the backup file	清單鍵

`securityadmin [-s`	-au] [-db] -l where -l specified command
檢查鍵	`securityadmin [-s`
-au] [-db] -ck where -ck specified command exit code: 1 error 2 default key(s) 3 unique keys	VERIF-keystore （伺服器）

`securityadmin [-s] [-db] -v`
 	
`where`
 	
`-v specified command`
	升級

`securityadmin [-s`	-au] [-db] [-lu <user>] [-lp <password>] -u where -u specified command For server vault, if -lu is not present, then authentication will be performed for <user> =_internal and <password> = _internal’s password from vault. For acquisition vault, if -lu is not present, then no authentication will be attempted

置換鍵	`securityadmin [-s`
-au] [-db] [-lu <user>] [-lp <password>] -rk where -rk specified command	還原資料保險箱備份
`securityadmin [-s`	-au] [-db] [-lu <user>] [-lp <password>] -r <backup-file> where -r specified command <backup-file> the backup file location

變更密碼（伺服器）	`securityadmin [-s] [-db] [-lu <user>] [-lp <password>] -up -un <user> -p [<password>] [-sh]`
	
	`where`
	
	`-up specified command ("update-password")`
	`-un <user> entry ("user") name to update`
	`-p <password> new password. If <password not supplied, user will be prompted.`
	`-sh for mySQL user, use strong hash`

擷取使用者的變更密碼（擷取）	`securityadmin [-au] [-db] [-lu <user>] [-lp <password>] -up -p [<password>]`
	
	`where`
	
	`-up specified command ("update-password")`
	`-p <password> new password. If <password not supplied, user will be prompted.`

truststore—_password 的 change-password （取得）	`securityadmin [-au] [-db] [-lu <user>] [-lp <password>] -utp -p [<password>]`
	
	`where`
	
	`-utp specified command ("update-truststore-password")`
	`-p <password> new password. If <password not supplied, user will be prompted.`

與資料保險箱同步（伺服器）	`securityadmin [-s] [-db] [-lu <user>] [-lp <password>] -sv <backup-file>`
	
	`where`
	
	`-sv specified command`

執行安全管理工具 - 互動模式

互動式 - 主功能表

若要以互動模式執行 SA 工具、請輸入下列命令：

```
 securityadmin -i
```

在伺服器或雙安裝上、 `securityadmin` 會提示使用者選擇伺服器或本機擷取單元。

偵測到伺服器和擷取單元節點！選取需要重新設定安全性的節點：

```
1 - Server

2 - Local Acquisition Unit

9 - Exit

Enter your choice:
```

在 DWH 上、會自動選取「伺服器」。在遠端 AU 上、系統會自動選取「擷取單元」。

互動式 - 伺服器：根密碼還原

在伺服器模式中、 securityadmin Tool 會先檢查儲存的根密碼是否正確。如果沒有、工具會顯示 root 密碼恢復

畫面。

```
ERROR: Database is not accessible

1 - Enter root password

2 - Get root password from vault backup

9 - Exit

Enter your choice:
```

如果選擇選項 1 、系統會提示使用者輸入正確的密碼。

```
 Enter password (blank = don't change)
 Enter correct password for 'root':
```

如果輸入正確的密碼、將會顯示下列內容。

```
 Password verified.  Vault updated
```

按下 `ENTER` 會顯示伺服器不受限制的功能表。

如果輸入的密碼錯誤、將會顯示下列內容

```
 Password verification failed - Access denied for user 'root'@'localhost'
(using password: YES)
```

按下 `ENTER` 會返回恢復功能表。

如果選取選項 2 、系統會提示使用者提供備份檔案的名稱、以便從中讀取正確的密碼：

```
 Enter Backup File Location:
```

如果備份的密碼正確、則會顯示下列內容。

```
 Password verified.  Vault updated
```

按下 `ENTER` 會顯示伺服器不受限制的功能表。

如果備份中的密碼不正確、則會顯示下列內容

```
 Password verification failed - Access denied for user 'root'@'localhost'
(using password: YES)
```
按下 `ENTER` 會返回恢復功能表。

互動式 - 伺服器：正確密碼

「正確密碼」動作用於變更儲存在資料保險箱中的密碼、使其符合安裝所需的實際密碼。此命令在安全性管理工具以外的地方變更安裝時非常有用。範例包括：

- SQL 使用者的密碼是透過直接存取 MySQL 來修改的。
- 使用 keytool 替換密鑰庫或更改密鑰庫的密碼。
- OCI 資料庫已還原、且該資料庫有不同的內部使用者密碼

「正確密碼」會先提示使用者選擇要儲存正確值的密碼。

```
Replace incorrect stored password with correct password.  (Does not change
the required password)
Select User:  (Enter 'b' to go Back)

1 - _internal

2 - acquisition

3 - cognos_admin

4 - cognos keystore

5 - dwh

6 - dwh_internal

7 - dwhuser

8 - hosts

9 - inventory

10 - sso keystore

11 - server keystore

12 - root

13 - server truststore

14 - AU truststore

Enter your choice:
```

選取要修正的項目之後、系統會提示使用者提供值的方式。

```
1 - Enter {user} password

2 - Get {user} password from vault backup

9 - Exit

Enter your choice:
```

如果選擇選項 1 、系統會提示使用者輸入正確的密碼。

```
 Enter password (blank = don't change)
 Enter correct password for '{user}':
```
如果輸入正確的密碼、將會顯示下列內容。

```
 Password verified.  Vault updated
```
按下 `ENTER` 會返回伺服器不受限制的功能表。

如果輸入的密碼錯誤、將會顯示下列內容

```
Password verification failed - {additional information}
Vault entry not updated.
```

按下 ENTER 會返回伺服器不受限制的功能表。

如果選取選項 2 、系統會提示使用者提供備份檔案的名稱、以便從中讀取正確的密碼：

```
 Enter Backup File Location:
```
如果備份的密碼正確、則會顯示下列內容。

```
 Password verified.  Vault updated
```
按下 `ENTER` 會顯示伺服器不受限制的功能表。

如果備份中的密碼不正確、則會顯示下列內容

```
Password verification failed - {additional information}
Vault entry not updated.
```

按下 ENTER 會顯示伺服器不受限制的功能表。

互動式 - 伺服器：驗證 Vault 內容

確認 Vault 內容會檢查資料保險箱是否有與以舊版 OCI 發佈的預設資料保險箱相符的金鑰、並檢查資料保險箱中的每個值是否與安裝相符。

每個關鍵字的可能結果如下：

好的	資料保險箱值正確
未核取	無法對照安裝檢查此值
不良	此值與安裝不符

遺失	缺少預期的項目。

```
Encryption keys secure: unique, non-default encryption keys detected

             cognos_admin: OK
                    hosts: OK
             dwh_internal: OK
                inventory: OK
                  dwhuser: OK
        keystore_password: OK
                      dwh: OK
      truststore_password: OK
                     root: OK
                _internal: OK
          cognos_internal: Not Checked
             key_password: OK
              acquisition: OK
           cognos_archive: Not Checked
 cognos_keystore_password: Missing


Press enter to continue
```

互動式 - 伺服器：備份

備份將提示輸入儲存備份 zip 檔案的目錄。目錄必須已存在、且檔案名稱為 ServerSecurityBackup-yyyy-mm-dd-hh-mm.zip 。

```
Enter backup directory location [C:\Program Files\SANscreen\backup\vault]
:

Backup Succeeded!   Backup File: C:\Program
Files\SANscreen\backup\vault\ServerSecurityBackup-2024-08-09-12-02.zip
```

互動式 - 伺服器：登入

登入動作用於驗證使用者、並存取修改安裝的作業。使用者必須擁有管理 Privileges 。與伺服器一起執行時、可以使用任何管理員使用者；在直接模式下執行時、使用者必須是本機使用者、而非 LDAP 使用者。

```
Authenticating via server. Enter user and password

UserName: admin

Password:
```

或

```
Authenticating via database.  Enter local user and password.

UserName: admin

Password:
```

如果密碼正確且使用者是管理員使用者、則會顯示受限功能表。

如果密碼不正確、則會顯示下列內容：

```
Authenticating via database.  Enter local user and password.

UserName: admin

Password:

Login Failed!
```

如果使用者不是管理員、則會顯示下列內容：

```
Authenticating via server. Enter user and password

UserName: user

Password:

User 'user' does not have 'admin' role!
```

互動式 - 伺服器：受限功能表

使用者登入後、工具會顯示「受限制的功能表」。

```
Logged in as: admin
Select Action:

2 - Change Password

3 - Verify Vault Contents

4 - Backup

5 - Restore

6 - Change Encryption Keys

7 - Fix installation to match vault

9 - Exit

Enter your choice:
```

互動式 - 伺服器：變更密碼

「變更密碼」動作用於將安裝密碼變更為新值。

「變更密碼」會先提示使用者選擇要變更的密碼。

```
Change Password
Select User:  (Enter 'b' to go Back)

1 - _internal

2 - acquisition

3 - cognos_admin

4 - cognos keystore

5 - dwh

6 - dwh_internal

7 - dwhuser

8 - hosts

9 - inventory

10 - sso keystore

11 - server keystore

12 - root

13 - server truststore

14 - AU truststore

Enter your choice:
```

選取要修正的項目之後、如果使用者是 MySQL 使用者、系統會詢問使用者是否要加強密碼雜湊

```
MySQL supports SHA-1 and SHA-256 password hashes. SHA-256 is stronger but
requires all clients use SSL connections

Use strong password hash? (Y/n): y
```

接著、系統會提示使用者輸入新密碼。

```
New Password for '{user}':
If the password is empty, the operation is cancelled.

Password is empty - cancelling operation
```

如果輸入非空密碼、系統會提示使用者確認密碼。

```
New Password for '{user}':

Confirm New Password for '{user}':

Password successfully updated for 'dwhuser'!
```

如果變更不成功、則會顯示錯誤或例外。

互動式 - 伺服器：還原

互動式 - 伺服器：變更加密金鑰

「變更加密金鑰」動作將取代用於加密資料保險箱項目的加密金鑰、並取代用於資料保險箱加密服務的加密金鑰。由於加密服務的金鑰已變更、因此資料庫中的加密值將會重新加密；這些值將會讀取、以目前金鑰解密、以新金鑰加密、並儲存回資料庫。

直接模式不支援此動作、因為伺服器會為某些資料庫內容提供重新加密作業。

```
Replace encryption key with new key and update encrypted database values

Confirm (y/N): y

Change Encryption Keys succeeded! Restart 'Server' Service!
```

互動式 - 伺服器：修復安裝

「修復安裝」動作將會更新安裝。所有可透過安全管理工具變更的安裝密碼（ root 除外）都會設為資料保險箱中的密碼。

- 保監處內部使用者的密碼將會更新。
- MySQL 使用者的密碼（ root 除外）將會更新。
- Keystone 的密碼將會更新。

```
Fix installation - update installation passwords to match values in vault

Confirm:  (y/N): y

Installation update succeeded! Restart 'Server' Service.
```

此動作將在第一次不成功的更新時停止、並顯示錯誤或例外。

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`

如需詳細資訊、請參閱"安全性管理"文件。

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`

如需詳細資訊、請參閱"安全性管理工具"指示。

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/Rau 安全性組態的其中一個案例、是在伺服器上變更該使用者的密碼時、更新「取得」使用者密碼。Lau 和所有的 Raus 都使用與伺服器「取得」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。

如需詳細資訊、請參閱"安全性管理工具"指示。

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`

如需詳細資訊、請參閱"安全性管理"文件。

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。

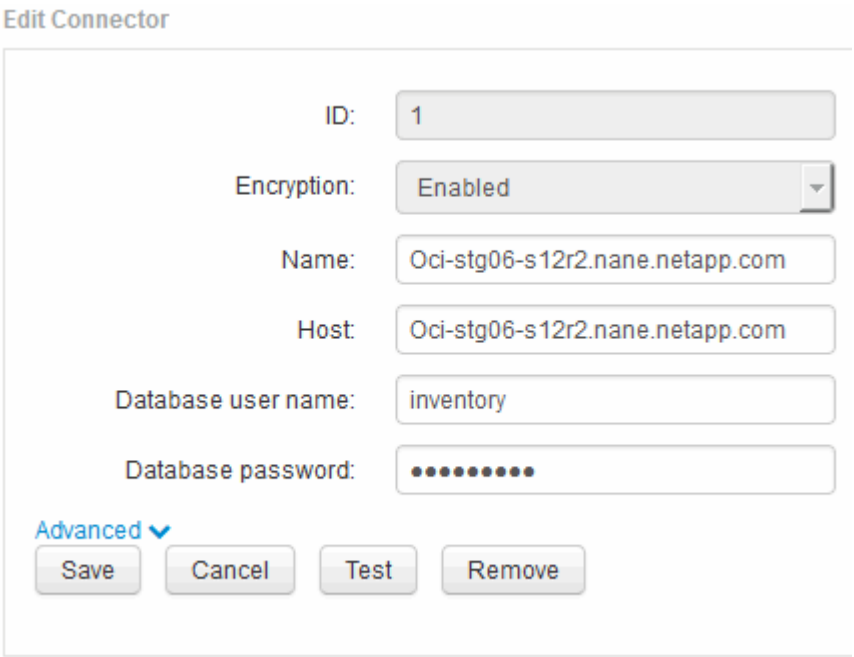
開始之前

您必須以系統管理員身分登入才能執行此工作。

步驟

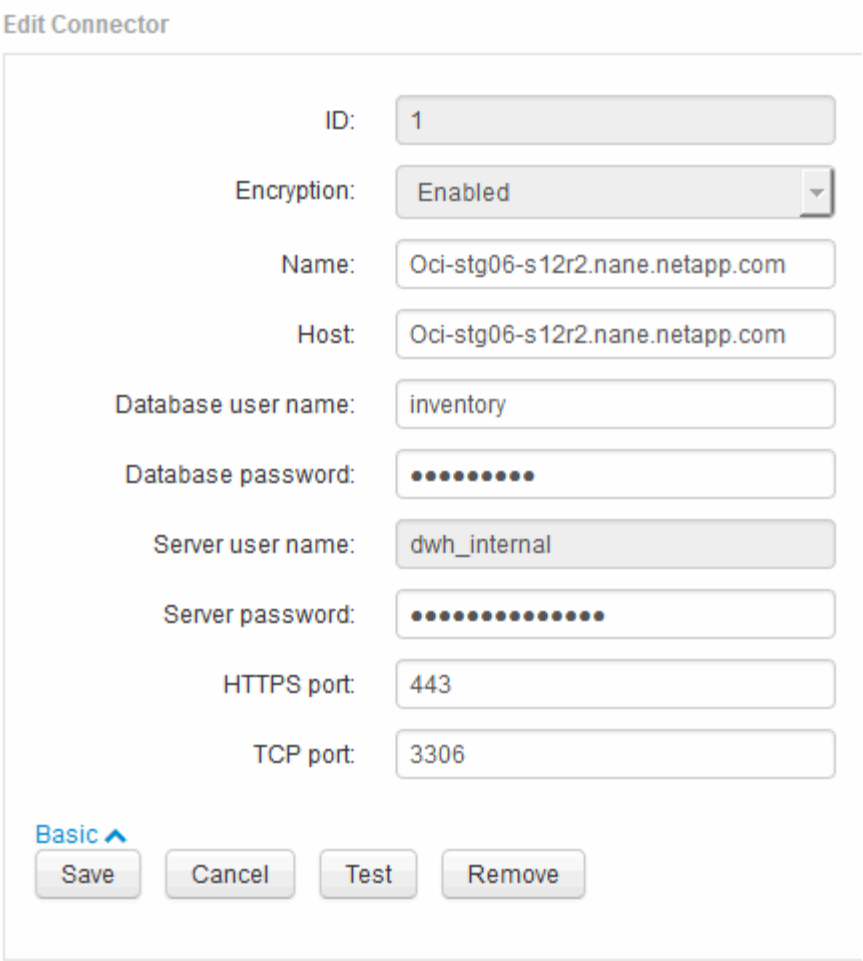
1. 登入資料倉儲入口網站： https://hostname/dwh、其中、主機名稱是OnCommand Insight 安裝了「IsorData倉儲」的系統名稱。
2. 在左側的導覽窗格中、按一下* Connectors *。

   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。

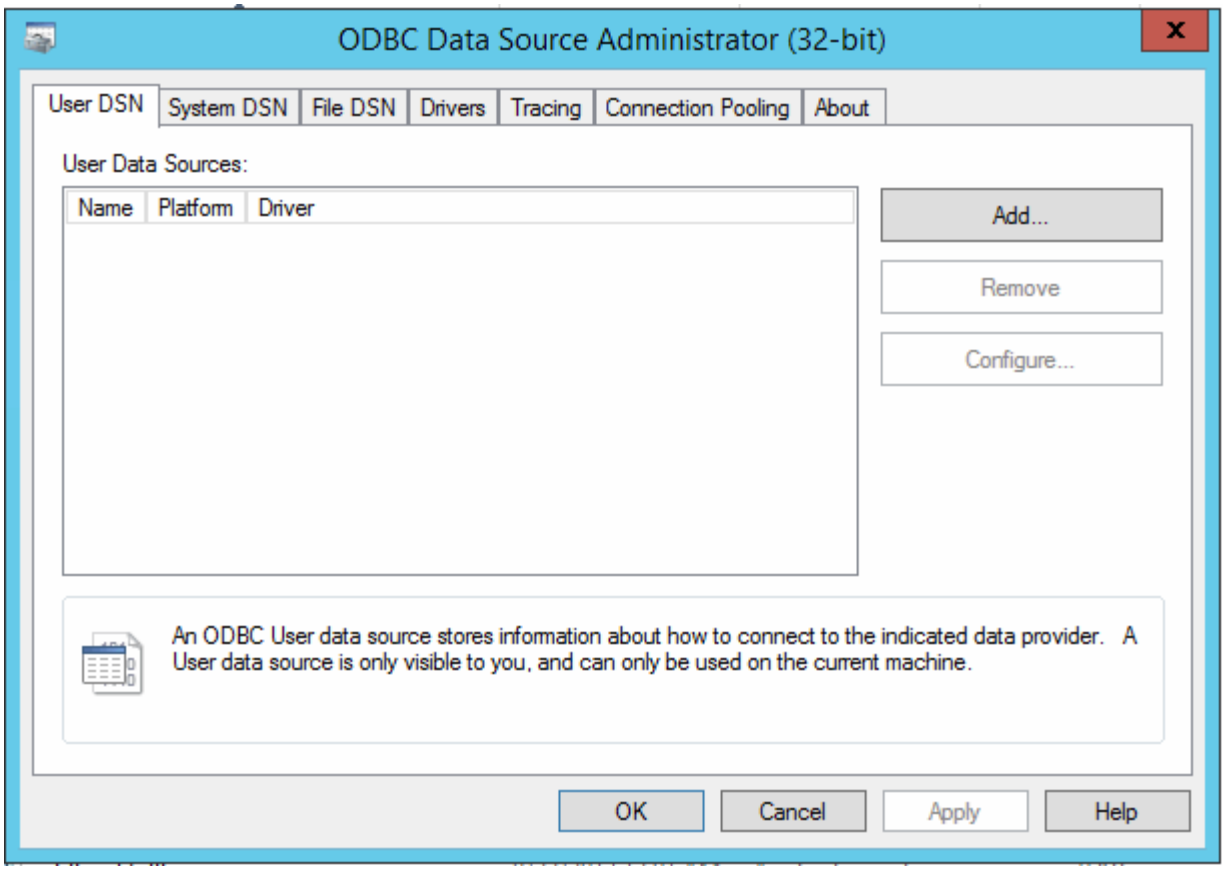
開始之前

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

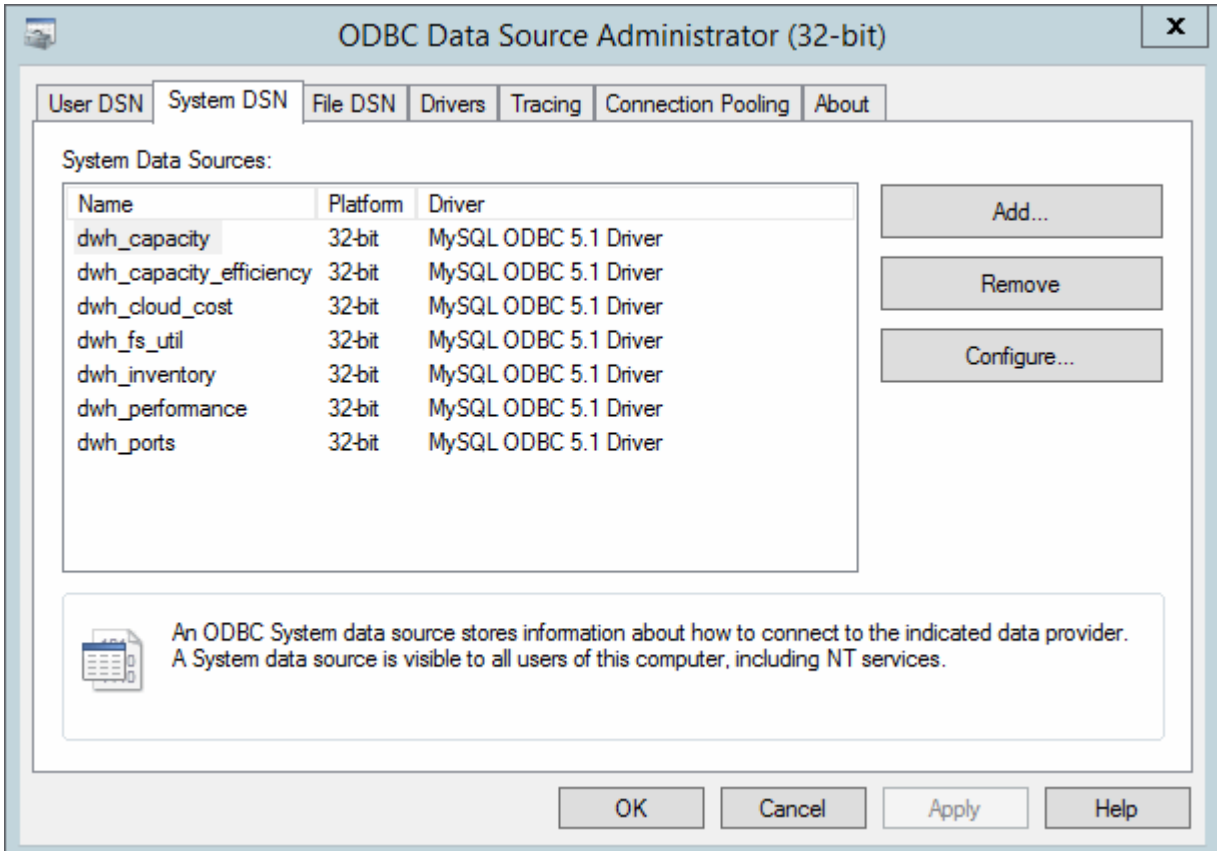
1. 遠端登入裝載該資料倉儲的伺服器。
2. 存取位於的「ODBC行政」工具 `C:\Windows\SysWOW64\odbcad32.exe`

   系統會顯示「ODBC資料來源管理員」畫面。



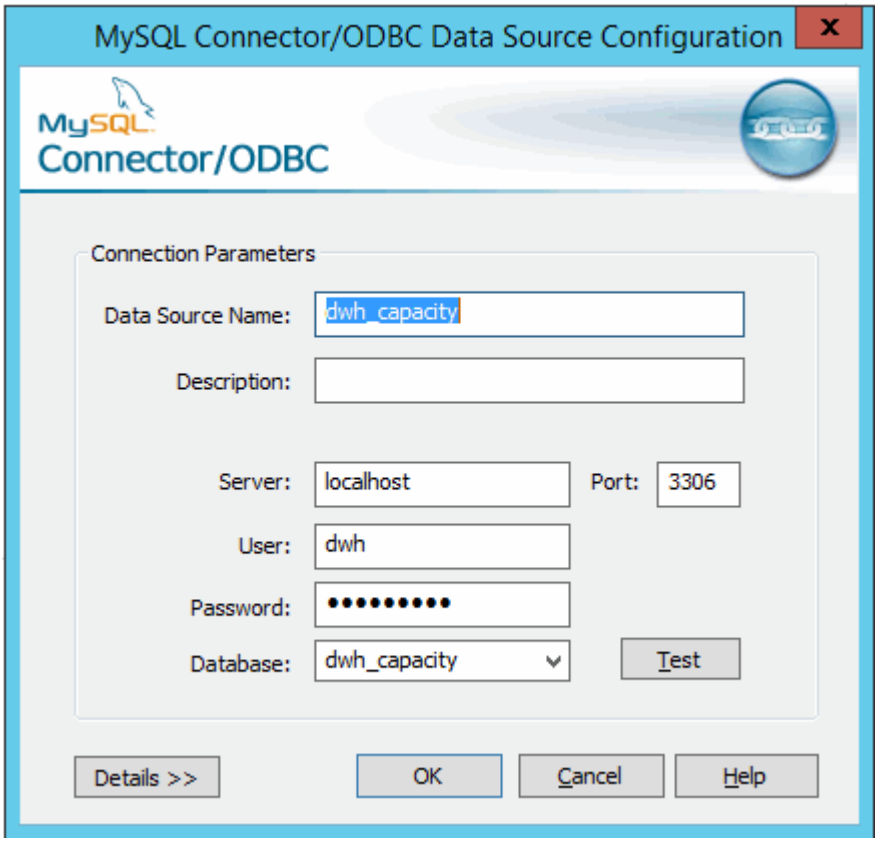
3. 單擊*系統DSN*

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。

如果使用更改了 *server.keystore* 和 / 或 *_server.trustore* 密碼"安全性管理"，請 *SANscreen* 在導入 *LDAP* 證書之前重新啓動 *_LDAP* 服務。

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。

根 CA 必須匯入信任存放區。

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「根憑證」 `/opt/netapp/oci/wildfly/standalone/configuration/server.truststore`
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。

> 如果使用更改了 *server.keystore* 和 / 或 *_server.trustore* 密碼"安全性管理"，請 *SANscreen* 在導入 *LDAP* 證書之前重新啓動 *_LDAP* 服務。

> 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`公用程式列出信任的 `CA` ： `C:\Program Files\SANscreen\java64\bin\keytool.exe -list -keystore server.trustore -storepass <password>` + 如需設定或變更 server_trustore 密碼的詳細資訊、請參閱"安全性管理"文件。

   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** 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`公用程式列出信任的 CA ： `..\IBM-JRE\JRE\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass <password>`

      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`通常是一個別名、可在作業中輕鬆識別 CA `keytool -list`。

f. 當系統提示您輸入密碼時、請輸入來自 __/m/bin/Cognos SANscreen info.dat 檔案的密碼。

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 7.3.10**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 <password> -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。
   c. 若為 <password> 、請使用來自 __/dat/bin/cognos SANscreen 資訊 .dat 檔案的密碼。
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\Cognos 。 crt -keystore Cognos \ anature\configuration\certs\CAMKeystore -storetype PKCS12 -storepass <password> -alias 加密
    c. 若為 <password> 、請使用來自 __/dat/bin/cognos SANscreen 資訊 .dat 檔案的密碼。
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:\temp\Cognos.crt -keystore wildfly\inold\configuration\server.trustore -storepass <password> -alias cognos3rdca
    c. 若為 <password> 、請使用來自 __/dat/bin/cognos SANscreen 資訊 .dat 檔案的密碼。
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 <password> -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

> 強烈建議您在升級之前備份資料保險箱。
>
> 如需有關資料保險箱和密碼管理的詳細資訊、請參閱"安全性管理工具"指示。

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"`

   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。

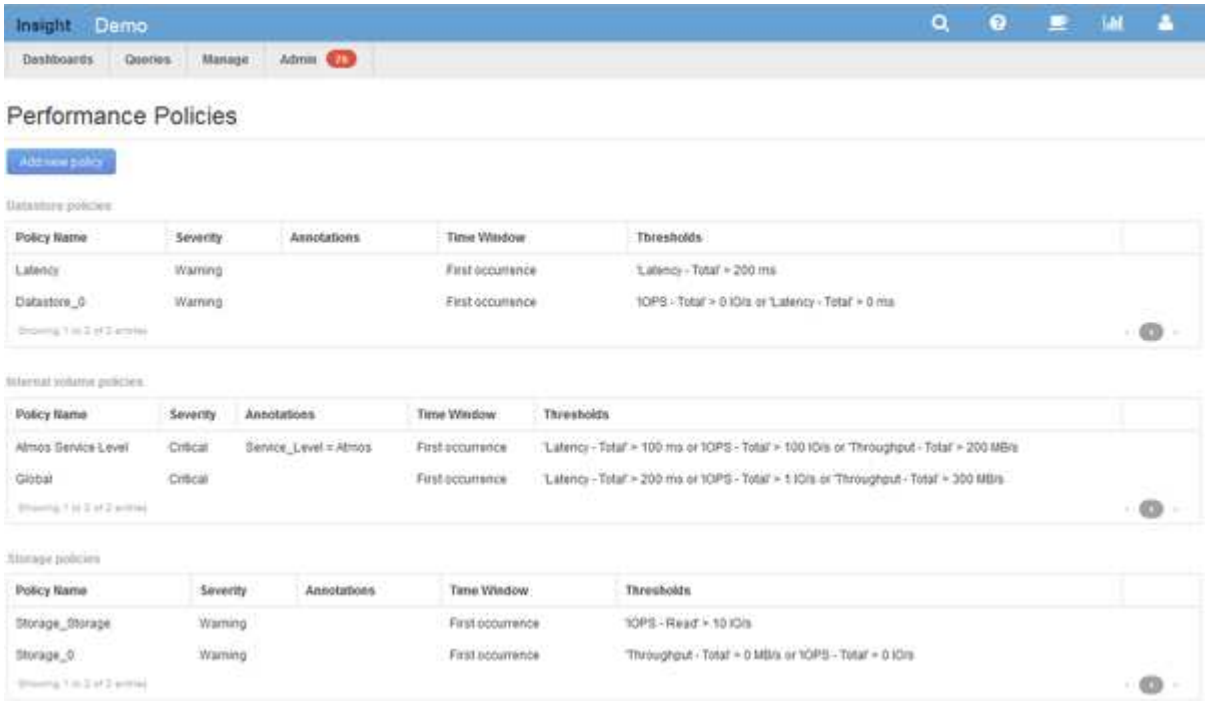
建立效能原則

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。
>
> +

Insight Security

OnCommand Insight 提供的功能可讓 Insight 環境以增強的安全性運作。這些功能包括加密、密碼雜湊、以及變更內部使用者密碼和密碼加密和解密金鑰配對的能力。您可以使用 securityadmin Tool 在 Insight 環境中的所有伺服器上管理這些功能。

什麼是安全性管理工具？

安全性管理工具支援變更資料保險箱的內容、以及協調一致地變更 OnCommand Insight 安裝。

安全性管理工具的主要用途是 * 備份 * 和 * 還原 * 安全性組態（即資料保險箱）和密碼。例如、您可以在本機擷取單元上備份資料保險箱、並在遠端擷取單元上還原資料保險箱、確保整個環境都能協調密碼。或者、如果您的環境中有多部 OnCommand Insight 伺服器、您可能需要備份伺服器資料保險箱、並將其還原至其他伺服器、以保持密碼相同。以下只是安全性管理可用於確保環境內凝聚力的兩個範例。

> 強烈建議您在備份 OnCommand Insight 資料庫時 * 備份資料保險箱 * 。否則可能導致存取中斷。

此工具同時提供 * 互動 * 和 * 命令列 * 模式。

許多 securityadmin Tool 作業會變更資料保險箱的內容、也會變更安裝、確保資料保險箱和安裝保持同步。

例如、

- 當您變更 Insight 使用者密碼時、 SANscreen 。 Users 表格中的使用者項目將會以新的雜湊更新。
- 當您變更 MySQL 使用者密碼時、將會執行適當的 SQL 陳述式、以更新 MySQL 執行個體中的使用者密碼。

在某些情況下、會對安裝進行多項變更：

- 修改 dwh MySQL 使用者時、除了更新 MySQL 資料庫中的密碼之外、也會更新多個 ODBC 登錄項目。

在下列各節中、使用「協調式變更」一詞來描述這些變更。

執行模式

- 正常 / 預設操作 - SANscreen 伺服器服務必須執行

  對於默認執行模式， securityadmin Tool 要求 SANscreen 服務器服務 * 正在運行。伺服器用於驗證、許多協調一致的安裝變更都是透過呼叫伺服器來進行。

- 直接操作 - SANscreen 伺服器服務可能正在執行或停止。

  在 OCI 伺服器或 DWH 安裝上執行時、工具也可以在「直接」模式下執行。在此模式中、驗證和協調變更是使用資料庫來執行。未使用伺服器服務。

  操作與一般模式相同、但有下列例外：

- 驗證僅支援非網域管理員使用者。（密碼和角色位於資料庫中的使用者、而非 LDAP ）。
- 不支援「置換金鑰」操作。
- 會略過資料保險箱還原的重新加密步驟。
- 恢復模式即使無法同時存取伺服器和資料庫、也可能執行此工具（例如、因為資料保險箱中的根密碼不正確）。

  在此模式下執行時、無法進行驗證、因此無法執行協調變更安裝的作業。

  恢復模式可用於：

- 判斷哪些資料保險箱項目錯誤（使用驗證作業）
- 請以正確的值取代不正確的根密碼。（這不會變更密碼。使用者必須輸入目前的密碼。）

> 如果資料保險箱中的根密碼不正確、而且密碼未知、而且沒有正確的根密碼備份資料保險箱、則無法使用 securityadmin Tool 還原安裝。恢復安裝的唯一方法是按照中介紹的步驟重置 MySQL 實例的密碼 https://dev.mysql.com/doc/refman/8.4/en/resetting-permissions.html。執行重設程序後、請使用正確的儲存密碼操作、將新密碼輸入資料保險箱。

命令

無限制命令

無限制命令會對安裝進行任何協調的變更（信任存放區除外）。不受限制的命令可在不進行使用者驗證的情況下執行。

命令	說明
備份資料保險箱	建立包含資料保險箱的 zip 檔案。至資料保險箱檔案的相對路徑將與相對於安裝根目錄的資料保險箱路徑相符。 • Wildfly / 獨立 / 組態 / 資料保險箱 / * • ACQ/conf/vVault/*
檢查預設金鑰	檢查資料保險箱的金鑰是否與 7.3.16 之前版本中使用的預設資料保險箱金鑰相符。
正確儲存的密碼	以使用者已知的正確密碼取代儲存在資料保險箱中的（不正確）密碼。 當資料保險箱和安裝不一致時、可能會使用此選項。* 請注意、它不會變更安裝中的實際密碼。 *
change-trust 儲存區密碼	變更用於信任存放區的密碼、並將新密碼儲存在資料保險箱中。信任存放區的目前密碼必須為「已知」。
驗證 Keystore	檢查資料保險箱中的值是否正確： • 對於 OCI 使用者、密碼雜湊是否與資料庫中的值相符 • 對於 MySQL 使用者、可以建立資料庫連線 • 對於 Keystore 、是否可以載入 Keystore 及其金鑰（如果有）讀取
清單鍵	列出資料保險箱中的項目（不顯示儲存的值）

受限命令

任何對安裝進行協調變更的非隱藏命令都需要驗證：

命令	說明
還原資料保險箱備份	以包含在指定資料保險箱備份檔案中的資料保險箱取代目前的資料保險箱。 執行所有協調的動作來更新安裝以符合還原資料保險箱中的密碼： • 更新 OCI 通訊使用者密碼 • 更新 MySQL 使用者密碼、包括 root • 對於每個 Keystore 、如果 Keystore 密碼為「已知」、請使用還原資料保險箱中的密碼來更新 Keystore 。 以正常模式執行時、也會從執行個體讀取每個加密值、使用目前資料保險箱的加密服務將其解密、使用還原的資料保險箱加密服務重新加密、以及儲存重新加密的值。

與資料保險箱同步	執行所有協調的動作來更新安裝，以符合還原資料保險箱中的使用者密碼： • 更新 OCI 通訊使用者密碼 • 更新 MySQL 使用者密碼、包括 root
變更密碼	變更資料保險箱中的密碼並執行協調的動作。
置換鍵	建立新的空資料保險箱（其金鑰與現有的資料保險箱不同）。然後將項目從目前的資料保險箱複製到新的資料保險箱。然後從執行個體讀取每個加密值、使用目前資料保險箱的加密服務將其解密、使用還原的資料保險箱加密服務重新加密、並儲存重新加密的值。

隱藏命令

SA 工具提供下列命令、這些命令不需要驗證、但必須對安裝進行協調的變更。

清單金鑰升級（伺服器）	如果使用者尚未驗證、請使用目前資料保險箱中的內部帳戶和密碼進行驗證。然後以備份檔案中的資料保險箱取代目前的資料保險箱，並執行協調的動作。
升級（併購）	以備份檔案中的資料保險箱取代目前的資料保險箱，並執行協調的動作。

協調行動

伺服器資料保險箱

內部_	更新資料庫中使用者的密碼雜湊
併購	更新資料庫中使用者的密碼雜湊 如果有擷取資料保險箱、請同時更新擷取資料保險箱中的項目
dwh_internal	更新資料庫中使用者的密碼雜湊
Cogns_admin	更新資料庫中使用者的密碼雜湊 如果是 DWH 和 Windows 、請更新 SANscreen / Cognos / 分析 / 組態 / SANscreenAP.properties 、將 Cognos ． admin 屬性設定為密碼。
根	執行 SQL 以更新 MySQL 執行個體中的使用者密碼
庫存	執行 SQL 以更新 MySQL 執行個體中的使用者密碼

dwh	執行 SQL 以更新 MySQL 執行個體中的使用者密碼 如果是 DWH 和 Windows 、請更新 Windows 登錄、將下列與 ODBC 相關的項目設定為新密碼： • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_capies\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_capal_Efficiation\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_FS_util\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_inventory\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_Performance \PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_ports \PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_sa\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_Cloud 成本 \PWD
dwhuser	執行 SQL 以更新 MySQL 執行個體中的使用者密碼
主機	執行 SQL 以更新 MySQL 執行個體中的使用者密碼
Keystore 密碼	使用新密碼重新寫入金鑰儲存區： wildfly/standbed/configuration/server.keystore
truststore_password	使用新密碼重新寫入金鑰儲存區： wildfly/standbed/configuration/server.trustore
key_password	使用新密碼重新寫入金鑰儲存區： wildfly/standbed/configuration/sso.jks
Cognos 歸檔	無

擷取 **Vault**

併購	無

truststore_password	使用新密碼（如果存在）重新寫入密鑰庫 - acq/conf/cert / client.keystore

執行安全管理工具 - 命令列

在命令列模式中執行 SA 工具的語法如下：

```
securityadmin [-s | -au] [-db] [-lu <user> [-lp <password>]] <additional-
options>

where

-s                      selects server vault
-au                     selects acquisition vault

-db                     selects direct operation mode

-lu <user>              user for authentication
-lp <password>          password for authentication
<addition-options>      specifies command and command arguments as
described below
```

附註：

- 命令列上可能沒有「 -I 」選項（因為這會選取互動模式）。
- 對於 "-s" 和 "-au" 選項：
  - Rau 不允許使用 "-s"
  - DWH 不允許使用 "-au"
  - 如果兩者都不存在、則
    - 伺服器資料保險箱是在伺服器、 DWH 和雙工上選取
    - 擷取資料保險箱是在 Rau 上選取
- Lu 和 -lp 選項用於使用者驗證。
  - 如果已指定 <user> 且未指定 <password> 、則系統會提示使用者輸入密碼。
  - 如果未提供 <user> 且需要驗證、則系統會提示使用者輸入 <user> 和 <password> 。

命令：

命令	使用量
正確儲存的密碼	`securityadmin [-s`

-au] [-db] -pt <key> [<value>]
 	
`where`
 	
-pt specifies the command ("put") <key> is the key <value> is the value. If not present, user will be prompted for value
 	
``
	備份資料保險箱

`securityadmin [-s`	-au] [-db] -b [<backup-dir>] where -b specified command <backup-dir> is the output directory. If not present, default location of SANscreen/backup/vault is used The backup file will be named ServerSecurityBackup-yyyy-MM-dd-HH-mm.zip ``
備份資料保險箱	`securityadmin [-s`
-au] [-db] -ub <backup-file> where -ub specified command ("upgrade-backup") <backup-file> The location to write the backup file ``	清單鍵
`securityadmin [-s`	-au] [-db] -l where -l specified command ``

檢查鍵	`securityadmin [-s`
-au] [-db] -ck where -ck specified command exit code: 1 error 2 default key(s) 3 unique keys	VERIF-keystore （伺服器）

`securityadmin [-s] [-db] -v`
 	
`where`
 	
`-v specified command`
	升級

`securityadmin [-s`	-au] [-db] [-lu <user>] [-lp <password>] -u where -u specified command For server vault, if -lu is not present, then authentication will be performed for <user> =_internal and <password> = _internal’s password from vault. For acquisition vault, if -lu is not present, then no authentication will be attempted
置換鍵	`securityadmin [-s`

-au] [-db] [-lu <user>] [-lp <password>] -rk where -rk specified command ``	還原資料保險箱備份
`securityadmin [-s`	-au] [-db] [-lu <user>] [-lp <password>] -r <backup-file> where -r specified command <backup-file> the backup file location ``

變更密碼（伺服器）	`securityadmin [-s] [-db] [-lu <user>] [-lp <password>] -up -un <user> -p [<password>] [-sh]`
	
	`where`
	
	`-up specified command ("update-password")`
	`-un <user> entry ("user") name to update`
	`-p <password> new password. If <password not supplied, user will be prompted.`
	`-sh for mySQL user, use strong hash`

擷取使用者的變更密碼（擷取）	`securityadmin [-au] [-db] [-lu <user>] [-lp <password>] -up -p [<password>]`
	
	`where`
	
	`-up specified command ("update-password")`
	`-p <password> new password. If <password not supplied, user will be prompted.`

truststore—_password 的 change-password （取得）	`securityadmin [-au] [-db] [-lu <user>] [-lp <password>] -utp -p [<password>]`
	
	`where`
	
	`-utp specified command ("update-truststore-password")`
	`-p <password> new password. If <password not supplied, user will be prompted.`

與資料保險箱同步（伺服器）	`securityadmin [-s] [-db] [-lu <user>] [-lp <password>] -sv <backup-file>`
	
	`where`
	
	`-sv specified command`

執行安全管理工具 - 互動模式

互動式 - 主功能表

若要以互動模式執行 SA 工具、請輸入下列命令：

```
securityadmin -i
```

在伺服器或雙安裝上、 `securityadmin` 會提示使用者選擇伺服器或本機擷取單元。

偵測到伺服器和擷取單元節點！選取需要重新設定安全性的節點：

```
1 - Server

2 - Local Acquisition Unit

9 - Exit

Enter your choice:
```

在 DWH 上、會自動選取「伺服器」。在遠端 AU 上、系統會自動選取「擷取單元」。

互動式 - 伺服器：根密碼還原

在伺服器模式中、 securityadmin Tool 會先檢查儲存的根密碼是否正確。如果沒有、工具會顯示 root 密碼恢復畫面。

```
ERROR: Database is not accessible

1 - Enter root password

2 - Get root password from vault backup

9 - Exit

Enter your choice:
```

如果選擇選項 1 、系統會提示使用者輸入正確的密碼。

```
 Enter password (blank = don't change)
 Enter correct password for 'root':
```

如果輸入正確的密碼、將會顯示下列內容。

```
 Password verified.  Vault updated
```

按下 `ENTER` 會顯示伺服器不受限制的功能表。

如果輸入的密碼錯誤、將會顯示下列內容

```
 Password verification failed - Access denied for user 'root'@'localhost'
(using password: YES)
```

按下 `ENTER` 會返回恢復功能表。

如果選取選項 2 、系統會提示使用者提供備份檔案的名稱、以便從中讀取正確的密碼：

```
 Enter Backup File Location:
```

如果備份的密碼正確、則會顯示下列內容。

```
 Password verified.  Vault updated
```

按下 `ENTER` 會顯示伺服器不受限制的功能表。

如果備份中的密碼不正確、則會顯示下列內容

```
 Password verification failed - Access denied for user 'root'@'localhost'
(using password: YES)
```
按下 `ENTER` 會返回恢復功能表。

互動式 - 伺服器：正確密碼

「正確密碼」動作用於變更儲存在資料保險箱中的密碼、使其符合安裝所需的實際密碼。此命令在安全性管理工具以外的地方變更安裝時非常有用。範例包括：

- SQL 使用者的密碼是透過直接存取 MySQL 來修改的。
- 使用 keytool 替換密鑰庫或更改密鑰庫的密碼。
- OCI 資料庫已還原、且該資料庫有不同的內部使用者密碼

「正確密碼」會先提示使用者選擇要儲存正確值的密碼。

```
Replace incorrect stored password with correct password.  (Does not change
the required password)
Select User:  (Enter 'b' to go Back)

1 - _internal

2 - acquisition

3 - cognos_admin

4 - cognos keystore

5 - dwh

6 - dwh_internal

7 - dwhuser

8 - hosts

9 - inventory

10 - sso keystore

11 - server keystore

12 - root

13 - server truststore

14 - AU truststore

Enter your choice:
```

選取要修正的項目之後、系統會提示使用者提供值的方式。

```
1 - Enter {user} password

2 - Get {user} password from vault backup

9 - Exit

Enter your choice:
```

如果選擇選項 1 、系統會提示使用者輸入正確的密碼。

```
 Enter password (blank = don't change)
 Enter correct password for '{user}':
```
如果輸入正確的密碼、將會顯示下列內容。

```
 Password verified.  Vault updated
```
按下 `ENTER` 會返回伺服器不受限制的功能表。

如果輸入的密碼錯誤、將會顯示下列內容

```
Password verification failed - {additional information}
Vault entry not updated.
```

按下 ENTER 會返回伺服器不受限制的功能表。

如果選取選項 2 、系統會提示使用者提供備份檔案的名稱、以便從中讀取正確的密碼：

```
 Enter Backup File Location:
```
如果備份的密碼正確、則會顯示下列內容。

```
 Password verified.  Vault updated
```
按下 `ENTER` 會顯示伺服器不受限制的功能表。

如果備份中的密碼不正確、則會顯示下列內容

```
Password verification failed - {additional information}
Vault entry not updated.
```

按下 ENTER 會顯示伺服器不受限制的功能表。

互動式 **-** 伺服器：驗證 **Vault** 內容

確認 Vault 內容會檢查資料保險箱是否有與以舊版 OCI 發佈的預設資料保險箱相符的金鑰、並檢查資料保險箱中的每個值是否與安裝相符。

每個關鍵字的可能結果如下：

好的	資料保險箱值正確
未核取	無法對照安裝檢查此值

不良	此值與安裝不符
遺失	缺少預期的項目。

```
Encryption keys secure: unique, non-default encryption keys detected

             cognos_admin: OK
                    hosts: OK
             dwh_internal: OK
                inventory: OK
                  dwhuser: OK
        keystore_password: OK
                      dwh: OK
      truststore_password: OK
                     root: OK
                _internal: OK
          cognos_internal: Not Checked
             key_password: OK
              acquisition: OK
           cognos_archive: Not Checked
 cognos_keystore_password: Missing


Press enter to continue
```

互動式 - 伺服器：備份

備份將提示輸入儲存備份 zip 檔案的目錄。目錄必須已存在、且檔案名稱為 ServerSecurityBackup-yyyy-mm-dd-hh-mm.zip 。

```
Enter backup directory location [C:\Program Files\SANscreen\backup\vault]
:

Backup Succeeded!   Backup File: C:\Program
Files\SANscreen\backup\vault\ServerSecurityBackup-2024-08-09-12-02.zip
```

互動式 - 伺服器：登入

登入動作用於驗證使用者、並存取修改安裝的作業。使用者必須擁有管理 Privileges 。與伺服器一起執行時、可以使用任何管理員使用者；在直接模式下執行時、使用者必須是本機使用者、而非 LDAP 使用者。

```
Authenticating via server. Enter user and password

UserName: admin

Password:
```

或

```
Authenticating via database.  Enter local user and password.

UserName: admin

Password:
```

如果密碼正確且使用者是管理員使用者、則會顯示受限功能表。

如果密碼不正確、則會顯示下列內容：

```
Authenticating via database.  Enter local user and password.

UserName: admin

Password:

Login Failed!
```

如果使用者不是管理員、則會顯示下列內容：

```
Authenticating via server. Enter user and password

UserName: user

Password:

User 'user' does not have 'admin' role!
```

互動式 - 伺服器：受限功能表

使用者登入後、工具會顯示「受限制的功能表」。

```
Logged in as: admin
Select Action:

2 - Change Password

3 - Verify Vault Contents

4 - Backup

5 - Restore

6 - Change Encryption Keys

7 - Fix installation to match vault

9 - Exit

Enter your choice:
```

互動式 - 伺服器：變更密碼

「變更密碼」動作用於將安裝密碼變更為新值。

「變更密碼」會先提示使用者選擇要變更的密碼。

```
Change Password
Select User:  (Enter 'b' to go Back)

1 - _internal

2 - acquisition

3 - cognos_admin

4 - cognos keystore

5 - dwh

6 - dwh_internal

7 - dwhuser

8 - hosts

9 - inventory

10 - sso keystore

11 - server keystore

12 - root

13 - server truststore

14 - AU truststore

Enter your choice:
```

選取要修正的項目之後、如果使用者是 MySQL 使用者、系統會詢問使用者是否要加強密碼雜湊

```
MySQL supports SHA-1 and SHA-256 password hashes. SHA-256 is stronger but
requires all clients use SSL connections

Use strong password hash? (Y/n): y
```

接著、系統會提示使用者輸入新密碼。

```
New Password for '{user}':
If the password is empty, the operation is cancelled.

Password is empty - cancelling operation
```

如果輸入非空密碼、系統會提示使用者確認密碼。

```
New Password for '{user}':

Confirm New Password for '{user}':

Password successfully updated for 'dwhuser'!
```

如果變更不成功、則會顯示錯誤或例外。

互動式 - 伺服器：還原

互動式 - 伺服器：變更加密金鑰

「變更加密金鑰」動作將取代用於加密資料保險箱項目的加密金鑰、並取代用於資料保險箱加密服務的加密金鑰。由於加密服務的金鑰已變更、因此資料庫中的加密值將會重新加密；這些值將會讀取、以目前金鑰解密、以新金鑰加密、並儲存回資料庫。

直接模式不支援此動作、因為伺服器會為某些資料庫內容提供重新加密作業。

```
Replace encryption key with new key and update encrypted database values

Confirm (y/N): y

Change Encryption Keys succeeded! Restart 'Server' Service!
```

互動式 - 伺服器：修復安裝

「修復安裝」動作將會更新安裝。所有可透過安全管理工具變更的安裝密碼（ root 除外）都會設為資料保險箱中的密碼。

- 保監處內部使用者的密碼將會更新。
- MySQL 使用者的密碼（ root 除外）將會更新。
- Keystone 的密碼將會更新。

```
Fix installation - update installation passwords to match values in vault

Confirm:  (y/N): y

Installation update succeeded! Restart 'Server' Service.
```

此動作將在第一次不成功的更新時停止、並顯示錯誤或例外。

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`

如需詳細資訊、請參閱"安全性管理"文件。

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`

如需詳細資訊、請參閱"安全性管理工具"指示。

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/Rau 安全性組態的其中一個案例、是在伺服器上變更該使用者的密碼時、更新「取得」使用者密碼。Lau 和所有的 Raus 都使用與伺服器「取得」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。

如需詳細資訊、請參閱"安全性管理工具"指示。

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`

如需詳細資訊、請參閱"安全性管理"文件。

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。

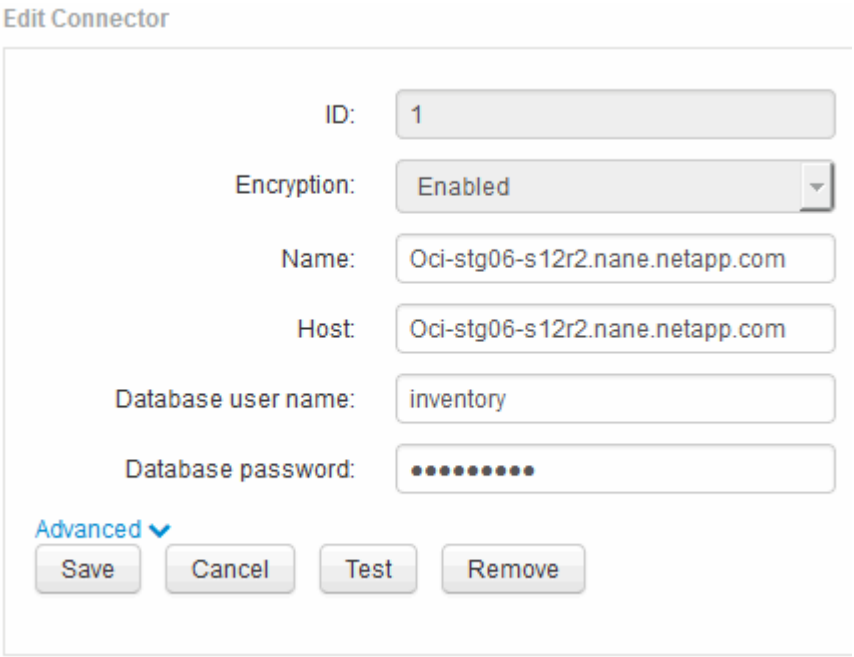
開始之前

您必須以系統管理員身分登入才能執行此工作。

步驟

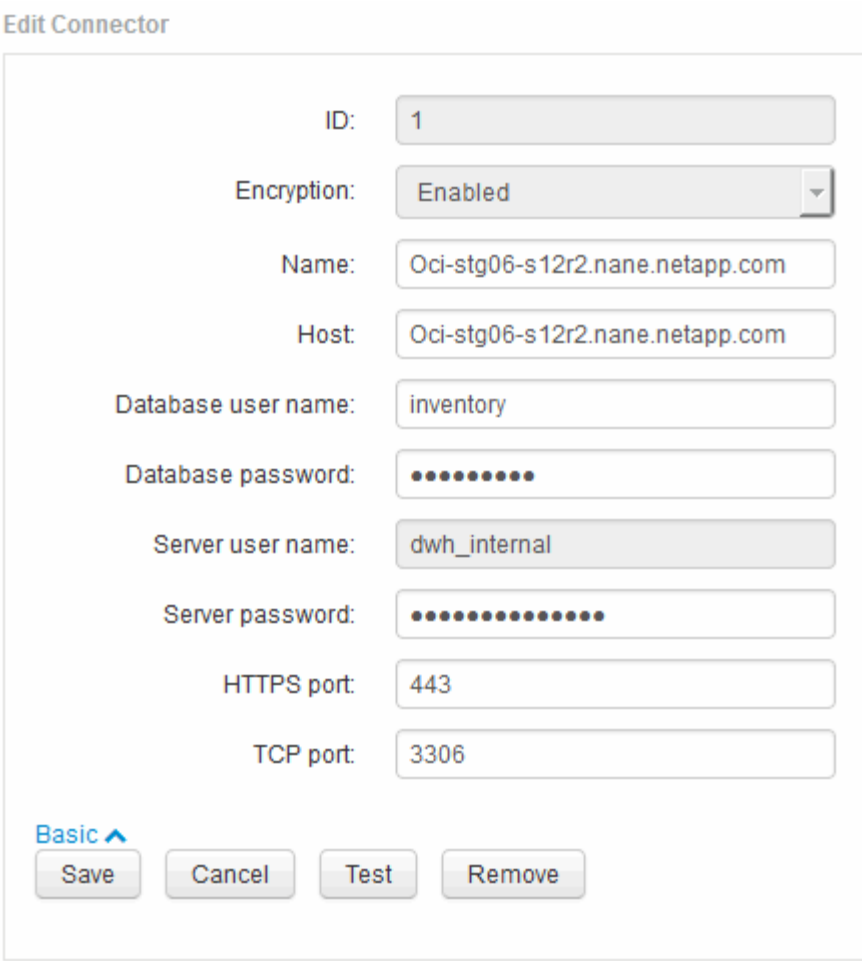
1. 登入資料倉儲入口網站： https://hostname/dwh、其中、主機名稱是OnCommand Insight 安裝了「IsorData倉儲」的系統名稱。
2. 在左側的導覽窗格中、按一下* Connectors *。

   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。

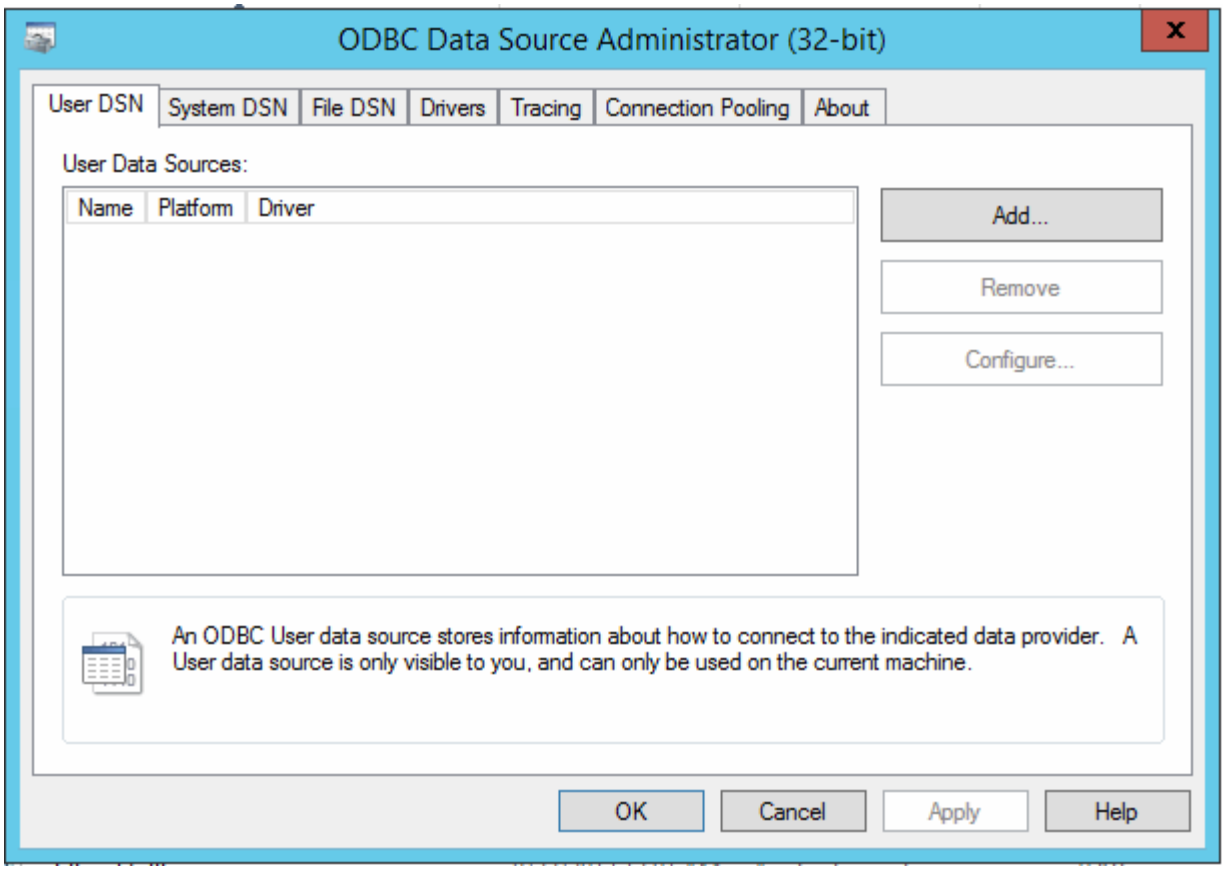
開始之前

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

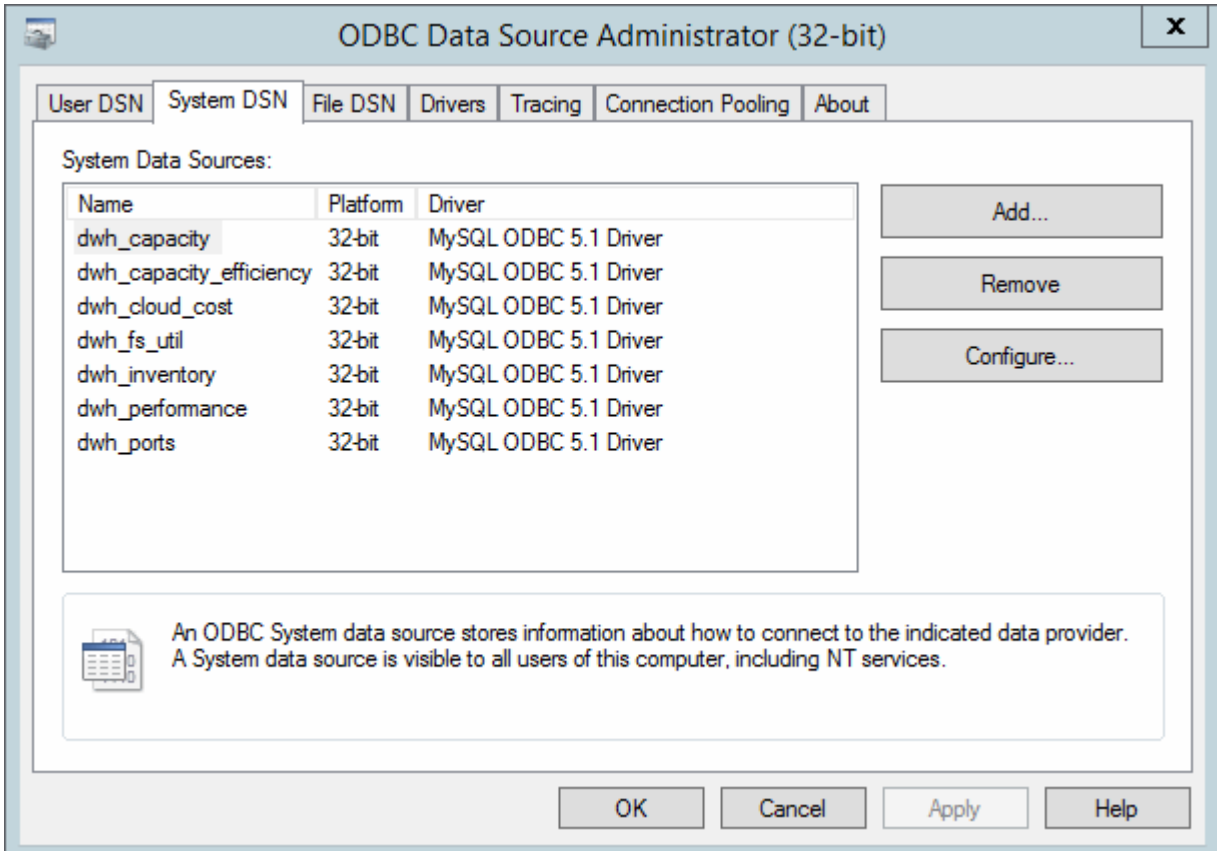
1. 遠端登入裝載該資料倉儲的伺服器。
2. 存取位於的「ODBC行政」工具 `C:\Windows\SysWOW64\odbcad32.exe`

   系統會顯示「ODBC資料來源管理員」畫面。



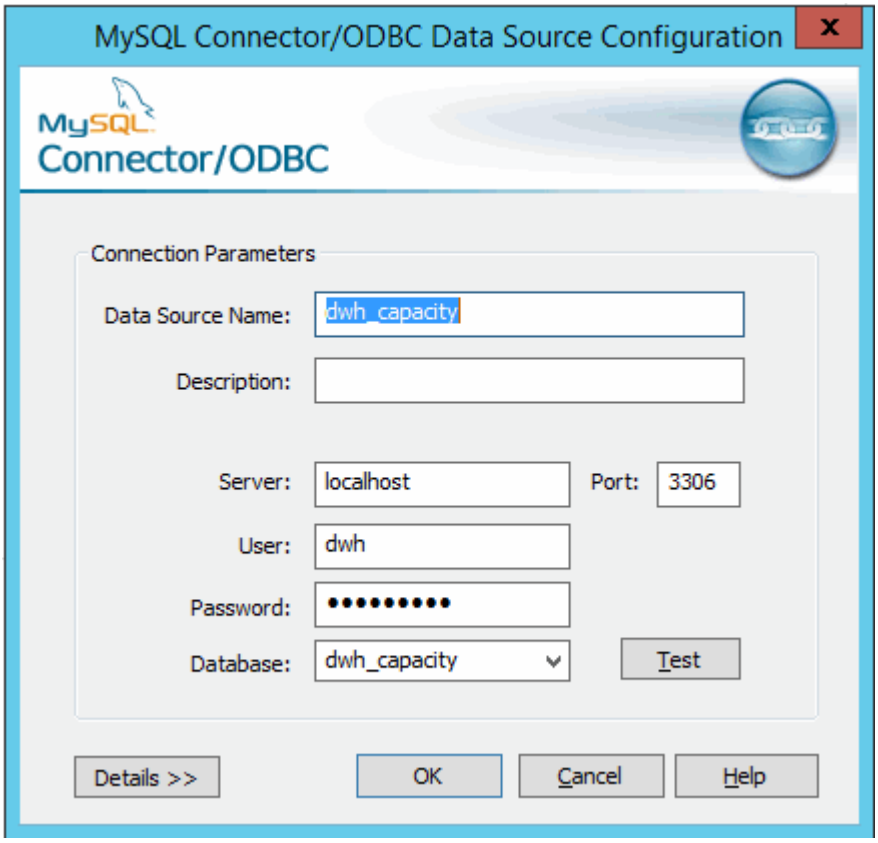
3. 單擊*系統DSN*

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。

如果使用更改了 *server.keystore* 和 / 或 *_server.trustore* 密碼*"安全性管理"*，請 *SANscreen* 在導入 *LDAP* 證書之前重新啓動 *_LDAP* 服務。

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。

根 CA 必須匯入信任存放區。

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「根憑證」 `/opt/netapp/oci/wildfly/standalone/configuration/server.truststore`
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。

> 如果使用更改了 *server.keystore* 和 / 或 *_server.trustore* 密碼"安全性管理"，請 *SANscreen* 在導入 *LDAP* 證書之前重新啓動 *_LDAP* 服務。

> 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``公用程式列出信任的 `CA` ： `C:\Program Files\SANscreen\java64\bin\keytool.exe -list -keystore server.trustore -storepass <password>` + 如需設定或變更 server_trustore 密碼的詳細資訊、請參閱"安全性管理"文件。

      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** 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`公用程式列出信任的 CA ： `..\IBM-JRE\JRE\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass <password>`

      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`通常是一個別名、可在作業中輕鬆識別 CA `keytool -list`。

f. 當系統提示您輸入密碼時、請輸入來自 __/m/bin/Cognos SANscreen info.dat 檔案的密碼。

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 7.3.10**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 <password> -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。
   c. 若為 <password> 、請使用來自 __/dat/bin/cognos SANscreen 資訊 .dat 檔案的密碼。
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\Cognos 。 crt -keystore Cognos \ anature\configuration\certs\CAMKeystore -storetype PKCS12 -storepass <password> -alias 加密
   c. 若為 <password> 、請使用來自 __/dat/bin/cognos SANscreen 資訊 .dat 檔案的密碼。
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:\temp\Cognos.crt -keystore wildfly\inold\configuration\server.trustore -storepass <password> -alias cognos3rdca
   c. 若為 <password> 、請使用來自 __/dat/bin/cognos SANscreen 資訊 .dat 檔案的密碼。
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 <password> -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。

> 如果使用更改了 *server.keystore* 和 / 或 *_server.trustore* 密碼"安全性管理"，請 *SANscreen* 在導入 *LDAP* 證書之前重新啓動 *_LDAP* 服務。

> 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`公用程式列出信任的 `CA` ： `C:\Program Files\SANscreen\java64\bin\keytool.exe -list -keystore server.trustore -storepass <password>` + 如需設定或變更 server_trustore 密碼的詳細資訊、請參閱"安全性管理"

文件。

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 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`公用程式列出信任的 CA ： `..\IBM-JRE\JRE\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass <password>`

      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`通常是一個別名、可在作業中輕鬆識別 CA `keytool -list`。

   f. 當系統提示您輸入密碼時、請輸入來自 __/m/bin/Cognos SANscreen info.dat 檔案的密碼。
   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 7.3.10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 <password> -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。
   c. 若為 <password> 、請使用來自 __/dat/bin/cognos SANscreen 資訊 .dat 檔案的密碼。
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\Cognos 。 crt -keystore Cognos \ anature\configuration\certs\CAMKeystore -storetype PKCS12 -storepass <password> -alias 加密
   c. 若為 <password> 、請使用來自 __/dat/bin/cognos SANscreen 資訊 .dat 檔案的密碼。
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:\temp\Cognos.crt -keystore wildfly\inold\configuration\server.trustore -storepass <password> -alias cognos3rdca
   c. 若為 <password> 、請使用來自 __/dat/bin/cognos SANscreen 資訊 .dat 檔案的密碼。

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 <password> -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

> 強烈建議您在升級之前備份資料保險箱。
>
> 如需有關資料保險箱和密碼管理的詳細資訊、請參閱"安全性管理工具"指示。

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"`

   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。

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

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。

Insight資料來源管理

資料來源是用來維護OnCommand Insight 整個環境的最重要元件。由於這些資料來源是Insight的主要資訊來源、因此您必須將資料來源維持在執行中狀態。

您可以選取資料來源來檢查與其狀態相關的事件、並記下可能造成問題的任何變更、藉此監控網路中的資料來源。

除了檢查個別資料來源之外、您還可以執行下列作業：

- 複製資料來源、在Insight中建立許多類似的資料來源
- 編輯資料來源資訊
- 變更認證資料
- 控制輪詢
- 刪除資料來源
- 安裝資料來源修補程式
- 從修補程式安裝新的資料來源
- 為NetApp客戶支援部門準備錯誤報告

在Insight中設定您的資料來源

資料來源是維護Insight環境最重要的元件。資料來源會探索用於分析和驗證的網路資訊。您需要在Insight中設定資料來源、以便在網路中監控。

對於每個資料來源、定義該資料來源的特定需求取決於對應裝置的廠商和機型。在新增資料來源之前、您需要所有裝置的網路位址、帳戶資訊和密碼、而且可能還需要這些額外詳細資料：

- 交換器
- 裝置管理站
- 具備IP連線能力的儲存系統
- 儲存管理站
- 執行管理軟體的主機伺服器、適用於沒有IP連線的儲存裝置

如需資料來源定義的詳細資訊、請參閱本節中的「廠商專屬資料來源參考」資訊。

資料來源支援資訊

在進行組態規劃時、您應確保Insight能夠監控環境中的裝置。若要這麼做、您可以查看資料來源支援對照表、以取得作業系統、特定裝置和傳輸協定的詳細資料。部分資料來源可能無法在所有作業系統上使用。

最新版資料來源支援對照表的位置

每個Service Pack版本都會更新《支援資料來源對照表》OnCommand Insight 。如需最新版本的文件、請參閱"NetApp 支援網站"。。

新增資料來源

您可以使用「新增資料來源」對話方塊、快速新增資料來源。

步驟

1. 在OnCommand Insight 瀏覽器中開啟、然後以具有管理權限的使用者身分登入。
2. 選擇*管理*並選擇*資料來源*。
3. 按一下「+附加」按鈕。

   此時會開啟「新增資料來源」精靈。

4. 在*設定*區段中、輸入下列資訊：

欄位	說明
名稱	輸入此資料來源的唯一網路名稱。附註：資料來源名稱僅允許使用字母、數字和底線（_）字元。
廠商	從下拉式清單中選擇資料來源的廠商。
模型	從下拉式清單中選擇資料來源的模型。
執行地點	選擇「本機」、或者如果您的環境中已設定Rau、您也可以選擇遠端擷取設備。
收集內容	對於大部分的資料來源、這些選項將是「庫存與效能」。庫存一律預設為選取狀態、無法取消選取。請注意、某些資料來源可能有不同的選項。您選取的集合選項會變更「組態」和「進階組態」區段中的可用欄位。

5. 按一下「組態」連結、輸入所選資料收集類型之資料來源所需的基本設定資訊。
6. 如果此類資料來源通常需要更詳細的資訊才能在網路中設定、請按一下*進階組態*連結以輸入其他資訊。
7. 如需特定資料來源所需或可用之組態或進階組態資訊的詳細"廠商專屬的資料來源參考"資訊，請參閱。
8. 按一下「* Test*」連結、確定資料來源已正確設定。

9. 按一下「 * 儲存 * 」。

從試算表匯入資料來源

您可以從OnCommand Insight 試算表將多個資料來源匯入到支援功能。如果您已在試算表中維護探索裝置、這可能很有幫助。此程序會新增資料來源、但無法用來更新現有的資料來源。

關於這項工作

包含試算表、可協助您建立資料來源OnCommand Insight 。此試算表具有下列屬性：

- 試算表可搭配Microsoft Excel 2003或更新版本使用。
- 每個索引標籤都有一種資料來源類型、例如Brocade SSE/CLI。
- 每一列代表要建立的新資料來源執行個體。

試算表包含一個巨集、可在OnCommand Insight 功能表中建立新的資料來源。

步驟

1. 在中找到試算表 `<install_directory>/SANscreen/acq/bin/acqcli/SiteSurvey_DataSourceImporter_w_Macro.zip`。
2. 在試算表中、以色彩在儲存格中輸入資料來源資訊。
3. 刪除空白列。
4. 從試算表執行 `CreateDataSources` 建立資料來源的巨集。
5. 當系統提示您輸入認證時、請輸入OnCommand Insight 支援伺服器的管理使用者名稱和密碼。

   結果會記錄在擷取記錄中。

6. 系統會出現提示、詢問目前執行巨集的機器是否OnCommand Insight 已安裝。

   選取下列其中一項：

   - 否：如果要建立批次檔、且必須在OnCommand Insight 該機器上執行、請選取「否」。從安裝目錄執行此批次檔。
   - 是：如果OnCommand Insight 已經安裝了此功能、請選取「是」、而且不需要其他步驟來產生資料來源資訊。
7. 若要驗證新增的資料來源、請在瀏覽器中開啟Insight。
8. 在Insight工具列上、按一下*管理*。
9. 檢查您匯入的資料來源清單。

透過修補程式新增資料來源

新的資料來源會以修補程式檔案形式發佈、並使用修補程序程序程序載入系統。此程序可讓OnCommand Insight 您在預定發行的版本之間取得新的資料來源。

開始之前

您必須上傳要安裝的修補程式檔案。

步驟

1. 在Insight工具列上、按一下*管理*。
2. 選擇*修補程式*。
3. 選取*「動作*」>*「安裝Service Pack或修補程式*」。
4. 在「安裝**Service Pack**或修補程式」對話方塊中、按一下「瀏覽」以找出並選取您上傳的修補程式檔案。
5. 按一下「修補摘要」對話方塊中的「下一步」。
6. 檢閱*讀取本人*資訊、然後按*下一步*繼續。
7. 在「安裝」對話方塊中、按一下「完成」。

複製資料來源

使用複製工具、您可以快速新增與其他資料來源具有相同認證和屬性的資料來源。複製可讓您輕鬆設定相同裝置類型的多個執行個體。

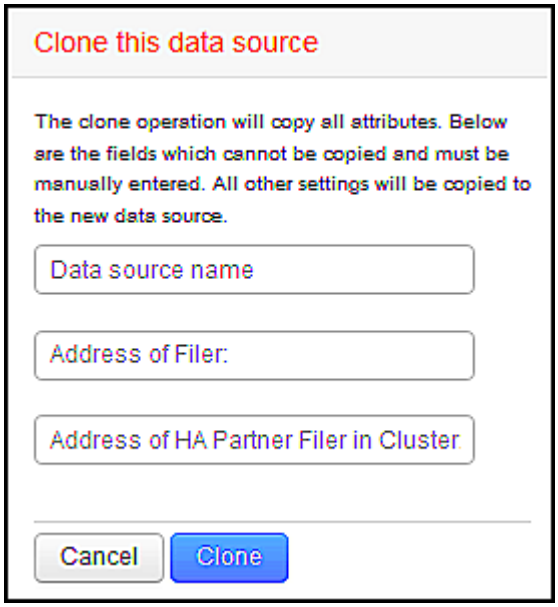
步驟

1. 在Insight工具列上、按一下*管理*。

   資料來源清單隨即開啟。

2. 反白顯示含有您要用於新資料來源之設定資訊的資料來源。
3. 在反白顯示的資料來源右側、按一下* Clone（複製）*圖示。

   Clone this data source（複製此資料來源）對話方塊會列出您必須為所選資料來源提供的資訊、如以下NetApp資料來源範例所示：



4. 在欄位中輸入必要資訊；這些詳細資料無法從現有的資料來源複製。
5. 按一下* Clone（複製）*。

結果

複製作業會複製所有其他屬性和設定、以建立新的資料來源。

測試資料來源組態

新增資料來源時、您可以在儲存或更新該資料來源之前、先驗證組態是否正確、以便與裝置通訊。

當您按一下資料來源精靈中的* Test*按鈕時、就會檢查與指定裝置的通訊。測試會產生下列其中一項結果：

- 通過：資料來源設定正確。
- 警告：測試不完整、可能是因為處理期間逾時或擷取未執行。
- 失敗：已設定的資料來源無法與指定的裝置通訊。檢查組態設定並重新測試。

廠商專屬的資料來源參考

組態詳細資料會因所新增資料來源的廠商和機型而有所不同。

如果廠商的資料來源需要進階的Insight組態指示、例如特殊需求和特定命令、則本節將會提供這些資訊。

3PAR InServ資料來源

使用3PAR InServ（韌體2.2.2+、SSH）資料來源、探索HP 3PAR StoreServ儲存陣列的庫存OnCommand Insight 。

術語

從3PAR InServ資料來源取得下列庫存資訊OnCommand Insight 。對於Insight取得的每種資產類型、都會顯示此資產最常用的術語。檢視或疑難排解此資料來源時、請謹記下列術語：

廠商/模型術語	Insight術語
實體磁碟	磁碟
儲存系統	儲存設備
控制器節點	儲存節點
通用資源配置群組	儲存資源池
虛擬Volume	Volume

這些只是通用的術語對應、可能不代表此資料來源的每個案例。

需求

- InServ叢集的IP位址或FQDN
- 針對庫存、InServ伺服器的唯讀使用者名稱和密碼。
- 為達到效能、請將使用者名稱和密碼讀寫至InServ伺服器。
- 連接埠需求：22（庫存收集）、5988或5989（效能收集）[附註：InServ OS 3.x+支援3PAR效能]
- 若要收集效能、請透過SSH登入3PAR陣列、確認SMI-S已啟用。

組態

欄位	說明
叢集IP	InServ叢集的IP位址或完整網域名稱
使用者名稱	InServ伺服器的使用者名稱
密碼	InServ伺服器使用的密碼
SMI-S主機IP	SMI-S Provider主機的IP位址
SMI-S使用者名稱	SMI-S Provider主機的使用者名稱
SMI-S密碼	SMI-S Provider主機使用的密碼

進階組態

欄位	說明
庫存輪詢時間間隔（分鐘）	庫存輪詢之間的時間間隔（預設為40分鐘）
排除裝置	要排除的裝置IP清單以逗號分隔
SSH程序等待逾時（秒）	SSH程序逾時（預設為60秒）
SSH重試次數	SSH重試嘗試次數
SSH橫幅等待逾時（秒）	SSH橫幅等待逾時（預設為20秒）
SMI-S連接埠	SMI-S Provider Host使用的連接埠
傳輸協定	用於連線至SMI-S供應商的傳輸協定

SMI-S命名空間	SMI-S命名空間
效能意見調查時間間隔（秒）	效能輪詢之間的時間間隔（預設為300秒）
SMI-S連線重試次數	SMI-S連線重試次數

Amazon AWS EC2資料來源

利用此資料來源探索Amazon AWS EC2的庫存和效能OnCommand Insight 。

先決條件：

若要從Amazon EC2裝置收集資料、您必須具備下列資訊：

- 您必須擁有IAM存取金鑰ID
- 您必須擁有Amazon EC2雲端帳戶的秘密存取金鑰
- 您必須擁有「清單組織」權限
- 連接埠433 HTTPS
- EC2執行個體可報告為虛擬機器、或（較不自然）主機。EBS Volume可報告為VM使用的虛擬磁碟、以及提供虛擬磁碟容量的資料存放區。

存取金鑰包含存取金鑰ID（例如：ASIIOSFODBNODNE7EXAMPLE）和秘密存取金鑰（例如：wJALrXUtnFEM/K7MDENG/bPxRfiCYEXAMPLEKEY）。如果您使用Amanzon EC2 SDK、REST或查詢API作業、您可以使用存取金鑰來簽署您對EC@提出的程式設計要求。這些金鑰會隨您的Amazon合約一起提供。

如何設定此資料來源

若要設定Amazon AWS EC2資料來源、您需要AWS帳戶的AWS IAM存取金鑰ID和秘密存取金鑰。

根據下表填寫資料來源欄位：

組態：

欄位	說明
AWS區域	選擇AWS區域
IAM角色	僅在AWS的AU上取得時使用。如需IAM角色的詳細資訊、請參閱下方。
AWS IAM存取金鑰ID	輸入AWS IAM存取金鑰ID。如果您不使用IAM角色、則為必要項目。
AWS IAM秘密存取金鑰	輸入AWS IAM秘密存取金鑰。如果您不使用IAM角色、則為必要項目。

我瞭解AWS會向我收取API要求的費用	請勾選此選項、確認您瞭解AWS會針對Insight輪詢所提出的API要求提出帳單

進階組態：

欄位	說明
包括額外的區域	指定要納入輪詢的其他區域。
跨帳戶角色	存取不同AWS帳戶中資源的角色。
庫存輪詢時間間隔（分鐘）	庫存輪詢之間的時間間隔（預設為60分鐘）
HTTP連線和通訊端逾時（秒）	HTTP連線逾時（預設為300秒）
包括AWS標籤	核取此選項、即可在Insight註釋中啟用AWS標籤支援
效能意見調查時間間隔（秒）	效能輪詢之間的時間間隔（預設為1800秒）

將**AWS**標籤對應至**Insight**標註

AWS EC2資料來源包含一個選項、可讓您使用AWS上設定的標記來填入Insight附註。註釋的名稱必須與AWS標籤完全相同。Insight一律會填入相同名稱的文字類型附註、並會「最佳」嘗試填入其他類型（數字、布林等）的附註。如果您的註釋類型不同、而且資料來源無法填入註釋、則可能需要移除註釋、然後以文字類型重新建立註釋。

請注意、AWS區分大小寫、而Insight則不區分大小寫。因此、如果您在Insight中建立名為「'Owner'」的註釋、並在AWS中建立名為「'Owner'」、「'Owner'」和「'Owner'」的標記、則所有的AWS變體「'Owner'」都會對應至Insight的「'Owner'」註釋。

相關資訊：

"管理IAM使用者的存取金鑰"

包括額外的區域

在AWS Data Collector 進階組態*區段中、您可以設定*包含額外區域*欄位、以英文或分號分隔、以包含其他區域。根據預設、此欄位會設為***_us-.**、收集所有美國AWS區域的資料。若要在_all_區域收集資料、請將此欄位設定為*。*。

如果*包含額外區域*欄位為空白、則資料收集器會收集在*組態*區段中指定的* AWS區域*欄位中所指定的資產。

從**AWS**子帳戶收集

Insight可在單一AWS資料收集器中、支援AWS子帳戶的集合。此集合的組態會在AWS環境中執行：

- 您必須將每個子帳戶設定為使用AWS角色、讓主要帳戶ID從子帳戶存取EC2詳細資料。
- 每個子帳戶都必須將角色名稱設定為相同字串

- 在「跨帳戶角色」欄位的Insight AWS Data Collector * Advanced Configuration（Insight AWS資料收集器*進階組態*）區段中輸入此角色名稱字串。

最佳實務做法：強烈建議將AWS預先定義的Amazon EC2ReadOnlyAccess原則指派給ECS主要帳戶。此外、在資料來源中設定的使用者應至少指派預先定義的_AWSOrganizationsReadOnlyAccess__policy、以便查詢AWS。

如需設定環境以允許Insight從AWS子帳戶收集的相關資訊、請參閱下列內容：

"教學課程：使用IAM角色委派整個AWS帳戶的存取權"

"AWS設定：在您擁有的另一個AWS帳戶中提供存取IAM使用者的權限"

"建立角色、將權限委派給IAM使用者"

IAM角色

使用_IAM角色_安全性時、您必須確保所建立或指定的角色擁有存取資源所需的適當權限。

例如、如果您建立名為_InstanceEc2ReadOnly_的IAM角色、則必須設定原則、將此IAM角色的所有EC2資源授予EC2唯讀清單存取權限。此外、您必須授予STs（安全性權杖服務）存取權、以便允許此角色擔任跨帳戶的角色。

建立IAM角色之後、您可以在建立新EC2執行個體或任何現有EC2執行個體時附加該角色。

將IAM角色_InstanceEec2ReadOnly_附加至EC2執行個體之後、您將能夠透過IAM角色名稱的執行個體中繼資料擷取暫用認證資料、並使用它來存取此EC2執行個體上執行的任何應用程式AWS資源。

只有在擷取設備執行於AWS執行個體時、才能使用IAM角色。

Brocade Enterprise Fabric Connectivity Manager資料來源

利用Brocade Enterprise Fabric Connectivity Manager（EFCM）資料來源、探索Brocade EFCM交換器的庫存OnCommand Insight 。Insight支援EFCM 9.5、9.6及9.7版。

需求

此資料收集器無法從OnCommand Insight 功能介紹7.3.11開始使用。

- EFCM伺服器的網路位址或完整網域名稱
- EFCM版本必須為9.5、9.6或9.7
- EFCM伺服器的IP位址
- EFCM伺服器的唯讀使用者名稱和密碼
- 已驗證從Insight伺服器透過Telnet存取Connectrix交換器、使用連接埠51512上的唯讀使用者名稱和密碼

組態

欄位	說明

EFC伺服器	EFC伺服器的IP位址或完整網域名稱
使用者名稱	交換器的使用者名稱
密碼	用於交換器的密碼

進階組態

欄位	說明
庫存輪詢時間間隔（分鐘）	庫存輪詢之間的時間間隔（預設為15分鐘）
網路名稱	要由EFCM資料來源回報的網路名稱。保留空白以將網路名稱報告為WWN。
通訊連接埠	用於與交換器通訊的連接埠
啟用資料綁定	選取以在從裝置接收SNMP設陷時啟用擷取。如果您選取「啟用補漏白」、也必須啟動SNMP。
設陷之間的最短時間（秒）	擷取嘗試之間由陷阱觸發的最短時間（預設為15秒）
非作用中的區域集	除了在作用中分區集上執行擷取之外、還要在其上執行擷取的非作用中分區清單
要使用的NIC	指定在SAN裝置上報告時、應在Rau上使用哪個網路介面
排除裝置	要在輪詢中包含或排除的單位名稱以逗號分隔的清單
使用EFCM交換器暱稱做為Insight交換器名稱	選取以使用EFCM交換器暱稱做為Insight交換器名稱
效能意見調查時間間隔（秒）	效能輪詢之間的時間間隔（預設為300秒）

Brocade FC交換器資料來源

支援使用Brocade FC交換器（SSH）資料來源來探索執行因素作業系統（FOS）韌體4.2及更新版本之Brocade或重新品牌交換器裝置的庫存OnCommand Insight 。同時支援FC交換器和存取閘道模式的裝置。

術語

從Brocade FC交換器資料來源取得下列庫存資訊OnCommand Insight 。對於Insight取得的每種資產類型、都會顯示此資產最常用的術語。檢視或疑難排解此資料來源時、請謹記下列術語：

廠商/模型術語	Insight術語
交換器	交換器
連接埠	連接埠
虛擬架構、實體架構	網路
區域	區域
邏輯交換器	邏輯交換器
LSAN區域	IVR區域

這些只是通用的術語對應、可能不代表此資料來源的每個案例。

需求

- 擷取單元（本機或遠端）會啟動與Brocade交換器TCP連接埠22的連線、以收集庫存資料。AU也會啟動連接至udp連接埠161的連線、以收集效能資料。
- 網路中的所有交換器都必須具備IP連線能力。如果您選取「Discover all switches in the fabric」（探索網路中的所有交換器）核取方塊、OCI會識別網路中的所有交換器；不過、它需要IP連線到這些額外交換器才能探索這些交換器。
- 網路中的所有交換器都需要相同的帳戶。您可以使用Putty（開放原始碼終端機模擬器）來確認存取。
- 如果安裝了Perform授權、則光纖網路中的所有交換器都必須開啟連接埠161和162、才能進行SNMP效能輪詢。
- SNMP唯讀社群字串

組態

欄位	說明
交換器IP	交換器的IP位址或完整網域名稱
使用者名稱	交換器的使用者名稱
密碼	用於交換器的密碼
SNMP版本	SNMP版本
SNMP社群字串	用於存取交換器的SNMP唯讀社群字串
SNMP使用者名稱	SNMP版本傳輸協定使用者名稱（僅適用於SNMP v3）

SNMP密碼	SNMP版本傳輸協定密碼（僅適用於SNMP v3）

進階組態

欄位	說明
網路名稱	要由資料來源回報的網路名稱。保留空白以將網路名稱報告為WWN。
排除裝置	要從輪詢中排除的裝置ID清單、以逗號分隔
庫存輪詢時間間隔（分鐘）	庫存輪詢之間的時間間隔（預設為15分鐘）
逾時（秒）	連線逾時（預設30秒）
橫幅等待逾時（秒）	SSH橫幅等待逾時（預設5秒）
管理網域作用中	如果使用管理網域、請選取
擷取MPR-資料	選取以從多重傳輸協定路由器（MPR-）取得路由資料
啟用資料綁定	選取以在從裝置接收SNMP設陷時啟用擷取。如果您選取「啟用補漏白」、也必須啟動SNMP。
設陷之間的最短時間（秒）	擷取嘗試之間由陷阱觸發的最短時間（預設為10秒）
探索網路中的所有交換器	選取以探索網路中的所有交換器
選擇「偏好HBA、而不是」區域別名	選擇是否偏好HBA或區域別名
效能意見調查時間間隔（秒）	效能輪詢之間的時間間隔（預設為300秒）
SNMP驗證傳輸協定	SNMP驗證傳輸協定（僅限SNMP v3）
SNMP隱私權傳輸協定	SNMP隱私傳輸協定（僅限SNMP v3）
SNMP隱私密碼	SNMP隱私密碼（僅限SNMP v3）
SNMP重試次數	SNMP重試嘗試次數
SNMP逾時（毫秒）	SNMP逾時（預設值5000毫秒）

Brocade Sphereon / Intrepid交換器資料來源

利用Brocade Sphereon / Intrepid交換器（SNMP）資料來源、探索Brocade Sphereon或Intrepid交換器的庫存OnCommand Insight 。

需求

> 此資料收集器無法從OnCommand Insight 功能介紹7.3.11開始使用。

- 網路中的所有交換器都必須具備IP連線能力。如果您選取「Discover all switches in the fabric」（探索網路中的所有交換器）核取方塊、OCI會識別網路中的所有交換器；不過、它需要IP連線到這些額外交換器才能探索這些交換器。
- 如果使用SNMP V1或SNMP V2、則為唯讀社群字串。
- 以HTTP存取交換器以取得分區資訊。
- 執行來存取驗證 `snmpwalk` 公用程式至交換器（請參閱 `<install_path\>\bin\)`。

組態

欄位	說明
Sphereon交換器	交換器的IP位址或完整網域名稱
SNMP版本	SNMP版本
SNMP社群	用於存取交換器的SNMP唯讀社群字串
使用者名稱	交換器的SMI-S使用者名稱（僅限SNMP v3）
密碼	交換器的SMI-S密碼（僅限SNMP v3）

進階組態

欄位	說明
庫存輪詢時間間隔（分鐘）	庫存輪詢之間的時間間隔（預設為15分鐘）
SNMP驗證傳輸協定	SNMP驗證傳輸協定（僅限v3）
SNMP隱私權傳輸協定	SNMP隱私傳輸協定（僅限v3）
SNMP隱私密碼	SNMP隱私密碼
SNMP重試次數	SNMP重試嘗試次數

SNMP逾時（毫秒）	SNMP逾時（預設值5000毫秒）
網路名稱	要由資料來源回報的網路名稱。保留空白以將網路名稱報告為WWN。
啟用資料綁定	選取以在從裝置接收SNMP設陷時啟用擷取。如果您選取「啟用補漏白」、也必須啟動SNMP。
Ttraps之間的最短時間（秒）	擷取嘗試之間由陷阱觸發的最短時間（預設為10秒）
效能意見調查時間間隔（秒）	效能輪詢之間的時間間隔（預設為300秒）

Cisco FC交換器韌體（**SNMP**）資料來源

利用Cisco FC交換器韌體2.0+（SNMP）資料來源、探索Cisco MDS Fibre Channel交換器的庫存、以及啟用FC服務的各種Cisco Nexus FCoE交換器OnCommand Insight 。此外、您也可以利用此資料來源、探索以NPV模式執行的許多Cisco裝置機型。

術語

從Cisco FC交換器資料來源取得下列庫存資訊OnCommand Insight 。對於Insight取得的每種資產類型、都會顯示此資產最常用的術語。檢視或疑難排解此資料來源時、請謹記下列術語：

廠商/模型術語	Insight術語
交換器	交換器
連接埠	連接埠
vSAN	網路
區域	區域
邏輯交換器	邏輯交換器
名稱伺服器項目	名稱伺服器項目
VSAN間路由（IVR）區域	IVR區域

這些只是通用的術語對應、可能不代表此資料來源的每個案例。

需求

- 網路或個別交換器中的一個交換器IP位址

- 機箱探索、以啟用網路探索
- 如果使用SNMP V2、則為唯讀社群字串
- 連接埠161用於存取裝置
- 使用存取驗證 `snmpwalk` 公用程式至交換器（請參閱 `<install_path\>\bin\`）

組態

欄位	說明
Cisco交換器IP	交換器的IP位址或完整網域名稱
SNMP版本	擷取效能時需要SNMP v2或更新版本
SNMP社群字串	用於存取交換器的SNMP唯讀社群字串（不適用於SNMP v3）
使用者名稱	交換器的使用者名稱（僅限SNMP v3）
密碼	用於交換器的密碼（僅限v3）

進階組態

欄位	說明
庫存輪詢時間間隔（分鐘）	庫存輪詢之間的時間間隔（預設為40分鐘）
SNMP驗證傳輸協定	SNMP驗證傳輸協定（僅限v3）
SNMP隱私權傳輸協定	SNMP隱私傳輸協定（僅限v3）
SNMP隱私密碼	SNMP隱私密碼
SNMP重試次數	SNMP重試嘗試次數
SNMP逾時（毫秒）	SNMP逾時（預設值5000毫秒）
啟用資料綁定	選取以啟用補漏白。如果啟用補漏白、您也必須啟動SNMP通知。
設陷之間的最短時間（秒）	擷取嘗試之間由陷阱觸發的最短時間（預設為10秒）
探索All Fabric交換器	選取以探索網路中的所有交換器

排除裝置	要從輪詢中排除的裝置IP清單、以逗號分隔
包括裝置	輪詢中要包含的裝置IP清單、以逗號分隔
檢查裝置類型	選取此選項、只接受明確宣稱自己為Cisco裝置的裝置
主要別名類型	提供別名解析的第一個偏好設定。請從下列選項中選擇： • 設備別名 這是連接埠WWN（pWWN）的易用名稱、可視需要用於所有組態命令。Cisco MDS 9000系列中的所有交換器都支援分散式裝置別名服務（裝置別名）。 • 無 請勿回報任何別名 • 連接埠說明 可協助識別連接埠清單中的連接埠的說明 • 區域別名（全部） 連接埠的使用者易記名稱、僅可用於分區組態 • 區域別名（僅作用中） 連接埠的使用者易記名稱、只能用於作用中組態。這是預設值。
次要別名類型	提供別名解析的第二個偏好設定
第三別名類型	提供別名解析的第三個偏好設定
啟用SANTAP Proxy模式支援	如果您的Cisco交換器在Proxy模式下使用SANTAP、請選取此選項。如果您使用的是EMC RecoverPoint、則可能是使用SANTap。
效能意見調查時間間隔（秒）	效能輪詢之間的時間間隔（預設為300秒）

EMC Celerra資料來源

Celerra（SSH）資料來源會從Celerra儲存設備收集庫存資訊。對於組態、此資料來源需要儲存處理器的IP位址、以及_唯讀_使用者名稱和密碼。

術語

從EMC Celerra資料來源取得下列庫存資訊OnCommand Insight 。對於Insight取得的每種資產類型、都會顯示此資產最常用的術語。檢視或疑難排解此資料來源時、請謹記下列術語：

廠商/模型術語	Insight術語
Celerra網路伺服器	儲存設備
Celerra中繼磁碟區/ Celerra儲存資源池	儲存資源池
檔案系統	內部Volume
資料移轉	控制器
掛載在Data Mover上的檔案系統	檔案共用
CIFS與NFS匯出	分享
磁碟區	後端LUN

這些只是通用的術語對應、可能不代表此資料來源的每個案例。

需求

- 儲存處理器的IP位址
- 唯讀使用者名稱和密碼
- SSH連接埠22

組態

欄位	說明
Celerra的位址	Celerra裝置的IP位址或完整網域名稱
使用者名稱	用於登入Celerra裝置的名稱
密碼	用於登入Celerra裝置的密碼

進階組態

欄位	說明
庫存輪詢時間間隔（分鐘）	庫存輪詢之間的時間間隔（預設為20分鐘）

SSH程序等待逾時（秒）	SSH程序逾時（預設為600秒）
重試次數	嘗試進行庫存重試的次數
SSH橫幅等待逾時（秒）	SSH橫幅等待逾時（預設為20秒）

EMC CLARiiON（NaviCLI）資料來源

在設定此資料來源之前、請先確定目標裝置和Insight伺服器上已安裝EMC Navisphere CLI。Navisphere CLI版本必須與控制器上的韌體版本相符。若要收集效能資料、必須開啟統計資料記錄功能。

Navisphere Command Line介面語法

```
naviseccli.exe -h <IP address> -user <user> -password <password> -scope
<scope,use 0 for global scope> -port <use 443 by default> command
```

術語

從EMC CLARiiON資料來源取得下列庫存資訊OnCommand Insight 。對於Insight取得的每種資產類型、都會顯示此資產最常用的術語。檢視或疑難排解此資料來源時、請謹記下列術語：

廠商/模型術語	Insight術語
磁碟	磁碟
儲存設備	儲存設備
儲存處理器	儲存節點
精簡集區、RAID群組	儲存資源池
LUN	Volume

這些只是通用的術語對應、可能不代表此資料來源的每個案例。

需求

- 每個CLARiiON儲存處理器的IP位址
- CLARiiON陣列的唯讀式Navisphere使用者名稱和密碼
- navicli必須安裝在Insight伺服器/ Rau上
- 存取驗證：使用上述使用者名稱和密碼、從Insight伺服器執行NaviCLI至每個陣列。

- navicli版本應與陣列上最新的Flare程式碼相對應
- 為了達到效能、必須開啟統計資料記錄功能。
- 連接埠需求：80、443

組態

欄位	說明
CLARiiON儲存設備	CLARiiON儲存設備的IP位址或完整網域名稱
使用者名稱	用於登入CLARiiON儲存設備的名稱。
密碼	用於登入CLARiiON儲存設備的密碼。
通往navicli.exe路徑或naviseccli.exe路徑的CLI路徑	的完整路徑 `navicli.exe` 或 `naviseccli.exe` 執行檔

進階組態

欄位	說明
庫存輪詢時間間隔（分鐘）	庫存輪詢之間的時間間隔（預設為40分鐘）
使用安全用戶端（naviseccli）	選擇使用安全用戶端（navseccli）
範圍	安全的用戶端範圍。預設值為Global。
CLARiiON CLI連接埠	用於CLARiiON CLI的連接埠
庫存外部處理逾時（秒）	外部處理程序逾時（預設值1800秒）
效能意見調查時間間隔（秒）	效能輪詢之間的時間間隔（預設為300秒）
效能外部處理逾時（秒）	外部處理程序逾時（預設值1800秒）

EMC Data Domain資料來源

此資料來源會從EMC Data Domain重複資料刪除儲存系統收集儲存與組態資訊。若要新增資料來源、您必須使用特定的組態指示和命令、並注意資料來源需求和使用建議。

術語

從EMC Data Domain資料來源取得下列庫存資訊OnCommand Insight 。對於Insight取得的每種資產類型、都會顯示此資產最常用的術語。檢視或疑難排解此資料來源時、請謹記下列術語：

廠商/模型術語	Insight術語
磁碟	磁碟
陣列	儲存設備
連接埠	連接埠
檔案	內部Volume
Mtree	qtree
配額	配額
NFS與CIFS共用	檔案共享

這些只是通用的術語對應、可能不代表此資料來源的每個案例。

需求

- 資料網域裝置的IP位址
- Data Domain儲存設備的唯讀使用者名稱和密碼
- SSH連接埠22

組態

欄位	說明
IP 位址	Data Domain儲存陣列的IP位址或完整網域名稱
使用者名稱	Data Domain儲存陣列的使用者名稱
密碼	Data Domain儲存陣列的密碼

進階組態

欄位	說明
庫存輪詢時間間隔（分鐘）	庫存輪詢之間的時間間隔（預設為20分鐘）
SSH程序等待逾時（秒）	SSH程序逾時（預設為180秒）
SSH連接埠	SSH服務連接埠

EMC ECC StorageScope資料來源

EMC ECC StorageScope裝置有三種類型的資料來源：5.x、6.0和6.1。

組態

此資料收集器已不再提供OnCommand Insight 、從版本號為e.7.3.11開始。

欄位	說明
ECC伺服器	ECC伺服器的IP位址或完整網域名稱
使用者名稱	ECC伺服器的使用者名稱
密碼	ECC伺服器的密碼

進階組態

欄位	說明
ECC連接埠	用於ECC伺服器的連接埠
庫存輪詢時間間隔（分鐘）	庫存輪詢之間的時間間隔（預設為30分鐘）
連接至資料庫的傳輸協定	用於連線至資料庫的傳輸協定
查詢檔案系統資訊	選取以擷取WWN別名和檔案系統的詳細資料。

Dell EMC ECS資料來源

此資料收集器會從EMC ECS儲存系統取得庫存和效能資料。對於組態、資料收集器需要ECS伺服器的IP位址和管理層級網域帳戶。

術語

從EMC ECS資料來源取得下列庫存資訊OnCommand Insight 。對於Insight取得的每種資產類型、都會顯示此資產最常用的術語。檢視或疑難排解此資料來源時、請謹記下列術語：

廠商/模型術語	Insight術語
ClUser	儲存設備
租戶	儲存資源池
鏟斗	內部Volume

磁碟	磁碟

這些只是通用的術語對應、可能不代表此資料來源的每個案例。

需求

- ECS管理主控台的IP位址
- ECS系統的管理層級網域帳戶
- 連接埠443（HTTPS）。需要連線至ECS系統上的TCP連接埠443。
- 若要獲得效能、請使用唯讀的使用者名稱和密碼進行ssh / scp存取。
- 為了達到效能、需要連接埠22。

組態

欄位	說明
ECS主機	ECS系統的IP位址或完整網域名稱
ECS主機連接埠	用於與ECS主機通訊的連接埠
ECS廠商ID	ECS的廠商ID
密碼	用於ECS的密碼

進階組態

欄位	說明
庫存輪詢時間間隔（分鐘）	庫存輪詢之間的時間間隔。預設值為360分鐘。

EMC Isilon資料來源

Isilon SSH資料來源會從EMC Isilon橫向擴充NAS儲存設備收集庫存和效能。

術語

從EMC Isilon資料來源取得下列庫存資訊OnCommand Insight 。對於Insight取得的每種資產類型、都會顯示此資產最常用的術語。檢視或疑難排解此資料來源時、請謹記下列術語：

廠商/模型術語	Insight術語
磁碟機	磁碟
叢集	儲存設備

節點	儲存節點
檔案系統	內部Volume

這些只是通用的術語對應、可能不代表此資料來源的每個案例。

需求

- Isilon儲存設備的系統管理員權限
- 使用驗證存取 `telnet` 連接埠22

組態

欄位	說明
IP 位址	Isilon叢集的IP位址或完整網域名稱
使用者名稱	Isilon叢集的使用者名稱
密碼	Isilon叢集的密碼

進階組態

欄位	說明
庫存輪詢時間間隔（分鐘）	庫存輪詢之間的時間間隔（預設為20分鐘）
效能意見調查時間間隔（秒）	效能輪詢之間的時間間隔（預設為300秒）
SSH程序等候逾時	SSH程序逾時（預設為60秒）
SSH連接埠	SSH服務連接埠

執行**CLI**命令

從版本7.3.11和Service Pack 9開始OnCommand Insight 、EMC Isilon資料來源包含一項增強功能、可讓Insight執行更多CLI命令。如果您在資料來源中使用非root使用者、您可能已設定「sudoers」檔案、以授予該使用者帳戶透過SSH執行特定CLI命令的能力。

為了讓Insight瞭解EMC的「存取區域」功能、Insight現在將另外執行下列新的CLI命令：

- `sudo isi zone zones list --format json -verbose`
- `sudo isi zone zones list`

Insight會剖析這些命令的輸出、並執行更多現有命令的執行個體、以取得位於非預設存取區域的物件邏輯組態、

例如qtree、配額和NAS共用/匯出。Insight現在會針對非預設存取區域報告這些物件、因為這項增強功能。當Insight透過執行現有命令（使用不同選項）來取得資料時、不需要變更任何資料即可正常運作；只有在上述新命令推出後、才需要變更。

請更新您的sudoers檔案、以便Insight服務帳戶在升級至此Insight版本之前執行這些命令。否則、您的Isilon資料來源將會失敗。

「檔案系統」統計資料

EMC Isilon資料收集器從OnCommand Insight 功能完善的7.3.12開始、針對EMC Isilon的節點物件引進「檔案系統」統計資料。由ENetApp報告的現有節點統計資料OnCommand Insight 是以「磁碟」為基礎、例如、對於IOPs和儲存節點的處理量、此節點中的磁碟在集合體中有什麼作用？但對於快取記憶體中的讀取和/或壓縮正在使用中的工作負載、檔案系統工作負載可能遠高於實際達到磁碟的工作負載、因此壓縮5：1的資料集可能會有「檔案系統讀取處理量」值、即儲存節點讀取處理量的5倍、 當後者測量磁碟的讀取時、當節點解壓縮資料以服務用戶端的讀取要求時、磁碟的讀取量會增加5倍。

Dell EMC PowerStore資料來源

Dell EMC PowerStore資料收集器會從Dell EMC PowerStore儲存設備收集庫存資訊。對於組態、資料收集器需要儲存處理器的IP位址、以及唯讀使用者名稱和密碼。

術語

從EMC Data Domain資料來源取得下列庫存資訊OnCommand Insight 。對於Insight取得的每種資產類型、都會顯示此資產最常用的術語。檢視或疑難排解此資料來源時、請謹記下列術語：

廠商/模型術語	Insight術語
主機	主機
主機磁碟區對應	主機磁碟區對應
硬體（在「Extra _details」（額外詳細資料）物件下有磁碟機）：磁碟機	磁碟
應用裝置	StoragePool
叢集	儲存陣列
節點	StorageNode
FC_port	連接埠
Volume	Volume
內部Volume	檔案系統
檔案	內部Volume

Mtree	qtree
配額	配額
NFS與CIFS共用	檔案共享

這些只是通用的術語對應、可能不代表此資料來源的每個案例。

需求

- 儲存處理器的IP位址或完整網域名稱
- 唯讀使用者名稱和密碼

父序號說明

傳統上Insight能夠報告儲存陣列序號或個別儲存節點序號。不過、有些儲存陣列架構並未完全符合此要求。PowerStore叢集可由1-4個應用裝置組成、每個應用裝置有2個節點。如果應用裝置本身有序號、則該序號既不是叢集的序號、也不是節點的序號。

儲存節點物件上的「父序號」屬性會針對Dell/EMC PowerStore陣列適當填入、當個別節點位於僅屬於大型叢集一部分的中繼應用裝置/機箱內時。

組態

欄位	說明
PowerStore閘道	PowerStore儲存設備的IP位址或完整網域名稱
使用者名稱	PowerStore的使用者名稱
密碼	PowerStore使用的密碼

進階組態

欄位	說明
HTTPS連接埠	預設值為443
庫存輪詢時間間隔（分鐘）	庫存輪詢之間的時間間隔。預設值為60分鐘。

利用PowerStore的5分鐘精細資料來源、即可獲得VMware Insight的PowerStore效能集合OnCommand 。因此、Insight會每五分鐘輪詢一次該資料、而且這是無法設定的。

EMC RecoverPoint資料來源

EMC RecoverPoint資料來源會從EMC RecoverPoint儲存設備收集庫存資訊。對於組態、

資料來源需要儲存處理器的IP位址、以及_唯讀_使用者名稱和密碼。

EMC RecoverPoint資料來源會收集RecoverPoint在其他儲存陣列之間協調的磁碟區對磁碟區複寫關係。顯示每個RecoverPoint叢集的儲存陣列、並收集該叢集上節點和儲存連接埠的庫存資料OnCommand Insight 。不會收集儲存資源池或Volume資料。

需求

- 儲存處理器的IP位址或完整網域名稱
- 唯讀使用者名稱和密碼
- 透過連接埠443進行REST API存取
- 透過Putty存取SSH

組態

欄位	說明
RecoverPoint的位址	RecoverPoint叢集的IP位址或完整網域名稱
使用者名稱	RecoverPoint叢集的使用者名稱
密碼	RecoverPoint叢集的密碼

進階組態

欄位	說明
TCP連接埠	用於連線至RecoverPoint叢集的TCP連接埠
庫存輪詢時間間隔（分鐘）	庫存輪詢之間的時間間隔（預設為20分鐘）
排除的叢集	輪詢時要排除的叢集ID或名稱清單、以逗號分隔

EMC解決方案運用**SMI-S**效能資料來源來實現

利用Solutions Enabler探索Symmetrix儲存陣列OnCommand Insight `symcli` 命令搭配您環境中現有的Solutions Enabler伺服器。現有的Solutions Enabler伺服器可透過存取關守磁碟區、連線至Symmetrix儲存陣列。需要系統管理員權限才能存取此裝置。

術語

從EMC Solutions Enabler資料來源取得下列庫存資訊OnCommand Insight 。對於Insight取得的每種資產類型、都會顯示此資產最常用的術語。檢視或疑難排解此資料來源時、請謹記下列術語：

廠商/模型術語	Insight術語

磁碟	磁碟
磁碟群組	磁碟群組
儲存陣列	儲存設備
總監	儲存節點
裝置集區、儲存資源集區（SRP）	儲存資源池
裝置、TDev	Volume

這些只是通用的術語對應、可能不代表此資料來源的每個案例。

需求

在設定此資料來源之前、您應先確定OnCommand Insight 該伺服器已將TCP連線至現有Solutions Enabler伺服器上的連接埠2707。可探索此伺服器的所有「'local'」Symmetrix陣列、如該伺服器的「'symcfg list'」輸出所示OnCommand Insight 。

- 必須安裝採用SMI-S供應商應用程式的EMC Solutions Enabler（CLI）、且版本必須與Solutions Enabler Server上執行的版本相符或早於該版本。
- 正確設定 `{installdir}\EMC\SYMAPI\config\netcnfg` 檔案為必填。此檔案定義Solutions Enabler伺服器的服務名稱、以及存取方法（安全/ NOSEECURE /any）。
- 如果您需要儲存節點層級的讀取/寫入延遲、SMI-S Provider必須與VMAX應用程式的Unif則 執行中執行個體通訊。
- Solutions Enabler（SE）伺服器的系統管理員權限
- SE軟體的唯讀使用者名稱和密碼
- 解決方案促成伺服器6.5x需求：
  - SMI-S Provider 3.3.1（已安裝SMS-S V1.2）
  - 安裝後、請執行 `\Program Files\EMC\SYMCLI\bin>stordaemon start storsrvd`
- VMAX應用程式的Un禁 用型錄必須執行、並收集由SMI-S Provider安裝所管理的Symmetrix VMAX儲存陣列統計資料
- 存取驗證：確認SMI-S供應商正在執行： `telnet <se_server\> 5988`

組態

如果SMI-S使用者驗證未啟用、OnCommand Insight 則會忽略支援資訊來源中的預設值。

在Symmetrix陣列上啟用symauth、可能會阻礙OnCommand Insight 執行支援功能。系統使用者可在與Solutions Enabler伺服器通訊的E/遠端擷取單元伺服器上執行OnCommand Insight OnCommand Insight 。如果hostname\system沒有symauth權限、OnCommand Insight 則無法探索陣列。

EMC Solutions Enabler Symmetrix CLI資料來源支援精簡配置和Symmetrix Remote Data Facility（SRDF）的裝置組態。

提供光纖通道和交換器效能套件的定義。

欄位	說明
服務名稱	netcnfg-file中指定的服務名稱
CLI的完整路徑	Symmetrix CLI的完整路徑

進階組態

欄位	說明
庫存輪詢時間間隔（分鐘）	庫存輪詢之間的時間間隔（預設為40分鐘）
選擇「排除」或「包含」以指定清單	指定在收集資料時是否要納入或排除下列陣列清單
庫存排除裝置	要包含或排除的裝置ID清單、以逗號分隔
連線快取	選擇連線快取方法： • 本機是指OnCommand Insight 在Solutions Enabler伺服器上執行的「支援資料」服務、該伺服器具備光纖通道連線功能、可連線至您想要探索的Symmetrix陣列、並可存取關守磁碟區。部分遠端擷取設備（Rau）組態可能會出現此情形。 • remide_bed是預設值、在大多數情況下都應該使用。這會使用NETCNFG檔案設定、使用IP連線至Solutions Enabler伺服器、該伺服器必須具備光纖通道連線至您要探索的Symmetrix陣列、並可存取Gatekeeper磁碟區。 • 如果reme_clapped選項使CLI命令失敗、請使用遠端選項。請記住、這會拖慢擷取程序（在極端情況下可能會減至數小時甚至數天）。NETCNFG檔案設定仍可用於連接至Solutions Enabler伺服器的IP連線、該伺服器的Fibre Channel可連線至正在探索的Symmetrix陣列。 ⓘ 此設定不會變更OnCommand Insight「symcfg清單」輸出中所列為遠端陣列的非功能性行為。僅在本命令顯示為本機的裝置上收集資料OnCommand Insight 。
CLI逾時（秒）	CLI處理逾時（預設值為7200秒）

SMI-S主機IP	SMI-S Provider主機的IP位址
SMI-S連接埠	SMI-S Provider Host使用的連接埠
傳輸協定	用於連線至SMI-S供應商的傳輸協定
SMI-S命名空間	SMI-S供應商設定使用的互通性命名空間
SMI-S使用者名稱	SMI-S Provider主機的使用者名稱
SMI-S密碼	SMI-S Provider主機的使用者名稱
效能輪詢時間間隔（秒）	效能輪詢之間的時間間隔（預設為1000秒）
效能篩選器類型	指定在收集效能資料時、是否要納入或排除下列陣列清單
效能篩選器裝置清單	要包含或排除的裝置ID清單、以逗號分隔
RPO輪詢時間間隔（秒）	RPO輪詢之間的時間間隔（預設為300秒）

EMC VNX資料來源

對於組態設定、EMC VNX（SSH）資料來源需要控制站的IP位址、以及_唯讀_使用者名稱和密碼。

組態

欄位	說明
VNX IP	VNX Control Station的IP位址或完整網域名稱
VNX使用者名稱	VNX Control Station的使用者名稱
VNX密碼	VNX Control Station的密碼

需求

- Control Station的IP位址
- 唯讀使用者名稱和密碼。
- 存取驗證：透過Putty驗證SSH存取。

進階組態

欄位	說明
庫存輪詢時間間隔（分鐘）	庫存輪詢之間的時間間隔（預設為40分鐘）
VNX SSH程序等待逾時（秒）	VNX SSH程序逾時（預設為600秒）
Celerra命令重試嘗試次數	Celerra命令重試嘗試次數
庫存的CLARiiON外部程序逾時（秒）	庫存的CLARiiON外部程序逾時（預設值為1800秒）
效能意見調查時間間隔（秒）	效能輪詢之間的時間間隔（預設為300秒）
CLARiiON外部處理效能逾時（秒）	CLARiiON外部處理逾時效能（預設為1800秒）

EMC VNXe資料來源

EMC VNXe資料來源為EMC VNXe和Unity統一化儲存陣列提供庫存支援。

此資料來源是以CLI為基礎、您必須在VNXe資料來源所在的擷取設備上安裝適用於VNXe CLI（uemcli・exe）的Uner主機。uemcli.exe使用HTTPS作為傳輸傳輸傳輸傳輸協定、因此擷取單位必須能夠起始與VNXe/Unity陣列的HTTPS連線。您必須至少有唯讀使用者、才能供資料來源使用。

術語

從EMC VNXe資料來源取得下列庫存資訊OnCommand Insight 。對於Insight取得的每種資產類型、都會顯示此資產最常用的術語。檢視或疑難排解此資料來源時、請謹記下列術語：

廠商/模型術語	Insight術語
磁碟	磁碟
儲存陣列	儲存設備
處理器	儲存節點
儲存資源池	儲存資源池
一般iSCSI區塊資訊、VMware VMFS	Volume
共享資料夾	內部Volume
CIFS共用、NFS共用、從VMware NFS資料存放區共用	分享

複寫遠端系統	同步
iSCSI節點	iSCSI目標節點
iSCSI啟動器	iSCSI目標啟動器

這些只是通用的術語對應、可能不代表此資料來源的每個案例。

需求

以下是設定及使用此資料來源的需求：

- VNXe資料收集器是以CLI為基礎；您必須將Unaeris for VNXe CLI（uemcli．exe）安裝到VNXe資料收集器所在的擷取單元上。
- uemcli.exe使用HTTPS作為傳輸傳輸傳輸傳輸協定、因此擷取單位必須能夠啟動HTTPS連線至VNXe。
- 您必須至少有唯讀使用者、才能供資料來源使用。
- 管理解決方案促成者伺服器的IP位址。
- 連接埠443需要HTTPS
- EMC VNXe資料收集器提供NAS與iSCSI的庫存支援；光纖通道磁碟區將會被探索、但Insight不會報告FC對應、遮罩或儲存連接埠。

組態

欄位	說明
VNXe儲存設備	VNXe裝置的IP位址或完整網域名稱
使用者名稱	VNXe裝置的使用者名稱
密碼	VNXe裝置的密碼
uemcli執行檔的完整路徑	的完整路徑 `uemcli.exe` 執行檔

進階組態

欄位	說明
庫存輪詢時間間隔（分鐘）	庫存輪詢之間的時間間隔（預設為40分鐘）
VNXe CLI連接埠	用於VNXe CLI的連接埠
庫存外部處理逾時（秒）	外部處理程序逾時（預設值1800秒）

EMC VPLEX資料來源

對於組態、此資料來源需要VPLEX伺服器的IP位址和管理層級網域帳戶。

術語

從EMC VPLEX資料來源取得下列庫存資訊OnCommand Insight 。對於Insight取得的每種資產類型、都會顯示此資產最常用的術語。檢視或疑難排解此資料來源時、請謹記下列術語：

廠商/模型術語	Insight術語
叢集	儲存設備
引擎	儲存節點
裝置、系統擴充	後端儲存資源池
虛擬Volume	Volume
前端連接埠、後端連接埠	連接埠
分散式裝置	儲存同步
儲存檢視	Volume Map、Volume Mask
儲存Volume	後端LUN
ITLs	後端路徑

這些只是通用的術語對應、可能不代表此資料來源的每個案例。

需求

- VPLEX伺服器的IP位址
- VPLEX伺服器的管理層級網域帳戶
- 連接埠443（HTTPS）。需要連線至VPLEX管理站台上的TCP連接埠443。
- 若要獲得效能、請使用唯讀的使用者名稱和密碼進行ssh / scp存取。
- 為了達到效能、需要連接埠22。
- 驗證存取：使用進行驗證 `telnet` 連接埠443。用於預設連接埠以外的連接埠、並使用任何瀏覽器

組態

欄位	說明

VPLEX管理主控台的IP位址	VPLEX管理主控台的IP位址或完整網域名稱
使用者名稱	VPLEX CLI的使用者名稱
密碼	VPLEX CLI使用的密碼
VPLEX管理主控台的效能遠端IP位址	VPLEX管理主控台的效能遠端IP位址
效能遠端使用者名稱	Performance VPLEX管理主控台的遠端使用者名稱
效能遠端密碼	VPLEX管理主控台的效能遠端密碼

進階組態

欄位	說明
通訊連接埠	用於VPLEX CLI的連接埠
庫存輪詢時間間隔（分鐘）	庫存輪詢之間的時間間隔（預設為20分鐘）
連線逾時（秒）	連線逾時（預設為60秒）
重試次數	嘗試進行庫存重試的次數
效能意見調查時間間隔（秒）	效能輪詢之間的時間間隔（預設為600秒）
效能SSH程序等待逾時（秒）	SSH程序逾時（預設為600秒）
SSH橫幅等待逾時（秒）	SSH橫幅等待逾時（預設為20秒）
重試次數	重試效能的次數

EMC XtremIO資料來源

若要設定EMC XtremIO（HTTP）資料來源、您必須擁有XtremIO管理伺服器（XMS）主機位址、以及具有系統管理員權限的帳戶。

術語

從EMC XtremIO資料來源取得下列庫存資訊OnCommand Insight 。對於Insight取得的每種資產類型、都會顯示此資產最常用的術語。檢視或疑難排解此資料來源時、請謹記下列術語：

廠商/模型術語	Insight術語

磁碟（SSD）	磁碟
叢集	儲存設備
控制器	儲存節點
Volume	Volume
LUN對應	Volume Map
啟動器、目標	Volume遮罩

這些只是通用的術語對應、可能不代表此資料來源的每個案例。

需求

- 每個XtremIO管理伺服器的IP位址
- 具有管理員權限的帳戶
- 存取連接埠443（HTTPS）

組態

欄位	說明
XMS主機	XtremIO管理伺服器的IP位址或完整網域名稱
使用者名稱	XtremIO管理伺服器的使用者名稱
密碼	XtremIO管理伺服器的密碼

進階組態

欄位	說明
TCP連接埠	TCP連接埠用於連線至XTremIO管理伺服器（預設443）
庫存輪詢時間間隔（分鐘）	庫存輪詢之間的時間間隔（預設為60分鐘）
連線逾時（秒）	連線逾時（預設為60秒）
效能意見調查時間間隔（秒）	效能輪詢之間的時間間隔（預設為300秒）

Fujitsu Eternus資料來源

Fujitsu Eternus資料來源需要儲存設備的IP位址。不能以逗號分隔。

術語

從Fujitsu Eternus資料來源取得下列庫存資訊OnCommand Insight 。對於Insight取得的每種資產類型、都會顯示此資產最常用的術語。檢視或疑難排解此資料來源時、請謹記下列術語：

廠商/模型術語	Insight術語
磁碟	磁碟
儲存設備	儲存設備
精簡集區、彈性層級集區、 RAID群組	儲存資源池
標準Volume、Snap Data Volume（SDV）、 SnapData Pool Volume（SDPV）、 精簡配置磁碟區（TPV）	Volume

這些只是通用的術語對應、可能不代表此資料來源的每個案例。

需求

- 外部儲存設備的IP位址、不能以逗號分隔
- SSH管理層級的使用者名稱和密碼
- 連接埠22
- 確定已停用頁面捲動。（停用clilenv-show-More捲動功能）

組態

欄位	說明
外部儲存設備的IP位址	外部儲存設備的IP位址
使用者名稱	外部儲存設備的使用者名稱
密碼	用於sternus的密碼

進階組態

欄位	說明
庫存輪詢時間間隔（分鐘）	庫存輪詢之間的時間間隔（預設為20分鐘）
SSH程序等待逾時（秒）	SSH程序逾時（預設為600秒）

Hitachi Content Platform（HCP）資料來源

此資料收集器使用保健專業人員管理API支援Hitachi內容平台（HCPs）。

術語

從保健專業人員資料來源取得下列庫存資訊OnCommand Insight 。對於Insight取得的每種資產類型、都會顯示此資產最常用的術語。檢視或疑難排解此資料來源時、請謹記下列術語：

廠商/模型術語	Insight術語
保健專業人員叢集	儲存設備
租戶	儲存資源池
命名空間	內部Volume
節點	節點

這些只是通用的術語對應、可能不代表此資料來源的每個案例。

庫存需求

- hcp.伺服器的IP位址
- 用於保健專業人員軟體和對等權限的唯讀使用者名稱和密碼

組態

欄位	說明
HCP主機	hcp.主機的IP位址或完整網域名稱
hcp.連接埠	預設值為9090
hcp.使用者ID	hcp.主機的使用者名稱
hcp.密碼	用於保健專業人員主機的密碼

HCP-驗證類型	選擇HCP_local或active_directory

進階組態

欄位	說明
庫存輪詢時間間隔（分鐘）	庫存輪詢之間的時間間隔（預設為60分鐘）
效能輪詢時間間隔（秒）	效能輪詢之間的時間間隔（預設為900秒）

HDS HiCommand Device Manager資料來源

HDS HiCommand和1TB精簡版資料來源支援該伺服器。使用標準的HiCommand API與HiCommand Device Manager伺服器通訊OnCommand Insight 。

術語

從HDS的Hndon和Hndon Lite資料來源取得下列庫存資訊OnCommand Insight 。對於Insight取得的每種資產類型、都會顯示此資產最常用的術語。檢視或疑難排解此資料來源時、請謹記下列術語：

廠商/模型術語	Insight術語
PDEV	磁碟
日誌集區	磁碟群組
儲存陣列	儲存設備
連接埠控制器	儲存節點
Array Group、DP Pool	儲存資源池
邏輯單元、LDEV	Volume

這些只是通用的術語對應、可能不代表此資料來源的每個案例。

庫存需求

- Hndvice Manager伺服器的IP位址
- 適用於HiCommand Device Manager軟體和對等權限的唯讀使用者名稱和密碼
- 連接埠需求：2001（http）或2443（https）
- 驗證存取：
  - 使用對等使用者名稱和密碼登入HiCommand Device Manager軟體。

- 驗證對HiCommand Device Manager API的存取： `telnet <HiCommand Device_Manager_server_ip\> 2001`

效能要求

- HDS USP、USP V和VSP效能
  - 效能監視器必須獲得授權。
  - 必須啟用監控交換器。
  - 匯出工具 (`Export.exe`）必須複製到OnCommand Insight The樣部伺服器。
  - 匯出工具版本必須符合目標陣列的微碼版本。
- HDS AMS效能
  - 效能監視器必須獲得授權。
  - 儲存導覽器模組2（SNM2）CLI公用程式需要安裝在OnCommand Insight SView Server上。
  - 您必須使用OnCommand Insight 下列命令、登錄所有需要由VMware取得效能的AMS、wms、SMS儲存陣列：
  - 您必須確保您註冊的所有陣列都列在此命令的輸出中： `auunitref.exe`。

組態

欄位	說明
和服務器	Hndvice Manager伺服器的IP位址或完整網域名稱
使用者名稱	使用者名稱。
密碼	用於HiCommand Device Manager伺服器的密碼。
裝置- VSP G1000（R800）、VSP（R700）、Hus VM（HM700）和USP儲存設備	VSP G1000（R800）、VSP（R700）、Hus VM（HM700）和USP儲存設備清單。每個儲存設備都需要： • 陣列的IP：儲存設備的IP位址 • 使用者名稱：儲存設備的使用者名稱 • 密碼：儲存設備的密碼 • 包含匯出公用程式Jar檔案的資料夾：包含匯出公用程式的資料夾 `.jar` 檔案

SNM2Device - WMS/SMS/AMS儲存	WMS/SMS/AMS儲存設備清單。每個儲存設備都需要： • 陣列的IP：儲存設備的IP位址 • Storage Navigator CLI路徑：SNM2 CLI路徑 • 帳戶驗證有效：選取以選擇有效的帳戶驗證 • 使用者名稱：儲存設備的使用者名稱 • 密碼：儲存設備的密碼
選擇「效能調校管理程式」	選擇「調校管理程式」以獲得效能、並覆寫其他效能選項
調校管理程式主機	調整管理程式的IP位址或完整網域名稱
調校管理器連接埠	用於調整管理程式的連接埠
調校管理程式使用者名稱	調整管理程式的使用者名稱
調校管理員密碼	調整管理程式的密碼

在HDS USP、USP V和VSP中、任何磁碟都可以屬於多個陣列群組。

進階組態

欄位	說明
Hndl伺服器連接埠	用於「HiCommand Device Manager」的連接埠
HTTPS已啟用	選取以啟用HTTPS
庫存輪詢時間間隔（分鐘）	庫存輪詢之間的時間間隔（預設為40分鐘）
選擇「排除」或「包含」以指定清單	指定在收集資料時是否要納入或排除下列陣列清單
排除或包含裝置	要包含或排除的裝置ID或陣列名稱清單、以逗號分隔
查詢主機管理程式	選取以查詢主機管理程式
HTTP逾時（秒）	HTTP連線逾時（預設為60秒）
效能輪詢時間間隔（秒）	效能輪詢之間的時間間隔（預設為300秒）

匯出逾時（以秒為單位）	匯出公用程式逾時（預設為300秒）

Hitachi Ops Center資料收集器

此資料收集器使用Hitachi Ops Center的整合式應用程式套件來存取多個儲存設備的庫存和效能資料。針對庫存和容量探索、您的Ops Center安裝必須同時包含「Common Services」（通用服務）和「Administrator」（管理員）元件。為了收集效能、您還必須部署「分析器」。

術語

OnCommand Insight 會從此資料收集器取得下列庫存資訊。對於所取得的每種資產類型、都會顯示此資產最常用的術語。檢視或疑難排解此資料收集器時、請謹記下列術語：

廠商/模型術語	詞彙**OnCommand Insight**
儲存系統	儲存設備
Volume	Volume
同位元檢查群組	儲存資源池（RAID）、磁碟群組
磁碟	磁碟
儲存資源池	儲存資源池（精簡、快照）
外部同位元檢查群組	儲存資源池（後端）、磁碟群組
連接埠	儲存節點→控制器節點→連接埠
主機群組	Volume對應與遮罩
Volume配對	儲存同步

附註：這些只是通用的術語對應、可能不代表此資料收集器的每個案例。

庫存需求

您必須具備下列條件才能收集庫存資料：

- 裝載「Common Services」元件之Ops Center伺服器的IP位址或主機名稱
- 裝載Ops Center元件的所有伺服器上都有root / Sysadmin使用者帳戶和密碼。HDS在Ops Center 10.8+之前、並未針對LDAP/SSO使用者實作REST API支援

效能要求

若要收集效能資料、必須符合下列要求：

- 必須安裝 HDS Ops Center 「 Analyzer 」模組
- 儲存陣列必須提供 Ops Center 「分析器」模組

組態

欄位	說明
Hitachi Ops Center IP位址	裝載「Common Services」元件之Ops Center伺服器的IP位址或完整網域名稱
使用者名稱	Ops Center伺服器的使用者名稱。
密碼	Ops Center伺服器使用的密碼。

進階組態

欄位	說明
連線類型	預設為HTTPS（連接埠443）
置換TCP連接埠	如果不是預設、請指定要使用的連接埠
庫存輪詢時間間隔（分鐘）	庫存輪詢之間的時間間隔。預設值為40。
選擇「排除」或「包含」以指定清單	指定在收集資料時是否要納入或排除下列陣列清單。
篩選裝置清單	要包含或排除的裝置序號以逗號分隔的清單
效能意見調查時間間隔（秒）	效能輪詢之間的時間間隔。預設值為300。

HDS儲存設備

適用於HDS儲存資產登陸頁面上可能找到的物件或參考的詞彙。

HDS儲存術語

下列詞彙適用於HDS儲存資產登陸頁面上可能找到的物件或參考資料。其中許多術語也適用於其他資料收集器。

- 名稱：直接來自HDS HndhvDevice Manager的「名稱」屬性、透過GetStorageArray XML API呼叫
- 機型：直接來自HDS HndyDevice Manager的「arrayType」屬性、透過GetStorageArray XML API呼叫
- 廠商：HDS
- 系列產品：直接來自HDS HndyDevice Manager的「arrayFamily」屬性、透過GetStorageArray XML API呼叫
- IP—這是陣列的管理IP位址、並非陣列上所有IP位址的詳盡清單
- 原始容量：代表此系統中所有磁碟總容量之和的BASE2值、無論磁碟角色為何。

HDS儲存資源池

適用於HDS儲存資源池資產登陸頁面上可能找到的物件或參考的詞彙。

HDS儲存資源池術語

下列詞彙適用於HDS儲存資源池資產登陸頁面上可能找到的物件或參考資料。其中許多術語也適用於其他資料收集器。

- 類型：此處的值為：
  - 保留-如果此資源池專用於資料磁碟區以外的用途、例如、日誌記錄、快照
  - 精簡配置（如果這是HDP池）
  - RAID Group（RAID群組）-您可能不會因為下列幾個原因而看到這些資訊：

    保監處採取堅定的立場、避免在任何成本下重複計算容量。在HDS上、通常需要從磁碟建立RAID群組、在這些RAID群組上建立集區磁碟區、以及從這些集區磁碟區建構集區（通常是HDP、但可能是特殊用途）。如果OCI同時報告基礎RAID群組和集區、則其原始容量總和將會大幅超過磁碟總和。

  相反地、OCI的HDS HDS-Data Collector會根據集區磁碟區的容量、任意縮減RAID群組的大小。這可能導致OCI完全不報告RAID群組。此外、任何產生的RAID群組都會以旗標方式標示、使其在OCI WebUI中不可見、但它們確實會流入OCI資料倉儲（DWH）。這些決策的目的是為了避免大部分使用者不關心的問題、因為如果HDS陣列有可用容量為50MB的RAID群組、您可能無法使用該可用空間來獲得任何有意義的結果。

- 節點-不適用、因為HDS集區不會繫結至任何一個特定節點
- 備援：集區的RAID層級。可能是由多種RAID類型所組成的HDP集區有多個值
- 容量%：集區用於資料使用量的百分比、以及已使用的GB和集區的總邏輯GB大小
- 過度委派容量：一種衍生值、表示「此資源池的邏輯容量因邏輯磁碟區總和超過此百分比之資源池邏輯容量而超額訂閱」
- Snapshot：顯示此資源池中保留用於快照使用的容量

HDS儲存節點

適用於HDS儲存節點資產登陸頁面上可能找到的物件或參考的術語。

HDS儲存節點術語

下列術語適用於HDS儲存節點資產登陸頁面上可能找到的物件或參考資料。其中許多術語也適用於其他資料收集器。

- 名稱：單片陣列上的前端導向器（FED）或通道介面卡名稱、或模組化陣列上的控制器名稱。給定的HDS陣列將有2個以上的儲存節點
- Volume（磁碟區）- Volume（磁碟區）表格會顯示對應至此儲存節點所擁有之任何連接埠的任何磁碟區

Hitachi Ops Center資料收集器

此資料收集器使用Hitachi Ops Center的整合式應用程式套件來存取多個儲存設備的庫存和效能資料。針對庫存和容量探索、您的Ops Center安裝必須同時包含「Common Services」（通用服務）和「Administrator」（管理員）元件。為了收集效能、您還必須部署「分析器」。

術語

OnCommand Insight 會從此資料收集器取得下列庫存資訊。對於所取得的每種資產類型、都會顯示此資產最常用的術語。檢視或疑難排解此資料收集器時、請謹記下列術語：

廠商/模型術語	詞彙**OnCommand Insight**
儲存系統	儲存設備
Volume	Volume
同位元檢查群組	儲存資源池（RAID）、磁碟群組
磁碟	磁碟
儲存資源池	儲存資源池（精簡、快照）
外部同位元檢查群組	儲存資源池（後端）、磁碟群組
連接埠	儲存節點→控制器節點→連接埠
主機群組	Volume對應與遮罩
Volume配對	儲存同步

附註：這些只是通用的術語對應、可能不代表此資料收集器的每個案例。

庫存需求

您必須具備下列條件才能收集庫存資料：

- 裝載「Common Services」元件之Ops Center伺服器的IP位址或主機名稱
- 裝載Ops Center元件的所有伺服器上都有root / Sysadmin使用者帳戶和密碼。HDS在Ops Center 10.8+之前、並未針對LDAP/SSO使用者實作REST API支援

效能要求

若要收集效能資料、必須符合下列要求：

- 必須安裝 HDS Ops Center 「 Analyzer 」模組
- 儲存陣列必須提供 Ops Center 「分析器」模組

組態

欄位	說明
Hitachi Ops Center IP位址	裝載「Common Services」元件之Ops Center伺服器的IP位址或完整網域名稱
使用者名稱	Ops Center伺服器的使用者名稱。
密碼	Ops Center伺服器使用的密碼。

進階組態

欄位	說明
連線類型	預設為HTTPS（連接埠443）
置換TCP連接埠	如果不是預設、請指定要使用的連接埠
庫存輪詢時間間隔（分鐘）	庫存輪詢之間的時間間隔。預設值為40。

選擇「排除」或「包含」以指定清單	指定在收集資料時是否要納入或排除下列陣列清單。
篩選裝置清單	要包含或排除的裝置序號以逗號分隔的清單
效能意見調查時間間隔（秒）	效能輪詢之間的時間間隔。預設值為300。

HDS NAS（HNAS）資料來源

HDS NAS（HNAS）資料來源是一種庫存和組態資料來源、可支援探索HDS NAS叢集。Insight支援探索NFS和CIFS共用、檔案系統（Insight內部Volume）和跨區（Insight Storage Pools）。

此資料來源為SSH型、因此裝載此資料的擷取單元必須能夠啟動SSH工作階段、以連線至HNAS本身或叢集所連線之系統管理單元（SMU）上的TCP 22。

術語

從HNAS資料來源取得下列庫存資訊OnCommand Insight 。對於Insight取得的每種資產類型、都會顯示此資產最常用的術語。檢視或疑難排解此資料來源時、請謹記下列術語：

廠商/模型術語	Insight術語
層級	磁碟群組
叢集	儲存設備
節點	儲存節點
跨距	儲存資源池
檔案系統	內部Volume

這些只是通用的術語對應、可能不代表此資料來源的每個案例。

需求

以下是設定及使用此資料來源的需求：

- 裝置IP位址
- 連接埠22、SSH傳輸協定
- 使用者名稱與密碼-權限層級：supervisor
- 附註：此資料收集器以SSH為基礎、因此主機必須能夠在HNAS本身或叢集所連接的系統管理單元（SMU）上、對TCP 22啟動SSH工作階段。

此資料收集器是以SSH為基礎、因此裝載它的AU必須能夠在HNAS本身或叢集所連線的系統管理單元（SMU）上、對TCP 22啟動SSH工作階段。

組態

欄位	說明
HNAS主機	HNAS管理主機的IP位址或完整網域名稱
使用者名稱	HNAS CLI的使用者名稱
密碼	HNAS CLI使用的密碼

進階組態

欄位	說明
庫存輪詢時間間隔（分鐘）	庫存輪詢之間的時間間隔（預設為30分鐘）
SSH橫幅等待逾時（秒）	SSH橫幅等待逾時（預設15秒）
SSH命令逾時（秒）	SSH命令逾時（預設30秒）

HP CommandView AE資料來源

HP CommandView Advanced Edition（AE）和CommandView AE CLI/SMI（AE精簡版）資料來源可從CommandView（又稱為「1TB」）Device Manager伺服器支援庫存和效能。

術語

從HP CommandView AE和AE精簡版資料來源取得下列庫存資訊OnCommand Insight 。對於Insight取得的每種資產類型、都會顯示此資產最常用的術語。檢視或疑難排解此資料來源時、請謹記下列術語：

廠商/模型術語	Insight術語
PDEV	磁碟
日誌集區	磁碟群組
儲存陣列	儲存設備
連接埠控制器	儲存節點
Array Group、DP Pool	儲存資源池
邏輯單元、LDEV	Volume

這些只是通用的術語對應、可能不代表此資料來源的每個案例。

庫存需求

- Hndvice Manager伺服器的IP位址
- CommandView AE軟體和對等權限的唯讀使用者名稱和密碼
- 設備管理程式的CommandView AE精簡版只有CLI授權
- 連接埠需求：2001年

效能要求

- HDS USP、USP V和VSP效能
  - 效能監視器必須獲得授權。
  - 必須啟用監控交換器。
  - 匯出工具 (`Export.exe`）必須複製到OnCommand Insight The樣部伺服器。
  - 匯出工具版本必須符合目標陣列的微碼版本。
- HDS AMS效能
  - 效能監視器必須獲得授權。
  - 儲存導覽器模組2（SNM2）CLI公用程式需要安裝在OnCommand Insight SView Server上。
  - 您必須使用OnCommand Insight 下列命令、登錄所有需要由VMware取得效能的AMS、wms、SMS儲存陣列：
  - 您必須確保您註冊的所有陣列都列在此命令的輸出中： `auunitref.exe`。

組態

欄位	說明
和服務器	Hndvice Manager伺服器的IP位址或完整網域名稱
使用者名稱	使用者名稱。
密碼	用於HiCommand Device Manager伺服器的密碼。
裝置：USP、USP V、VSP/R600儲存	VSP G1000（R800）、VSP（R700）、Hus VM（HM700）和USP儲存設備清單。每個儲存設備都需要： • 陣列的IP：儲存設備的IP位址 • 使用者名稱：儲存設備的使用者名稱 • 密碼：儲存設備的密碼 • 包含匯出公用程式Jar檔案的資料夾：包含匯出公用程式的資料夾 `.jar` 檔案

SNM2Device - WMS/SMS/AMS儲存	WMS/SMS/AMS儲存設備清單。每個儲存設備都需要： • 陣列的IP：儲存設備的IP位址 • Storage Navigator CLI路徑：SNM2 CLI路徑 • 帳戶驗證有效：選取以選擇有效的帳戶驗證 • 使用者名稱：儲存設備的使用者名稱 • 密碼：儲存設備的密碼
選擇「效能調校管理程式」	選擇「調校管理程式」以獲得效能、並覆寫其他效能選項
調校管理程式主機	調整管理程式的IP位址或完整網域名稱
調校管理器連接埠	用於調整管理程式的連接埠
調校管理程式使用者名稱	調整管理程式的使用者名稱
調校管理員密碼	調整管理程式的密碼

在HDS USP、USP V和VSP中、任何磁碟都可以屬於多個陣列群組。

進階組態

欄位	說明
Hndl伺服器連接埠	用於「HiCommand Device Manager」的連接埠
HTTPS已啟用	選取以啟用HTTPS
庫存輪詢時間間隔（分鐘）	庫存輪詢之間的時間間隔（預設為40分鐘）
選擇「排除」或「包含」以指定清單	指定在收集資料時是否要納入或排除下列陣列清單
排除或包含裝置	要包含或排除的裝置ID或陣列名稱清單、以逗號分隔
查詢主機管理程式	選取以查詢主機管理程式
HTTP逾時（秒）	HTTP連線逾時（預設為60秒）
效能輪詢時間間隔（秒）	效能輪詢之間的時間間隔（預設為300秒）

匯出逾時（以秒為單位）	匯出公用程式逾時（預設為300秒）

HP EVA儲存資料來源

對於組態設定、Eva Storage（SSSU）資料來源需要Command View（CV）伺服器的IP位址、以及CV軟體的_read-only（唯讀）使用者名稱和密碼。使用者必須在CV軟體中定義。

術語

從HP EVA資料來源取得下列庫存資訊OnCommand Insight 。對於Insight取得的每種資產類型、都會顯示此資產最常用的術語。檢視或疑難排解此資料來源時、請謹記下列術語：

廠商/模型術語	Insight術語
磁碟	磁碟
磁碟群組	磁碟群組（未建模）
儲存單元	儲存設備
虛擬磁碟	儲存資源池
虛擬磁碟	Volume

這些只是通用的術語對應、可能不代表此資料來源的每個案例。

庫存需求

- CV伺服器的IP位址
- CV軟體的唯讀使用者名稱和密碼。使用者必須在CV軟體中定義。
- 安裝在OnCommand Insight 《The》伺服器/ Rau上的第三方軟體： `sssu.exe`。。 `sssu.exe` 版本應對應於CV版本。
- 存取驗證：執行 `sssu.exe` 使用使用者名稱和密碼的命令。

效能要求

HP Storageworks Command View Eva軟體套件必須安裝在OnCommand Insight 該伺服器上。或者、您也可以在Eva伺服器上安裝遠端擷取裝置（Rau）：

1. 將HP Storageworks Command View Eva Software Suite安裝在OnCommand Insight The RisfServer上、或在Command View Eva伺服器上安裝遠端擷取裝置。
2. 找到 `evaperf.exe` 命令。例如、 `c:\Program Files\Hewlett-Packard\EVA Performance Monitor\`
3. 使用Command View伺服器的IP執行下列步驟：

a. 在預設連接埠為860的情況下執行此命令 `Evaperf.exe server <Command View Server IP\> 860 <username\>`

b. 在密碼提示字元中輸入Command View伺服器密碼。

   這應該會傳回命令列提示字元、而不會傳回其他項目。

4. 執行以驗證設定 `evaperf.exe ls`。

   您應該會看到由Command View伺服器管理的陣列或控制器清單。每一行都會顯示一個在一個Eva陣列上的控制器。

組態

欄位	說明
CommandView伺服器	Eva Storage Manager的IP位址或完整網域名稱
使用者名稱	Command View Manager的使用者名稱。名稱必須在Command View中定義。
密碼	用於Command View Manager的密碼。
效能使用者名稱	為了達到效能、命令檢視管理程式的使用者名稱。名稱必須在Command View中定義。
效能密碼	為了達到效能、命令檢視管理程式所使用的密碼。

進階組態

欄位	說明
庫存輪詢時間間隔（分鐘）	庫存輪詢之間的時間間隔（預設為40分鐘）
CLI首頁	CLI主目錄的完整路徑名稱（其中） `sssu.exe` 所在位置
庫存排除裝置	以逗號分隔的裝置名稱清單
效能意見調查時間間隔（秒）	效能輪詢之間的時間間隔（預設為300秒）
高效能CLI首頁	對於Array Performance（陣列效能）、請完整路徑名稱至sssu.exe所在的CLI主目錄。若要驗證存取、請執行 `sssu.exe`
命令逾時（秒）	`evaperf` 命令等待逾時（預設為600秒）

效能排除裝置	要從收集效能資料中排除的裝置名稱清單、以逗號分隔

HPE Nimble資料來源

HPE Nimble資料收集器支援HPE Nimble儲存陣列的庫存與效能資料。

術語

從HPE Nimble資料來源取得下列庫存資訊OnCommand Insight 。對於Insight取得的每種資產類型、都會顯示此資產最常用的術語。檢視或疑難排解此資料來源時、請謹記下列術語：

廠商/模型術語	Insight術語
陣列	儲存設備
磁碟	磁碟
資源池	儲存資源池
Volume	Volume
啟動器	儲存主機別名
控制器	儲存節點
Fibre Channel介面	控制器

這些只是通用的術語對應、可能不代表此資料來源的每個案例。

需求

- 陣列必須經過安裝和設定、並可從用戶端透過完整網域名稱（FQDN）或陣列管理IP位址進行存取。
- 陣列必須執行NimibleOS 2.3.x或更新版本。
- 您必須擁有陣列的有效使用者名稱和密碼。
- 陣列上的連接埠5392必須開啟。

組態

欄位	說明
陣列管理IP位址	完整網域名稱（FQDN）或陣列管理IP位址。
使用者名稱	Nimble陣列的使用者名稱

密碼	Nimble陣列的密碼

進階組態

欄位	說明
連接埠	Nimble REST API所使用的連接埠。預設值為5392。
庫存輪詢時間間隔（分鐘）	庫存輪詢之間的時間間隔（預設為60分鐘）

附註：預設的效能輪詢時間間隔為300秒、無法變更。這是Nimble唯一支援的時間間隔。

Huawei海洋儲存資料來源

本產品使用Huawei OceanStor（REST / HTTPS）資料來源來探索Huawei OceanStor儲存設備的庫存OnCommand Insight 。

術語

他向Huawei海洋儲存公司取得下列庫存與效能資訊OnCommand Insight 。針對由S仰賴 的每種資產類型OnCommand Insight 、會顯示此資產最常用的術語。檢視或疑難排解此資料收集器時、請謹記下列術語：

廠商/模型術語	詞彙OnCommand Insight
儲存資源池	儲存資源池
檔案系統	內部Volume
控制器	儲存節點
FC連接埠（對應）	Volume Map
主機FC啟動器（已對應）	Volume遮罩
NFS/CIFS共用	分享
分享	iSCSI目標節點
iSCSI連結啟動器	iSCSI啟動器節點
磁碟	磁碟
LUN	Volume

需求

以下是設定及使用此資料收集器的需求：

- 裝置IP
- 存取海洋儲存設備管理程式的認證資料
- 連接埠8088必須可用

組態

欄位	說明
海洋儲存主機IP位址	海洋儲存裝置管理員的IP位址或完整網域名稱
使用者名稱	用於登入海洋儲存裝置管理員的名稱
密碼	用於登入海洋儲存裝置管理員的密碼

進階組態

欄位	說明
TCP連接埠	TCP連接埠用於連線到海洋儲存裝置管理員（預設值8088）
庫存輪詢時間間隔（分鐘）	庫存輪詢之間的時間間隔（預設為60分鐘）
連線逾時（秒）	連線逾時（預設為60秒）

IBM Cleverafe資料來源

此資料來源會收集IBM Cleverafe的庫存和效能資料。

需求

以下是設定此資料來源的需求：

- Manager IP位址或主機名稱
- 相同的使用者名稱和密碼
- 連接埠9440

組態

欄位	說明
Cleversafe管理程式主機名稱或IP位址	CleverSafe裝置的主機IP位址

使用者名稱	用於登入Cleverafe的名稱
密碼	用於登入Cleverafe的密碼

進階組態

欄位	說明
庫存輪詢時間間隔（分鐘）	預設為60分鐘
HTTP連線逾時）	預設值為60秒

IBM DS資料來源

IBM DS（CLI）資料來源僅支援DS6xxx和DS8xxx裝置。NetApp E系列資料來源支援DS3xxx、DS4xxx和DS5xxx裝置。如需支援的機型和韌體版本、請參閱Insight資料來源支援對照表。

術語

從IBM DS資料來源取得下列庫存資訊OnCommand Insight 。對於Insight取得的每種資產類型、都會顯示此資產最常用的術語。檢視或疑難排解此資料來源時、請謹記下列術語：

廠商/模型術語	Insight術語
磁碟機模組	磁碟
儲存映像	儲存設備
範圍集區	儲存資源池
固定區塊Volume	Volume

這些只是通用的術語對應、可能不代表此資料來源的每個案例。

需求

- 每個DS陣列的IP位址
- 儲存設備顯示名稱為選用項目、僅供外觀使用
- 每個DS陣列上的唯讀使用者名稱和密碼
- 安裝在Insight伺服器上的協力廠商軟體：IBM dscli
- 存取驗證：執行 `dscli` 使用使用者名稱和密碼的命令
- 連接埠需求：80、443和750

組態

欄位	說明
DS儲存設備	DS儲存主機的IP位址或完整網域名稱
使用者名稱	用於DS CLI的名稱
密碼	用於DS CLI的密碼
執行檔dscli.exe路徑	的完整路徑 `dscli.exe`公用程式：

進階組態

欄位	說明
庫存輪詢時間間隔（分鐘）	庫存輪詢之間的時間間隔（預設為40分鐘）
儲存設備顯示名稱	IBM DS儲存陣列名稱
庫存排除裝置	要從庫存集合中排除的裝置序號清單、以逗號分隔
效能意見調查時間間隔（秒）	效能輪詢之間的時間間隔（預設為300秒）
效能篩選器類型	包括：僅從清單上的裝置收集資料。排除：不會從這些裝置收集資料
效能篩選器裝置清單	要納入或排除在效能集合之外的裝置ID清單、以逗號分隔

IBM PowerVM資料來源

IBM PowerVM（SSH）資料來源會收集在由硬體管理主控台（HMC）管理的IBM Power硬體執行個體上執行的虛擬分割區相關資訊。對於組態、此資料來源需要使用者名稱才能透過SSH登入HMC、以及HMC組態的檢視層級權限。

術語

從IBM PowerVM資料來源取得下列庫存資訊OnCommand Insight 。對於Insight取得的每種資產類型、都會顯示此資產最常用的術語。檢視或疑難排解此資料來源時、請謹記下列術語：

廠商/模型術語	Insight術語
hdisk	虛擬磁碟
託管系統	主機

LPAR、VIO伺服器	虛擬機器
Volume群組	資料儲存區
實體Volume	LUN

這些只是通用的術語對應、可能不代表此資料來源的每個案例。

需求

- 硬體管理主控台（HMC）的IP位址
- 使用者名稱和密碼、可透過SSH存取HMC
- 連接埠需求SSH-22
- 檢視所有管理系統和邏輯分割安全性網域的權限

  使用者也必須擁有HMC組態的「檢視」權限、以及收集HMC主控台安全性群組的VPD資訊的能力。使用者也必須能夠在「邏輯分割區」安全性群組下存取「虛擬IO伺服器命令」。最佳做法是從操作員角色開始、然後移除所有角色。HMC上的唯讀使用者沒有在AIX主機上執行代理命令的權限。

- IBM最佳實務做法是由兩個以上的HMC監控裝置。請注意、這可能會導致OnCommand Insight 無法回報重複的裝置、因此強烈建議您將備援裝置新增至此資料收集器的「進階組態」中的「排除裝置」清單。

組態

欄位	說明
硬體管理主控台（HMC）位址	PowerVM硬體管理主控台的IP位址或完整網域名稱
HMC使用者	硬體管理主控台的使用者名稱
密碼	硬體管理主控台使用的密碼

進階組態

欄位	說明
庫存輪詢時間間隔（分鐘）	庫存輪詢之間的時間間隔（預設為20分鐘）
SSH連接埠	用於SSH至PowerVM的連接埠
SSH程序等待逾時（秒）	SSH程序逾時（預設為600秒）
重試次數	嘗試進行庫存重試的次數

排除裝置	以逗號分隔的裝置ID清單或要排除的顯示名稱

IBM SVC資料來源

IBM SVC資料來源會使用SSH收集庫存與效能資料、以支援執行SVC作業系統的各種裝置。支援的裝置清單包括SVC、v7000、v5000和v3700等機型。如需支援的機型和韌體版本、請參閱Insight資料來源支援對照表。

術語

從IBM SVC資料來源取得下列庫存資訊OnCommand Insight 。對於Insight取得的每種資產類型、都會顯示此資產最常用的術語。檢視或疑難排解此資料來源時、請謹記下列術語：

廠商/模型術語	Insight術語
磁碟機	磁碟
叢集	儲存設備
節點	儲存節點
Mdisk群組	儲存資源池
vDisk	Volume
磁碟	後端LUN

這些只是通用的術語對應、可能不代表此資料來源的每個案例。

庫存需求

- 每個SVC叢集的IP位址
- 連接埠22可用
- 您可以透過Insight產生的公開和私密金鑰組、或是重複使用已在SVC上使用的金鑰組

  如果您要重複使用現有的金鑰組、則必須將其從Putty格式轉換為OpenSSH格式。

- 安裝在SVC叢集上的公開金鑰
- 需要在資料來源中識別私密金鑰
- 存取驗證：開啟 `ssh` 使用私密金鑰與SVC叢集之間的工作階段

無需安裝協力廠商軟體。

效能要求

- SVC主控台、適用於任何SVC叢集、且適用於SVC探索基礎套件。
- 只有將效能資料檔案從叢集節點複製到組態節點時、才需要管理存取層級。

> 由於SVC基礎探索套件不需要此存取層級、因此SVC基礎使用者可能無法成功運作。

- 需要連接埠22
- 必須為此使用者產生私有和公有SSH金鑰、並儲存私密金鑰、以便從擷取單位存取。如果SVC基礎使用者擁有適當的權限、則相同的使用者和金鑰也能正常運作。相同的SSH金鑰可用於庫存和效能資料。
- 透過SSH連線至SVC叢集並執行下列作業、以啟用資料收集： `svctask startstats -interval 1`

> 或者、也可以使用SVC管理使用者介面來啟用資料收集。

父序號說明

傳統上Insight能夠報告儲存陣列序號或個別儲存節點序號。不過、有些儲存陣列架構並未完全符合此要求。SVC叢集可由1-4個應用裝置組成、每個應用裝置有2個節點。如果應用裝置本身有序號、則該序號既不是叢集的序號、也不是節點的序號。

儲存節點物件上的「父序號」屬性、會在個別節點位於僅屬於大型叢集一部分的中繼應用裝置/機箱內時、適當地填入IBM SVC陣列。

組態

欄位	說明
叢集IP	SVC儲存設備完整網域名稱的IP位址
選擇「密碼」或「OpenSSH金鑰檔」以指定認證類型	用於透過SSH連線至裝置的認證類型
庫存使用者名稱	SVC CLI的使用者名稱
庫存密碼	SVC CLI的密碼
完整的庫存私密金鑰路徑	Inventory Private Key檔案的完整路徑
效能使用者名稱	用於收集效能的SVC CLI使用者名稱
效能密碼	用於收集效能的SVC CLI密碼
效能私密金鑰的完整路徑	效能私密金鑰檔案的完整路徑

進階組態

欄位	說明
庫存輪詢時間間隔（分鐘）	庫存輪詢之間的時間間隔（預設為40分鐘）
排除裝置	要從庫存集合中排除的裝置ID清單、以逗號分隔
SSH程序等待逾時（秒）	SSH程序逾時（預設值為200秒）
效能意見調查時間間隔（秒）	效能輪詢之間的時間間隔（預設為300秒）
效能排除裝置	要從效能集合中排除的裝置ID清單、以逗號分隔
效能SSH程序等待逾時（秒）	SSH程序逾時（預設值為200秒）
清除傾印的統計資料檔案	選取以清除傾印的統計資料檔案

IBM Tivoli監控資料來源

此資料來源僅用於檔案系統使用率。它直接與Tivoli監控資料庫通訊、也稱為Tivoli監控資料倉儲。支援Oracle和DB2資料庫。

Oracle錯誤訊息

此資料收集器已不再提供OnCommand Insight 、從版本號為e.7.3.11開始。

如果指定的SID導致嘗試連線時出現錯誤訊息「ORA-121554」、請仔細檢查Oracle DB網路服務組態。如果存取組態指定完整的主機名稱（例如「names.default_domain」）、請嘗試在SID欄位中插入完整的服務名稱。一個簡單的例子就是連線到SID `testdb` 失敗、且Oracle組態指定的網域`company.com`。您可以使用下列字串來取代基礎SID來嘗試連線： `testdb.company.com`。

組態

欄位	說明
Tivoli監控資料庫IP	Tivoli監控伺服器的IP位址或完整網域名稱
使用者名稱	Tivoli監控伺服器的使用者名稱
密碼	Tivoli監控伺服器的密碼

進階組態

欄位	說明
Tivoli監控資料庫連接埠	用於Tivoli監控資料庫的連接埠

Oracle SID或DB2資料庫名稱	Oracle接聽程式服務ID或DB2資料庫名稱
庫存輪詢時間間隔（分鐘）	庫存輪詢之間的時間間隔（預設為60分鐘）
要使用的資料庫驅動程式	選擇要使用的資料庫驅動程式
用於連線至資料庫的傳輸協定	用於連線至資料庫的傳輸協定
資料庫架構	輸入資料庫架構

IBM TotalStorage DS4000資料來源

此資料來源會收集庫存和效能資訊。有兩種可能的組態（韌體6.x和7.x+）、兩者都有相同的值。API會收集Volume資料統計資料。

組態

欄位	說明
以逗號分隔的陣列SANtricity 資訊控制器IP清單	控制器的IP位址或完整網域名稱、以逗號分隔

需求

- 每個DS5或FAStT陣列的IP位址
- 存取驗證：Ping每個陣列上兩個控制器的IP位址。

進階組態

欄位	說明
庫存輪詢時間間隔（分鐘）	庫存輪詢之間的時間間隔（預設為30分鐘）
效能意見調查時間間隔（最多3、600秒）	效能輪詢之間的時間間隔（預設為300秒）

IBM XIV資料來源

IBM XIV（CLI）資料來源詳細目錄是使用XIV命令列介面來執行。XIV效能是透過撥打SMI-S呼叫XIV陣列來達成、XIV陣列在連接埠5989上執行SMI-S供應商。

術語

從IBM XIV資料來源取得下列庫存資訊OnCommand Insight 。對於Insight取得的每種資產類型、都會顯示此資產最常用的術語。檢視或疑難排解此資料來源時、請謹記下列術語：

廠商/模型術語	Insight術語

磁碟	磁碟
儲存系統	儲存設備
儲存資源池	儲存資源池
Volume	Volume

這些只是通用的術語對應、可能不代表此資料來源的每個案例。

需求

- 連接埠需求：TCP連接埠7778
- XIV管理介面的IP位址
- 唯讀使用者名稱和密碼
- XIV CLI必須安裝在Insight伺服器或Rau上
- 存取驗證：使用使用者名稱和密碼、從Insight伺服器登入XIV使用者介面。

組態

欄位	說明
IP位址	XIV儲存設備的IP位址或完整網域名稱
使用者名稱	XIV儲存設備的使用者名稱
密碼	XIV儲存設備的密碼
XIV CLI目錄的完整路徑	XIV CLI目錄的完整路徑

進階組態

欄位	說明
庫存輪詢時間間隔（分鐘）	庫存輪詢之間的時間間隔（預設為40分鐘）
CLI程序等待逾時（毫秒）	CLI處理逾時（預設值為7200000 ms）
SMI-S主機IP	SMI-S Provider主機的IP位址
SMI-S連接埠	SMI-S Provider Host使用的連接埠

SMI-S傳輸協定	用於連線至SMI-S供應商的傳輸協定
SMI-S命名空間	SMI-S命名空間
使用者名稱	SMI-S Provider主機的使用者名稱
密碼	SMI-S Provider主機的密碼
效能意見調查時間間隔（秒）	效能輪詢之間的時間間隔（預設為300秒）
SMI-S連線重試次數	SMI-S連線重試次數

Infinidat InfinidBox資料來源

Infinidat Infinbox（HTTP）資料來源是用來收集Infinidat Infinidat InfinBox儲存設備的資訊。您必須能夠存取InfinBox管理節點。

術語

從Infininbox資料來源取得下列庫存資訊OnCommand Insight 。對於Insight取得的每種資產類型、都會顯示此資產最常用的術語。檢視或疑難排解此資料來源時、請謹記下列術語：

廠商/模型術語	Insight術語
磁碟機	磁碟
InfinabBox	儲存設備
節點	儲存節點
資源池	儲存資源池
Volume	Volume
FC連接埠	連接埠
檔案系統	內部Volume
檔案系統	檔案共享
檔案系統匯出	分享

這些只是通用的術語對應、可能不代表此資料來源的每個案例。

組態

欄位	說明
InfinBox主機	InfindBox管理節點的IP位址或完整網域名稱
使用者名稱	使用者名稱
密碼	InfindBox管理節點的密碼

進階組態

欄位	說明
TCP連接埠	TCP連接埠用於連線至InfinabBox伺服器（預設443）
庫存輪詢時間間隔（分鐘）	庫存輪詢之間的時間間隔（預設為60分鐘）
連線逾時	連線逾時（預設為60秒）

Microsoft Azure運算資料來源

Insights使用Azure運算資料收集器從Azure運算執行個體取得庫存和效能資料OnCommand。

需求

您需要下列資訊來設定此資料收集器：

- 連接埠需求：443 HTTPS
- Azure管理REST IP（management.azure.com）
- Azure服務主要應用程式（用戶端）ID（使用者帳戶）
- Azure服務主要驗證金鑰（使用者密碼）

您必須設定Azure帳戶才能進行Insight探索。一旦帳戶設定正確、且您已在Azure中註冊應用程式、您將擁有使用Insight探索Azure執行個體所需的認證資料。下列連結說明如何設定帳戶以進行探索：https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal

組態

根據下表、將資料輸入資料來源欄位：

欄位	說明
Azure服務主要應用程式（用戶端）ID（需具備讀取器角色）	Azure的登入ID。需要讀取器角色存取權。

Azure租戶ID	Microsoft租戶ID
Azure服務主要驗證金鑰	登入驗證金鑰
我瞭解Microsoft向我索取API要求	請勾選此選項、確認您瞭解Microsoft會針對Insight Polling所提出的API要求向您提出帳單。

進階組態

根據下表、將資料輸入資料來源欄位：

欄位	說明
庫存輪詢時間間隔（分鐘）	預設值為60
選擇「排除」或「包含」以套用至依標記篩選虛擬機器	指定在收集資料時、是否要加入或排除VM的by Tags。如果選取「include'」、則「標記金鑰」欄位不可為空白。
標記要篩選虛擬機器的金鑰和值	按一下「**+ Filter Tag**（**+**篩選標籤）」、選擇要納入/排除的VM（及相關磁碟）、方法是篩選符合VM上標籤的機碼和值。標記金鑰為必填、標記值為選用項目。當標記值為空白時、只要VM符合標記金鑰、就會進行篩選。
效能意見調查時間間隔（秒）	

資料來源**Azure NetApp Files**

此資料來源會擷取庫存和效能資料以供Azure NetApp Files 使用（ANF）。

需求

以下是設定此資料來源的需求：

- 連接埠需求：443 HTTPS
- Azure管理REST IP（management.azure.com）
- Azure服務主要應用程式（用戶端）ID（使用者帳戶）
- Azure服務主要驗證金鑰（使用者密碼）
- 您必須設定Azure帳戶Cloud Insights 才能進行不必要的探索。

  一旦帳戶設定正確、並在Azure中註冊應用程式、您就會擁有必要的認證資料、以便使用Cloud Insights 下列功能探索Azure執行個體。下列連結說明如何設定帳戶以進行探索：

  https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal

組態

欄位	說明
Azure服務主要應用程式（用戶端）ID	Azure的登入ID
Azure租戶ID	Azure租戶ID
Azure服務主要驗證金鑰	登入驗證金鑰
我瞭解Microsoft向我索取API要求	請勾選此選項、確認您瞭解Microsoft會針對Insight Polling所提出的API要求向您提出帳單。

進階組態

欄位	說明
庫存輪詢時間間隔（分鐘）	預設為60分鐘

Microsoft Hyper-V資料來源

在組態方面、Microsoft Hyper-V資料來源需要實體主機（Hypervisor）的IP位址或可解析的DNS名稱。此資料來源使用PowerShell（先前使用的WMITM）。

術語

從Hyper-V資料來源取得下列庫存資訊OnCommand Insight 。對於Insight取得的每種資產類型、都會顯示此資產最常用的術語。檢視或疑難排解此資料來源時、請謹記下列術語：

廠商/模型術語	Insight術語
虛擬硬碟	虛擬磁碟
主機	主機
虛擬機器	虛擬機器
叢集共用磁碟區（CSV）、分割磁碟區	資料儲存區
網際網路SCSI裝置、多重路徑SCSI LUN	LUN
Fibre Channel連接埠	連接埠

這些只是通用的術語對應、可能不代表此資料來源的每個案例。

需求

- Hyper-V需要開啟連接埠5985才能進行資料收集和遠端存取/管理。
- 叢集群組節點的IP位址
- Hypervisor上的本機管理員使用者與密碼
- 系統管理層級的使用者帳戶
- 連接埠需求：連接埠135和動態TCP連接埠、分別為Windows 2003和舊版指派1024-65535和Windows 2008指派49152-65535。
- 即使資料收集器只指向IP位址、DNS解析也必須成功。
- 每個Hyper-V Hypervisor必須為每個VM、每個主機上的每個VM開啟「資源計量」。如此一來、每Cloud Insights 個Hypervisor都能在每個來賓作業系統上提供更多資料以供其使用。如果未設定、則會為每個來賓取得較少的效能指標。如需資源計量的詳細資訊、請參閱Microsoft文件：

  "Hyper-V資源計量概觀"

  "啟用VMResource記數"

組態

欄位	說明
實體主機IP位址	實體主機（Hypervisor）的IP位址或完整網域名稱
使用者名稱	系統管理員使用者名稱是Hypervisor的名稱
密碼	Hypervisor密碼
NT網域	叢集中節點使用的DNS名稱

進階組態

欄位	說明
庫存輪詢時間間隔（分鐘）	庫存輪詢之間的時間間隔（預設為20分鐘）
連線逾時（毫秒）	連線逾時（預設為60000毫秒）

NetApp叢集Data ONTAP 式功能資料來源

此資料來源應用於使用叢集Data ONTAP 式功能的儲存系統、且需要使用系統管理員帳戶進行唯讀API呼叫。

術語

從叢集式的「叢集式功能」資料來源取得下列庫存資訊Data ONTAP OnCommand Insight 。對於Insight取得的

每種資產類型、都會顯示此資產最常用的術語。檢視或疑難排解此資料來源時、請謹記下列術語：

廠商/模型術語	Insight術語
磁碟	磁碟
RAID群組	磁碟群組
叢集	儲存設備
節點	儲存節點
Aggregate	儲存資源池
LUN	Volume
Volume	內部Volume

這些只是通用的術語對應、可能不代表此資料來源的每個案例。

需求

- 用於唯讀API呼叫的系統管理員帳戶
- 目標IP是叢集管理LIF
- 用於登入NetApp叢集的使用者名稱（使用預設Vserver的ontapi應用程式唯讀角色名稱）和密碼
- 連接埠需求：80或443
- 授權要求：探索所需的FCP授權和對應/遮罩磁碟區

組態

欄位	說明
NetApp管理IP	NetApp叢集的IP位址或完整網域名稱
使用者名稱	NetApp叢集的使用者名稱
密碼	NetApp叢集的密碼

進階組態

欄位	說明
庫存輪詢時間間隔（分鐘）	庫存輪詢之間的時間間隔（預設為20分鐘）

效能意見調查時間間隔（秒）	效能輪詢之間的時間間隔（預設為300秒）

叢集**Data ONTAP** 式功能儲存

適用於NetApp叢集Data ONTAP 式物件登陸頁面上可能找到的物件或參考的術語。

叢集**Data ONTAP** 式的「儲存術語」

下列詞彙適用於NetApp叢集Data ONTAP 式物件登陸頁面上的物件或參考資料。其中許多術語也適用於其他資料收集器。

- 模型：此叢集中唯一、獨立節點模型名稱的以逗號分隔清單。如果叢集內的所有節點都是相同的模型類型、則只會顯示一個模型名稱。
- 廠商：如果您要設定新的資料來源、您會看到相同的廠商名稱。
- 序號：陣列序號。在叢集架構儲存系統（例如NetApp叢集Data ONTAP 式功能）上、此序號可能不如個別的「儲存節點」序號使用。
- IP -通常是在資料來源中設定的IP或主機名稱。
- 微碼版本-韌體。
- 原始容量：系統中所有實體磁碟的基礎2總和、無論其角色為何。
- 延遲：代表主機面對的工作負載在讀取和寫入過程中所經歷的情況。理想情況下、OCI會直接取得此值、但這種情況通常不會發生。OCI通常會執行IOP加權計算、以個別內部磁碟區的統計資料來取代陣列。
- 處理量：從內部磁碟區彙總。
- 管理-這可能包含裝置管理介面的超連結。由Insight資料來源以程式設計方式建立、做為庫存報告的一部分。

叢集**Data ONTAP** 式功能儲存資源池

適用於NetApp叢集Data ONTAP 式物件或參考資料的術語、可在NetApp叢集式物件資源庫資產登陸頁面找到。

叢集**Data ONTAP** 式的《邊區儲存資源池術語》

下列詞彙適用於您在NetApp叢集式Data ONTAPStorage Pool資產登陸頁面上可能找到的物件或參考資料。其中許多術語也適用於其他資料收集器。

- 儲存設備：此儲存設備所使用的儲存陣列。必填。
- 鍵入：列舉的可能性清單中的描述性值。最常見的是「Aggregate」或「RAID Group」。
- 節點-如果此儲存陣列的架構使資源池屬於特定儲存節點、則此處的名稱將會顯示為其專屬登陸頁面的超連結。
- 使用Flash Pool（是/無值）、這種SATA/SAS型集區是否使用SSD來快取加速？
- 備援：RAID層級或保護方案。RAID-DP為雙同位元檢查、RAID_tp為三同位元檢查。
- 容量：此處的值是已用邏輯容量、可用容量和邏輯總容量、以及這些容量使用的百分比。
- 過度委派容量：如果使用效率技術、您已將容量總計或內部Volume容量分配給大於儲存資源池邏輯容量的總和、則此處的百分比值將大於0%。

- Snapshot（快照）-使用的快照容量和總容量（如果您的儲存資源池架構將部分容量專用於專為快照而設計的區段區域）。在不支援支援的情況下、支援的部分可能會出現這個問題、而其他的不支援的組態則較少ONTAP MetroCluster ONTAP 。
- 使用率-百分比值、顯示此儲存資源池中任何磁碟貢獻容量的最高磁碟使用率百分比。磁碟使用率不一定與陣列效能有密切的關聯、因為磁碟重建、重複資料刪除活動等原因、在缺乏主機驅動的工作負載的情況下、使用率可能會很高。此外、許多陣列的複寫實作可能會提高磁碟使用率、而不會顯示為內部磁碟區或磁碟區工作負載。
- IOPS：所有磁碟的IOPs總和、可為此儲存資源池提供容量。
- 處理量：所有磁碟的總處理量、可為此儲存資源池提供容量。

叢集**Data ONTAP** 式功能儲存節點

適用於NetApp叢集式Data ONTAP儲存節點資產登陸頁面上可能找到的物件或參考的術語。

叢集**Data ONTAP** 式的功能區儲存節點術語

下列詞彙適用於您在NetApp叢集Data ONTAP 式物件庫資產登陸頁面上可能找到的物件或參考資料。其中許多術語也適用於其他資料收集器。

- Storage（儲存設備）-此節點屬於何種儲存陣列。必填。
- HA合作夥伴：在節點容錯移轉至一個節點、而只有一個節點的平台上、通常會顯示於此處。
- State（狀態）-節點的健全狀況。只有當陣列健全狀況足以由資料來源進行庫存時、才能使用。
- 模型-節點的模型名稱。
- 版本-裝置的版本名稱。
- 序號：節點序號。
- Memory（記憶體）- base 2記憶體（若有）。
- 使用率- ONTAP 在功能方面、這是專屬演算法的控制器壓力索引。每次效能意見調查都會報告0到100%之間的數字、這是WAFL 指較高的VMware磁碟爭用或平均CPU使用率。如果您觀察到持續值> 50%、這表示容量偏低、可能是控制器/節點不夠大、或旋轉磁碟不足以吸收寫入工作負載。
- IOPS -直接衍生自ONTAP 節點物件上的RzZAPI呼叫。
- 延遲-直接衍生自ONTAP 節點物件上的RzZAPI呼叫。
- 處理量：直接衍生自ONTAP 節點物件上的RzZAPI呼叫。
- 處理器- CPU數量。

適用於**Unified Manager**資料來源的**NetApp**叢集**Data ONTAP** 式功能

此資料來源會從ONTAP Unified Manager（UM）6.0以上資料庫收集R2.1.x資料。Insight會使用此資料來源、探索在UM中設定和填入的所有叢集。為了提高效率、Insight不會在叢集本身上呼叫ZAPI。此資料來源不支援效能。

組態

此資料收集器已不再提供OnCommand Insight 、從版本號為e.7.3.11開始。

欄位	說明
Unified Manager IP	Unified Manager的IP位址或完整網域名稱
使用者名稱	Unified Manager的使用者名稱
密碼	Unified Manager密碼
連接埠	用於與Unified Manager通訊的連接埠（預設3306）

進階組態

欄位	說明
庫存輪詢時間間隔（分鐘）	庫存輪詢之間的時間間隔（預設為15分鐘）
排除叢集	要排除的叢集IP清單以逗號分隔

NetApp Data ONTAP 支援**7-Mode**資料來源

若儲存系統使用Data ONTAP 以7-Mode運作的VMware軟體、您應該使用ONTAPI資料來源、該資料來源會使用CLI取得容量編號。

術語

從NetApp供應的NetApp解決方案7-Mode資料來源取得下列庫存資訊Data ONTAP OnCommand Insight 。對於Insight取得的每種資產類型、都會顯示此資產最常用的術語。檢視或疑難排解此資料來源時、請謹記下列術語：

廠商/模型術語	Insight術語
磁碟	磁碟
RAID群組	磁碟群組
檔案管理器	儲存設備
檔案管理器	儲存節點
Aggregate	儲存資源池
LUN	Volume

Volume	內部Volume

這些只是通用的術語對應、可能不代表此資料來源的每個案例。

需求

- 靜態儲存控制器和FAS 合作夥伴的IP位址
- 連接埠443
- 控制器和合作夥伴的使用者名稱和密碼
- 控制器和合作夥伴控制器的自訂管理層級使用者名稱和密碼、具有7-Mode的下列角色功能：
  - 「API-*」：使用此選項可OnCommand Insight 讓效益管理程式執行所有NetApp儲存API命令。
  - 「login-http-admin」：使用此選項可透過OnCommand Insight HTTP連線至NetApp儲存設備。
  - 「安全性-API-vFilerTM」：使用此功能可OnCommand Insight 讓效益管理系統執行NetApp儲存API命令、以擷取vFiler單元資訊。
  - 「CLI選項」：使用此選項可讀取儲存系統選項。
  - 「CLI/LUN」：存取這些命令來管理LUN。顯示特定LUN或LUN類別的狀態（LUN路徑、大小、線上/離線狀態及共用狀態）。
  - "CLI/df"：使用此選項可顯示可用磁碟空間。
  - "CLI/ifconfig"：使用此選項可顯示介面和IP位址。

組態

欄位	說明
Filer位址	NetApp Filer的IP位址或完整網域名稱
使用者名稱	NetApp Filer的使用者名稱
密碼	NetApp Filer的密碼
叢集中HA合作夥伴Filer的位址	HA合作夥伴Filer的IP位址或完整網域名稱
叢集中HA合作夥伴Filer的使用者名稱	NetApp HA合作夥伴Filer的使用者名稱
叢集中HA合作夥伴Filer的密碼	NetApp HA合作夥伴Filer的密碼

進階組態

欄位	說明
庫存輪詢時間間隔（分鐘）	庫存輪詢之間的時間間隔（預設為20分鐘）

連線類型	選擇連線類型
連線連接埠	用於NetApp API的連接埠
效能意見調查時間間隔（秒）	效能輪詢之間的時間間隔（預設為300秒）

儲存系統連線

除了使用此資料來源的預設管理使用者之外、您也可以直接在NetApp儲存系統上設定具有管理權限的使用者、以便此資料來源從NetApp儲存系統取得資料。

連線至NetApp儲存系統時、需要在取得主pFiler（儲存系統所在）時指定的使用者符合下列條件：

- 使用者必須位於vfiler0（根Filer/pFiler0）上。

  擷取主要pFiler時、會擷取儲存系統。

- 下列命令定義使用者角色功能：
  - 「API-*」：使用此選項可OnCommand Insight 讓效益管理程式執行所有NetApp儲存API命令。使用ZAPI時需要使用此命令。
  - 「login-http-admin」：使用此選項可透過OnCommand Insight HTTP連線至NetApp儲存設備。使用ZAPI時需要使用此命令。
  - 「安全性-API-vFilerTM」：使用此功能可OnCommand Insight 讓效益管理系統執行NetApp儲存API命令、以擷取vFiler單元資訊。
  - 「CLI選項」：用於「選項」命令、用於合作夥伴IP和啟用的授權。
  - 「CLI/LUN」：存取以下命令以管理LUN。顯示特定LUN或LUN類別的狀態（LUN路徑、大小、線上/離線狀態及共用狀態）。
  - "CLI/df"：適用於"df -s"、"df -r"、"df -A -r"命令、用於顯示可用空間。
  - "CLI/ifconfig"：用於執行「ifconfig-A」命令、用於取得檔案管理器IP位址。
  - CLI字節：用於「rdfile /etc/netgroup」命令、用於取得netgroup。
  - 「CLI/date」：適用於「date」命令、用於取得Snapshot複本的完整日期。
  - 「CLCLI抓取」：適用於「快照清單」命令、可用於取得Snapshot複本。

如果未提供CLI日期或CLI快照權限、則擷取作業可以完成、但不會報告Snapshot複本。

若要成功取得7-Mode資料來源、且不會在儲存系統上產生任何警告、您應該使用下列其中一個命令字串來定義使用者角色。此處列出的第二個字串是第一個的精簡版本：

```
login-http-admin,api-*,security-api-vfile,cli-rdfile,cli-options,cli-
df,cli-lun,cli-ifconfig,cli-date,cli-snap,
or
login-http-admin,api-*,security-api-vfile,cli-*
```

NetApp E系列資料來源

NetApp E系列資料來源會收集庫存與效能資訊。有兩種可能的組態（韌體6.x和韌體7.x+）、兩者都有相同的值。

術語

從NetApp E系列資料來源取得下列庫存資訊OnCommand Insight 。對於Insight取得的每種資產類型、都會顯示此資產最常用的術語。檢視或疑難排解此資料來源時、請謹記下列術語：

廠商/模型術語	Insight術語
磁碟機	磁碟
Volume群組	磁碟群組
儲存陣列	儲存設備
控制器	儲存節點
Volume群組	儲存資源池
Volume	Volume

這些只是通用的術語對應、可能不代表此資料來源的每個案例。

需求

- 陣列上每個控制器的IP位址
- 連接埠需求2463

組態

欄位	說明
以逗號分隔的陣列SANtricity 資訊控制器IP清單	陣列控制器的IP位址和/或完整網域名稱

進階組態

欄位	說明
庫存輪詢時間間隔（分鐘）	庫存輪詢之間的時間間隔（預設為30分鐘）
效能意見調查時間間隔（最多3、600秒）	效能輪詢之間的時間間隔（預設為300秒）

適用於NetApp E系列儲存資產登陸頁面上可能找到的物件或參考的術語。

E系列儲存術語

下列術語適用於您在NetApp E系列儲存資產登陸頁面上可能找到的物件或參考資料。其中許多術語也適用於其他資料收集器。

- 機型：裝置的機型名稱。
- 廠商：如果您要設定新的資料來源、您會看到相同的廠商名稱。
- 序號：陣列序號。在叢集架構儲存系統（例如NetApp叢集Data ONTAP 式功能）上、此序號可能不如個別的「儲存節點」序號使用。
- IP -通常是在資料來源中設定的IP或主機名稱。
- 微碼版本-韌體。
- 原始容量：系統中所有實體磁碟的基礎2總和、無論其角色為何。
- 延遲：代表主機面對的工作負載在讀取和寫入過程中所經歷的情況。Insight會計算從儲存區中的磁碟區衍生出的IOP加權平均值。
- 處理量：陣列面對主機的總處理量。Insight會加總磁碟區的處理量、以得出此值。
- 管理-這可能包含裝置管理介面的超連結。由Insight資料來源以程式設計方式建立、做為庫存報告的一部分。

適用於NetApp E系列儲存資源池資產登陸頁面上可能找到的物件或參考的術語。

E系列儲存資源池術語

下列術語適用於您在NetApp E系列儲存資源池資產登陸頁面上可能找到的物件或參考資料。其中許多術語也適用於其他資料收集器。

- 儲存設備：此儲存設備所使用的儲存陣列。必填。
- 鍵入：列舉的可能性清單中的描述性值。最常見的是「精簡配置」或「RAID群組」。
- 節點-如果此儲存陣列的架構使資源池屬於特定儲存節點、則此處的名稱將會顯示為其專屬登陸頁面的超連結。
- 使用Flash Pool - Yes（是）/ No（否）值。
- 備援：RAID層級或保護方案。E系列報告DDP資源池的「RAID 7」。
- 容量：此處的值是已用邏輯容量、可用容量和邏輯總容量、以及這些容量使用的百分比。這些值都包括E系列的「保存」容量、因此數字和百分比都會高於E系列本身的使用者介面。
- 過度使用容量：如果使用效率技術、您已將大於儲存資源池邏輯容量的總Volume容量分配給總容量、則此處的百分比值將大於0%。
- Snapshot（快照）-使用的快照容量和總容量（如果您的儲存資源池架構將部分容量專用於專為快照而設計的區段區域）。
- 使用率-百分比值、顯示此儲存資源池中任何磁碟貢獻容量的最高磁碟使用中百分比。磁碟使用率不一定與陣列效能有密切的關聯、因為磁碟重建、重複資料刪除活動等原因、在缺乏主機驅動的工作負載的情況下、使

用率可能會很高。此外、許多陣列的複寫實作可能會提高磁碟使用率、而不會顯示為磁碟區工作負載。

- IOPS：所有磁碟的IOPs總和、可為此儲存資源池提供容量。
- 處理量：所有磁碟的總處理量、可為此儲存資源池提供容量。

E系列儲存節點

適用於NetApp E系列儲存節點資產登陸頁面上可能找到的物件或參考的術語。

E系列儲存節點術語

下列術語適用於您在NetApp E系列儲存資源池資產登陸頁面上可能找到的物件或參考資料。其中許多術語也適用於其他資料收集器。

- Storage（儲存設備）-此節點屬於何種儲存陣列。必填。
- HA合作夥伴：在節點容錯移轉至一個節點、而只有一個節點的平台上、通常會顯示於此處。
- State（狀態）-節點的健全狀況。只有當陣列健全狀況足以由資料來源進行庫存時、才能使用。
- 模型-節點的模型名稱。
- 版本-裝置的版本名稱。
- 序號：節點序號。
- Memory（記憶體）- base 2記憶體（若有）。
- 使用率- NetApp E系列目前無法使用使用率。
- IOPS -將專屬於此節點的磁碟區的所有IOPs加總計算得出。
- 延遲-代表此控制器上一般主機延遲或回應時間的數字。Insights會從專屬於此節點的磁碟區計算IOP加權平均值。
- 處理量：代表此控制器上主機驅動處理量的數字。計算方式是將專屬於此節點之磁碟區的所有處理量加總。
- 處理器- CPU數量。

NetApp主機與VM檔案系統資料來源

您可以使用NetApp主機和VM檔案系統資料來源、擷取所有Microsoft Windows主機和VM（虛擬機器）檔案系統、以及所有支援的Linux VM（僅限虛擬對應的VM）的檔案系統詳細資料和儲存資源對應。 已存在於Insight伺服器中、並以已設定的運算資源群組（CRG）進行註釋。

一般要求

- 此功能必須另行購買。

  如需協助、請聯絡Insight代表。

- 您應該查看Insight支援對照表、確認您的主機或虛擬機器作業系統是否受到支援。

  若要驗證是否已建立檔案系統與儲存資源之間的連結、請檢查相關的儲存設備或虛擬化廠商類型與版本是否報告所需的磁碟區或虛擬磁碟識別資料。

Microsoft Windows需求

- 此資料來源使用視窗管理規範（WMI）資料結構來擷取資料。

  此服務必須可從遠端運作且可供使用。尤其是、連接埠135必須可存取、而且如果位於防火牆後、必須開啟連接埠135。

- Windows網域使用者必須擁有適當的權限才能存取WMI結構。
- 需要系統管理員權限。
- 動態TCP連接埠指派1024-6555、適用於Windows 2003及更舊版本
- 適用於Windows 2008的連接埠49152-6555

> 一般而言、當您嘗試在Insight、AU及此資料來源之間使用防火牆時、應諮詢Microsoft團隊、以識別他們認為需要的連接埠。

Linux需求

- 此資料來源使用安全Shell（SSH）連線在Linux VM上執行命令。

  SSH服務必須可從遠端運作且可供使用。尤其是連接埠22必須可存取、而且如果在防火牆後必須開啟。

- SSH使用者必須擁有Sudo權限、才能在Linux VM上執行唯讀命令。

  您必須使用相同的密碼登入SSH、並回答任何的Sudo密碼挑戰。

使用建議

- 您應該使用相同的運算資源群組註釋、註釋一組具有通用作業系統認證的主機和虛擬機器。

  每個群組都有此資料來源的執行個體、可從這些主機和虛擬機器探索檔案系統詳細資料。

- 如果您有這個資料來源的執行個體成功率低（例如OnCommand Insight 、在1000部主機和群組中的虛擬機器中、僅有50部主機和虛擬機器會發現檔案系統詳細資料）、 您應該將成功探索的主機和虛擬機器移至個別的運算資源群組。

組態

欄位	說明
使用者名稱	作業系統使用者擁有適當權限、可為Windows作業系統使用者擷取檔案系統資料、其中必須包含網域首碼。
密碼	作業系統使用者的密碼
運算資源群組	用於標記資料來源主機和虛擬機器的註釋值會探索檔案系統。空白值表示資料來源會探索所有主機和虛擬機器的檔案系統、而這些主機和虛擬機器目前未註釋任何運算資源群組。

進階組態

欄位	說明
庫存輪詢時間間隔（分鐘）	庫存輪詢之間的時間間隔（預設為360分鐘）

NetApp SolidFire 產品資料來源

NetApp SolidFire 支援iSCSI與Fibre Channel SolidFire 之間的整合、可同時進行庫存與效能收集。

該資料來源採用了The Rizest API SolidFire SolidFire 。資料來源所在的擷取單元、必須能夠啟動HTTPS連線至SolidFire 叢集管理IP位址上的TCP連接埠443。資料來源需要能夠在SolidFire 叢集上進行REST API查詢的認證資料。

術語

從NetApp供應資料來源取得下列庫存資訊SolidFire OnCommand Insight 。對於Insight取得的每種資產類型、都會顯示此資產最常用的術語。檢視或疑難排解此資料來源時、請謹記下列術語：

廠商/模型術語	Insight術語
磁碟機	磁碟
叢集	儲存設備
節點	儲存節點
Volume	Volume
Fibre Channel連接埠	連接埠
Volume存取群組、LUN指派	Volume Map
iSCSI工作階段	Volume遮罩

這些只是通用的術語對應、可能不代表此資料來源的每個案例。

需求

以下是設定此資料來源的需求：

- 管理虛擬IP位址
- 連接埠443

組態

欄位	說明
管理虛擬IP位址（MVIP）	管理VMware叢集的虛擬IP位址SolidFire
使用者名稱	用來登入SolidFire 到Isname叢集的名稱
密碼	用於登入SolidFire 到故障叢集的密碼

進階組態

欄位	說明
庫存輪詢時間間隔（分鐘）	庫存輪詢之間的時間間隔（預設為60分鐘）
TCP連接埠	TCP連接埠用於連線SolidFire 至伺服器（預設443）
連線逾時（秒）	連線逾時（預設為60秒）
效能意見調查時間間隔（秒）	效能輪詢之間的時間間隔（預設為300秒）

疑難排解

當支援報告錯誤時SolidFire 、會以OnCommand Insight 下列方式顯示在功能表中：

```
An error message was received from a SolidFire device while trying to retrieve
data. The call was <method> (<parameterString> ). The error message from the
device was (check the device manual): <message>
```

其中：

- 方法是HTTP方法、例如GET或PUT。
- 參數字串>是以逗號分隔的參數清單、包含在REST呼叫中。
- 此為傳回的錯誤訊息。

NetApp StorageGRID 產品資料來源

此資料來源會收集庫存和效能資料StorageGRID 以供使用。

需求

以下是設定此資料來源的需求：

- 主機IP位址StorageGRID
- 已指派「度量查詢」和「租戶存取」角色的使用者使用者名稱和密碼

- 連接埠443

組態

欄位	說明
主機IP位址（MVIP StorageGRID ）	主機IP位址StorageGRID
使用者名稱	用來登入StorageGRID 此功能的名稱
密碼	用於登入StorageGRID 資訊區的密碼

進階組態

欄位	說明
庫存輪詢時間間隔（分鐘）	庫存輪詢之間的時間間隔（預設為60分鐘）
效能意見調查時間間隔（秒）	效能輪詢之間的時間間隔（預設為900秒）

OpenStack資料來源

OpenStack（REST API / KVM）資料來源會收集OpenStack硬體執行個體的相關資訊。此資料來源會收集所有OpenStack執行個體的庫存資料、以及VM效能資料（可選）。

需求

以下是設定OpenStack資料來源的需求。

- OpenStack控制器的IP位址
- 建議使用OpenStack管理員角色認證和Sudo存取Linux KVM Hypervisor。

> ⓘ 如果您沒有使用管理員帳戶或與管理員同等的權限、您仍可從資料來源取得資料。您需要修改原則組態檔（例如etc/nova/policy.json）、以允許具有非管理員角色的使用者呼叫API：

  - "OS_compute _API:os-Availability：區域：詳細資料"："
  - "OS_compute _API:os-hypervisor（OS運算API：OS Hypervisor）"："
  - OS_compute _API：伺服器：詳細資料：Get_all_租 戶"：""
- 為了收集效能、必須安裝並設定OpenStack Ceilometer模組。設定Ceilometer的方法是編輯 `nova.conf` 為每個Hypervisor建立檔案、然後在每個Hypervisor上重新啟動Nova運算服務。不同OpenStack版本的選項名稱會變更：
  - 冰屋
  - Juno
  - 公斤

    - 自由
    - Mitaka
    - Newton
    - 八田市
- 對於CPU統計資料、運算節點上的/etc/nova/nova.conf必須開啟「compute_mones=ComputeDriverCPUMonitor」。
- 連接埠需求：
    - http為5000、https為13000、Keystone服務為13000
    - 22適用於KVM SSH
    - 8774適用於Nova Compute Service
    - 8776適用於Cinder Block Service
    - 8777適用於Ceilometer Performance Service
    - 9292適用於Glance Image Service

> 連接埠會繫結至特定服務、服務可能會在控制器或其他大型環境中的主機上執行。

組態

欄位	說明
OpenStack控制器IP位址	OpenStack控制器的IP位址或完整網域名稱
OpenStack管理員	OpenStack管理的使用者名稱
OpenStack密碼	OpenStack管理所用的密碼
OpenStack管理員租戶	OpenStack管理員租戶
KVM Sudo使用者	KVM Sudo使用者名稱
選擇「密碼」或「OpenSSH金鑰檔」以指定認證類型	用於透過SSH連線至裝置的認證類型
完整的庫存私密金鑰路徑	完整的庫存私密金鑰路徑
KVM Sudo密碼	KVM Sudo密碼

進階組態

欄位	說明
透過SSH啟用Hypervisor庫存探索	核取此選項、即可透過SSH啟用Hypervisor庫存探索

OpenStack管理URL連接埠	OpenStack管理URL連接埠
使用HTTPS	核取以使用安全HTTP
HTTP連線逾時（秒）	HTTP連線逾時（預設為300秒）
SSH連接埠	用於SSH的連接埠
SSH程序等待逾時（秒）	SSH程序逾時（預設30秒）
SSH程序重試	嘗試進行庫存重試的次數
庫存輪詢時間間隔（分鐘）	庫存輪詢之間的時間間隔（預設為20分鐘）

Oracle ZFS資料來源

Oracle ZFS資料來源支援庫存與效能收集。

術語

從這個資料來源取得下列庫存資訊OnCommand Insight 。對於Insight取得的每種資產類型、都會顯示此資產最常用的術語。檢視或疑難排解此資料來源時、請謹記下列術語：

廠商/模型術語	Insight術語
磁碟（SDD）	磁碟
叢集	儲存設備
控制器	儲存節點
LUN	Volume
LUN對應	Volume Map
啟動器、目標	Volume遮罩
分享	內部Volume

這些只是通用的術語對應、可能不代表此資料來源的每個案例。

需求

以下是設定此資料來源的需求：

- ZFS Controller（ZFS控制器）-1和ZFS Controller（ZFS控制器）-2的主機名稱
- 系統管理員使用者名稱和認證
- 連接埠需求：215 HTTP / HTTPS

組態

ZFS控制器1主機名稱	儲存控制器1的主機名稱
ZFS控制器-2主機名稱	儲存控制器2的主機名稱
使用者名稱	儲存系統管理員使用者帳戶的使用者名稱
密碼	系統管理員使用者帳戶的密碼

進階組態

欄位	說明
TCP連接埠	用於連接至ZFS的TCP連接埠（預設為215）
連線類型	HTTP或HTTPS
庫存輪詢時間間隔	庫存輪詢時間間隔（預設為60分鐘）
連線逾時	預設值為60秒
效能意見調查時間間隔（秒）	效能輪詢之間的時間間隔（預設為300秒）

疑難排解

如果您在使用此資料收集器時遇到問題、請嘗試下列事項：

問題：	試用：
"登入認證資料無效"	驗證ZFS使用者帳戶和密碼
「組態錯誤」、並顯示錯誤訊息「停用REST服務」	確認此裝置已啟用REST服務。

「組態錯誤」、並顯示錯誤訊息「使用者未獲授權執行命令」	可能是因為某些角色（例如「進階分析」）不包含在設定的使用者<userName> 之間。可能的解決方案： • 使用唯讀角色修正使用者$｛user｝的分析（統計）範圍：-從「組態」→「使用者」畫面、將滑鼠移到角色上、然後按兩下以允許編輯 • 從範圍下拉式功能表中選取「分析」。可能的內容清單隨即出現。 • 按一下「最上方」核取方塊、即可選取三個屬性。-按一下右側的「新增」按鈕。 • 按一下快顯視窗右上角的「Apply（套用）」按鈕。快顯視窗隨即關閉。

Pure Storage FlashArray資料來源

Pure Storage FlashArray（HTTP）資料來源是用來收集Pure Storage Flash Array的資訊。Insight同時支援庫存管理和效能收集。

術語

從Pure Storage FlashArray資料來源取得下列庫存資訊OnCommand Insight 。對於Insight取得的每種資產類型、都會顯示此資產最常用的術語。檢視或疑難排解此資料來源時、請謹記下列術語：

廠商/模型術語	Insight術語
磁碟機（SSD）	磁碟
陣列	儲存設備
控制器	儲存節點
Volume	Volume
連接埠	連接埠
LUN對應（主機、主機群組、目標連接埠）	Volume Map、Volume Mask

這些只是通用的術語對應、可能不代表此資料來源的每個案例。

需求

- 儲存系統IP位址
- Pure儲存系統管理員帳戶的使用者名稱和密碼。
- 連接埠需求：HTTP/HTTPS 80/443

組態

欄位	說明
FlashArray主機	FlashArray Management Server的IIP位址或完整網域名稱
使用者名稱	FlashArray管理伺服器的使用者名稱
密碼	FlashArray管理伺服器的密碼

進階組態

欄位	說明
連線類型	管理伺服器
TCP連接埠	TCP連接埠用於連線至FlashArray伺服器（預設443）
連線逾時（秒）	連線逾時（預設為60秒）
庫存輪詢時間間隔（分鐘）	庫存輪詢之間的時間間隔（預設為60分鐘）
效能意見調查時間間隔（秒）	效能輪詢之間的時間間隔（預設為300秒）

QLogic FC交換器資料來源

對於組態設定、QLogic FC交換器（SNMP）資料來源需要FC交換器裝置的網路位址（指定為IP位址）、以及用來存取裝置的SNMP _read-only（SNMP唯讀）社群字串。

組態

欄位	說明
SANsurfer交換器	SANsurfer交換器的IP位址或完整網域名稱
SNMP版本	SNMP版本
SNMP社群	SNMP社群字串
使用者名稱	SANsurfer交換器的使用者名稱
密碼	SANsurfer交換器密碼

進階組態

欄位	說明
庫存輪詢時間間隔（分鐘）	庫存輪詢之間的時間間隔（預設為15分鐘）
SNMP驗證傳輸協定	SNMP驗證傳輸協定（僅限v3）
SNMP重試次數	SNMP重試嘗試次數
SNMP逾時（毫秒）	SNMP逾時（預設值5000毫秒）
啟用資料綁定	選取以啟用補漏白
設陷之間的最短時間（秒）	擷取嘗試之間由陷阱觸發的最短時間（預設為10秒）
網路名稱	要由資料來源回報的網路名稱。保留空白以將網路名稱報告為WWN。
效能意見調查時間間隔（秒）	效能輪詢之間的時間間隔（預設為300秒）

Red Hat（RHEV）資料來源

Red Hat Enterprise Virtualization（REST）資料來源會透過HTTPS收集RHEV執行個體的相關資訊。

需求

- 透過REST API透過連接埠443的RHEV伺服器IP位址
- 唯讀使用者名稱和密碼
- RHEV版本3.0+

組態

欄位	說明
RHEV伺服器IP位址	RHEV伺服器的IP位址或完整網域名稱
使用者名稱	RHEV伺服器的使用者名稱
密碼	RHEV伺服器使用的密碼

進階組態

欄位	說明

HTTPS通訊連接埠	用於HTTPS通訊至RHEV的連接埠
庫存輪詢時間間隔（分鐘）	庫存輪詢之間的時間間隔（預設為20分鐘）
連線逾時（秒）	連線逾時（預設為60秒）

小提琴**Flash Memory Array**資料來源

Violin 6000系列Flash記憶體陣列（HTTP）資料來源會收集網路資訊、以供Violin 6000系列Flash記憶體陣列進行分析和驗證。

術語

此資料收集器已不再提供OnCommand Insight 、從版本號為e.7.3.11開始。

從Violin 6000系列Flash Memory Array資料來源取得下列庫存資訊OnCommand Insight 。對於Insight取得的每種資產類型、都會顯示此資產最常用的術語。檢視或疑難排解此資料來源時、請謹記下列術語：

廠商/模型術語	Insight術語
小提琴智慧型記憶體模組（VIMMM）	磁碟
容器	儲存設備
記憶體閘道	儲存節點
LUN	Volume
啟動器、啟動器群組、目標	Volume Map、Volume Mask

這些只是通用的術語對應、可能不代表此資料來源的每個案例。

需求

- 您需要儲存設備的唯讀使用者名稱和密碼。
- 使用儲存IP位址、以網頁瀏覽器驗證存取。

組態

欄位	說明
Violin記憶體陣列主閘道的IP位址或FQDN	Violin記憶體陣列主閘道的IP位址或完整網域名稱
使用者名稱	Violin記憶體陣列主閘道的使用者名稱

密碼	Violin記憶體陣列主閘道的密碼

進階組態

欄位	說明
通訊連接埠	用於與Violin陣列通訊的連接埠
HTTPS已啟用	選取以使用HTTPS
庫存輪詢時間間隔（分鐘）	庫存輪詢之間的時間間隔（預設為20分鐘）
連線逾時（秒）	連線逾時（預設為60秒）
效能意見調查時間間隔（秒）	效能輪詢之間的時間間隔（預設為300秒）

VMware vSphere資料來源

VMware vSphere（Web服務）資料來源會收集ESX主機資訊、並要求虛擬中心內所有物件的_唯讀_權限。

術語

從VMware vSphere資料來源取得下列庫存資訊OnCommand Insight 。對於Insight取得的每種資產類型、都會顯示此資產最常用的術語。檢視或疑難排解此資料來源時、請謹記下列術語：

廠商/模型術語	Insight術語
虛擬磁碟	磁碟
主機	主機
虛擬機器	虛擬機器
資料儲存區	資料儲存區
LUN	LUN
Fibre Channel連接埠	連接埠

這些只是通用的術語對應、可能不代表此資料來源的每個案例。

需求

- Virtual Center伺服器的IP位址
- Virtual Center中的唯讀使用者名稱和密碼
- 虛擬中心內所有物件的唯讀權限。
- 存取Virtual Center伺服器上的SDK
- 連接埠需求：https-80 https-443
- 使用您的使用者名稱和密碼登入Virtual Center Client、並輸入以下命令驗證是否已啟用SDK、藉此驗證存取 `telnet <vc_ip\> 443`。

組態

欄位
說明
虛擬中心位址
虛擬中心或vSphere伺服器的網路位址、指定為IP _（nnn.n.n.n.nn.nnn_格式）位址或可透過DNS解析的主機名稱。
使用者名稱
VMware伺服器的使用者名稱。
密碼
VMware伺服器的密碼。

進階組態

欄位	說明
庫存輪詢時間間隔（分鐘）	庫存輪詢之間的時間間隔（預設為20分鐘）
連線逾時（毫秒）	連線逾時（預設為60000毫秒）
依篩選VM	選擇如何篩選VM
選擇「排除」或「包含」以指定清單	指定在收集資料時是否要納入或排除下列VM清單
要篩選的虛擬機器清單（以英文分隔、若值中使用以英文分隔、則以分號分隔）	要包含或排除在輪詢中的虛擬機器清單、以逗號分隔或以分號分隔
vCenter要求的重試次數	vCenter要求重試嘗試次數

通訊連接埠	用於VMware伺服器的連接埠
效能意見調查時間間隔（秒）	效能輪詢之間的時間間隔（預設為300秒）

變更資料來源認證

如果同類型的多個資料來源共用使用者名稱和密碼、您可以同時變更群組中所有裝置的密碼。

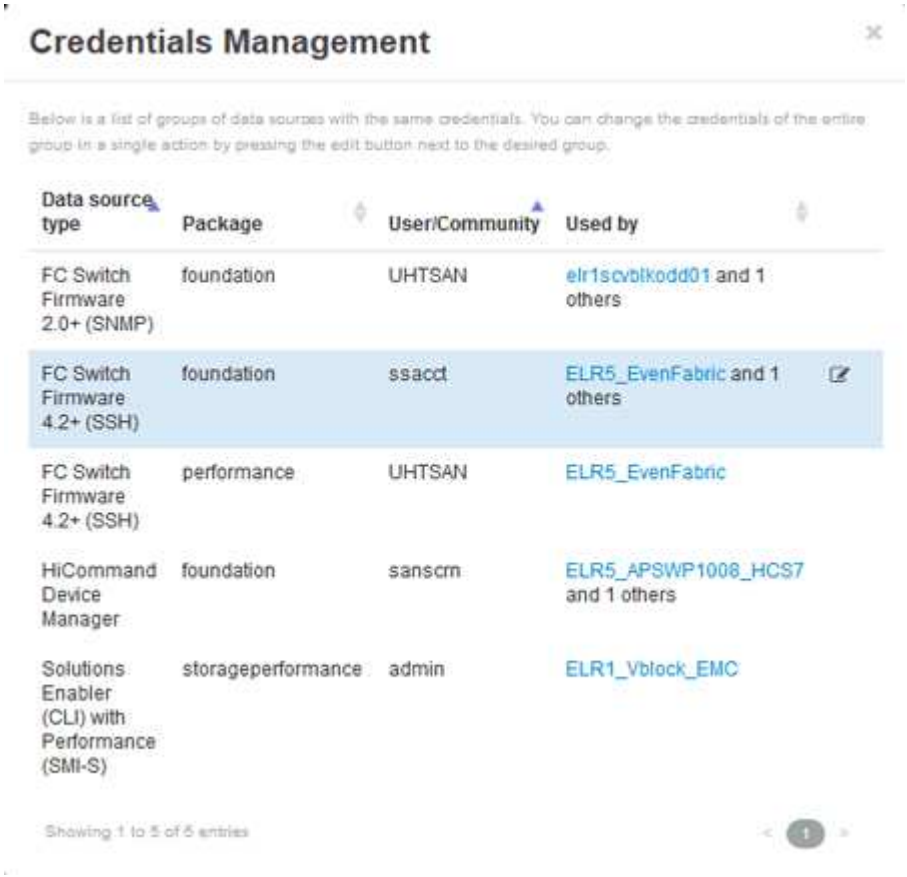
步驟

1. 在Insight工具列上、按一下*管理*。

   「資料來源」清單隨即開啟。

2. 按一下「動作」按鈕、然後選取「變更認證」選項。
3. 在「認證管理」對話方塊中、從清單中選取其中一個資料來源群組。

   「編輯」圖示（一張紙上的筆）會變成右側的作用中圖示。



4. 按一下 * 編輯 * 。
5. 輸入新密碼並加以確認。

導致資料收集問題的變更

如果OnCommand Insight 您在使用無法收集資料的功能時遇到問題、可能是環境發生變更。一般而言、您也應該在Insight中因應環境中的任何變更。

您可以使用此檢查清單來識別可能造成問題的網路變更：

- 您有變更任何密碼嗎？這些密碼在Insight中是否有所變更？
- 您是否從網路移除裝置？您也必須將此裝置從OnCommand Insight 更新中移除、以避免重新探索及重新導入。
- 您是否升級了基礎架構軟體（例如HP CommandView Eva或EMC Solutions Enabler）？

  確認採購單位已安裝適當版本的用戶端工具。如果資料來源故障持續發生、您需要聯絡技術支援部門以尋求協助、甚至是資料來源修補程式。

- 您的OnCommand Insight 所有采購單位是否都使用相同OnCommand Insight 的版本？如果遠端擷取單元和本機擷取單元執行不同OnCommand Insight 的版本、請在所有裝置上安裝相同版本、以修正資料收集問題。

  如果您需要在OnCommand Insight 所有的採購單位上安裝新版的更新版本、請前往支援網站下載正確版本。

- 您是否變更任何網域名稱或新增網域？您必須更新裝置解析度（先前稱為自動解析）方法。

詳細檢查一個資料來源

如果您發現資料來源故障或速度變慢、您可能需要檢查該資料來源的詳細資訊摘要、以判斷問題的原因。需要注意的資料來源會以紅色圓圈標記。

步驟

1. 在Insight工具列上、按一下*管理*。

   「資料來源」清單隨即開啟。任何列出的潛在問題資料來源都會以紅色圓圈標示。最嚴重的問題列在清單頂端。

2. 選取引起疑慮的資料來源。
3. 按一下資料來源名稱連結。
4. 在資料來源摘要頁面上、查看下列任何一節中的資訊：
   - 活動時間表

     列出與資料來源清單中顯示的目前狀態相關聯的事件。此摘要中的事件會依裝置顯示。錯誤以紅色顯示。您可以將滑鼠指標放在時間表項目上、以顯示其他資訊。

   - 此資料來源報告的裝置

     列出裝置類型、其IP位址、以及每個裝置的詳細資訊連結。

   - 此資料來源報告的變更（過去**3**週）

列出已新增或移除的任何裝置、或是已變更組態的裝置。

5. 在檢查資料來源資訊之後、您可能會想要使用頁面頂端的按鈕來執行下列其中一項作業：
   - *編輯*資料來源的說明、以修正問題。
   - *再次輪詢*強制輪詢、以顯示問題是否持續或間歇性。
   - *延後*資料來源輪詢3、7或30天、讓您有時間研究問題並停止警告訊息。
   - *在資料來源上安裝修補程式*以修正問題。
   - 準備*錯誤報告*以取得技術支援。
   - 刪除 Insight監控環境中的資料來源。

研究失敗的資料來源

如果資料來源顯示「* Inventory故障！」或「*效能故障！」訊息、以及高或中度影響、您必須使用資料來源摘要頁面及其連結資訊來研究此問題。

步驟

1. 按一下資料來源的連結*名稱*以開啟「摘要」頁面。
2. 在「Summary（摘要）」頁面上、查看* Comments（註解）*區域、以閱讀另一位工程師留下的任何附註、他們可能也正在調查此故障。
3. 記下任何效能訊息。
4. 如果此資料來源正在套用修補程式、請按一下連結以查看*修補程式頁面*、以查看是否導致此問題。
5. 將滑鼠指標移到*事件時間表*圖形的區段上、以顯示其他資訊。
6. 選取「裝置」的錯誤訊息、並顯示在「事件時間軸」下方、然後按一下訊息右側顯示的*錯誤詳細資料*圖示。

   錯誤詳細資料包括錯誤訊息的文字、最可能的原因、使用中的資訊、以及可嘗試修正問題的建議。

7. 在此資料來源所報告的裝置區域中、您可以篩選清單以僅顯示感興趣的裝置、然後按一下裝置的連結*名稱*以顯示該裝置的_asset頁面_。
8. 若要返回先前顯示的頁面、請使用下列其中一種技巧：
   - 按一下瀏覽器的上一頁箭頭。
   - 以滑鼠右鍵按一下返回箭頭、顯示頁面清單、然後選取您要的頁面。
9. 若要顯示其他資源的詳細資訊、請按一下「其他連結名稱」。
10. 當您返回資料來源摘要頁面時、請查看頁面底部的*變更*區域、查看最近的變更是否造成問題。

控制資料來源輪詢

變更資料來源之後、您可能希望它立即輪詢以檢查您的變更、或者您可能想要在處理問題時、將資料來源上的資料收集延遲一、三或五天。

步驟

1. 按一下「管理」、然後瀏覽至資料來源清單檢視
2. 選取您要控制輪詢的資料來源。
3. 按一下資料來源名稱連結。
4. 在資料來源摘要頁面上、檢查資訊、然後按一下以下兩個輪詢選項之一：
    - *再次輪詢*強制資料來源立即收集資料。
    - 延後、並從3、7或30天內選取輪詢延遲的長度。

完成後

如果您延後了資料來源上的資料收集、並想要重新啟動集合、請按一下摘要頁面上的* Resum*。

編輯資料來源資訊

您可以快速編輯資料來源設定資訊。

步驟

1. 按一下「管理」、然後瀏覽至資料來源清單檢視
2. 找出您要編輯的資料來源。
3. 使用下列其中一種方法開始變更：
    - 按一下所選資料來源右側的*編輯資料來源*。
    - 按一下所選資料來源的連結名稱、然後按一下*編輯*。這兩種方法都會開啟「編輯資料來源」對話方塊。
4. 進行所需的變更、然後按一下*「Save（儲存）」*。

編輯多個資料來源的資訊

您可以一次編輯同一廠商與模型的多個資料來源的大部分資訊。例如、如果這些資料來源共用使用者名稱和密碼、您可以在單一位置變更密碼、進而更新所有選取資料來源的密碼。

關於這項工作

您無法編輯所選資料來源的選項會顯示為灰色、或不會顯示在「編輯資料來源」對話方塊中。此外、當選項顯示*混合*的值時、表示選項的值會因選取的資料來源而異。例如、如果兩個選取資料來源的*逾時（秒）選項為*混合、則其中一個資料來源的逾時值可以是60、而另一個資料來源的值可以是90； 因此、如果您將此值變更為120、並將變更儲存至資料來源、則兩個資料來源的逾時設定都會變成120。

步驟

1. 按一下「管理」、然後瀏覽至資料來源清單檢視
2. 選取您要修改的資料來源。選取的資料來源必須屬於同一個廠商、機型和採購單位。

3. 單擊* Actions（操作）按鈕並選擇 Edit（編輯）*選項。
4. 在編輯對話方塊中、視需要變更任何*設定*。
5. 按一下「組態」連結、即可變更資料來源的任何基本選項。
6. 按一下「進階組態」連結、即可變更資料來源的任何進階選項。
7. 按一下「 * 儲存 * 」。

將資料來源標記對應至註釋

當資料來源設定為輪詢標記資料時、Insight會自動設定現有Insight附註的附註值、其名稱與標記相同。

如果Insight附註存在於資料來源中啟用標籤之前、資料來源標籤資料會自動新增至Insight附註。

當您在啟用標記之後建立註釋時、資料來源的初始輪詢不會自動更新註釋。更換或填入Insight附註所需的時間會延遲。為了避免延遲、您可以延後再恢復資料來源、強制標記更新註釋。

刪除資料來源

如果您已從環境中移除資料來源、也必須將其從OnCommand Insight 停止監控環境中刪除。

步驟

1. 在Insight工具列上、按一下*管理*。

   資料來源清單隨即開啟。

2. 選取您要刪除的資料來源。
3. 按一下連結的資料來源名稱。
4. 請檢查摘要頁面上所選資料來源的資訊、確定該資料來源是您要刪除的資料來源。
5. 按一下*刪除*。
6. 單擊*確定*確認操作。

什麼是資料來源修補程式

資料來源修補程式可修正現有修補程式的問題、也可讓您輕鬆新增資料來源類型（廠商和機型）。對於網路中的每種資料來源類型、您都可以上傳資料來源修補程式。您也可以安裝、測試及管理修補程序。不過、一次只能針對資料來源類型啟用一個修補程式。

您可以針對每個修補程式執行下列工作：

- 在比較每個接收修補程式的資料來源之前和之後、請檢查。
- 撰寫意見、說明決策或總結研究成果。
- 變更無法妥善回應修補程式的資料來源。

- 核准要提交至Insight伺服器的修補程式。
- 復原未如預期運作的修補程式。
- 以不同的修補程式取代故障的修補程式。

套用資料來源修補程式

資料來源修補程式會定期提供、讓您修正現有資料來源的問題、新增廠商的資料來源、或為廠商新增新模式。

開始之前

您必須已取得 `.zip` 包含最新資料來源的檔案 `.patch` 來自技術支援的檔案。

步驟

1. 在Insight工具列上、按一下*管理*。
2. 按一下*修補程式*。
3. 從「動作」按鈕選取*「套用修補程式」*。
4. 在「套用資料來源修補程式」對話方塊中、按一下「瀏覽」以找出 `.patch` 檔案：
5. 檢查*修補程式名稱*、說明*和*受影響的資料來源類型。
6. 如果選取的修補程式正確、請按一下*套用修補程式*。

   如果您套用的修補程式可修正資料來源的問題、則相同類型的所有資料來源都會隨修補程式一起更新、而且您必須核准修補程式。不會影響任何已設定資料來源的修補程式會自動核准。

完成後

如果您套用的修補程式是新廠商或新機型的資料來源、則必須在套用修補程式之後新增資料來源。

在一種資料來源上安裝修補程式

上傳資料來源修補程式之後、您可以將其安裝在相同類型的所有資料來源上。

開始之前

您必須已上傳要安裝在某種資料來源上的修補檔案。

步驟

1. 在Insight工具列上、按一下*管理*。
2. 按一下*修補程式*。
3. 從「動作」按鈕選取*「套用修補程式」*。
4. 在「套用資料來源修補程式」對話方塊中、按一下「瀏覽」以尋找上傳的修補程式檔案。
5. 請查看*修補程式名稱*、說明*和*受影響的資料來源類型。

6. 如果選取的修補程式正確、請按一下*套用修補程式*。

   相同類型的所有資料來源都會更新此修補程式。

管理修補程式

您可以檢閱所有套用至網路的資料來源修補程式目前狀態。如果您想要對修補程式執行動作、可以按一下目前審查中的修補程式表格中的連結名稱。

開始之前

您必須已上傳並安裝至少一個修補程式。

步驟

1. 在Insight工具列上、按一下*管理*。
2. 按一下*修補程式*。

   如果沒有安裝修補程式、目前正在審查的修補程式表將是空白的。

3. 在*目前正在審查的修補程式*中、檢查目前正在套用的資料來源修補程式狀態。
4. 若要檢查與特定修補程式相關的詳細資料、請按一下該修補程式的連結名稱。
5. 對於選取的修補程式、您可以按一下下列任一選項、對修補程式執行下一個動作：
   - *核准修補程式*將修補程式提交至資料來源。
   - *回溯*移除修補程式。
   - *置換修補程式*可讓您為這些資料來源選取不同的修補程式。

提交資料來源修補程式

您可以使用修補程式摘要中的資訊來決定修補程式是否如預期執行、然後將修補程式提交到您的網路。

開始之前

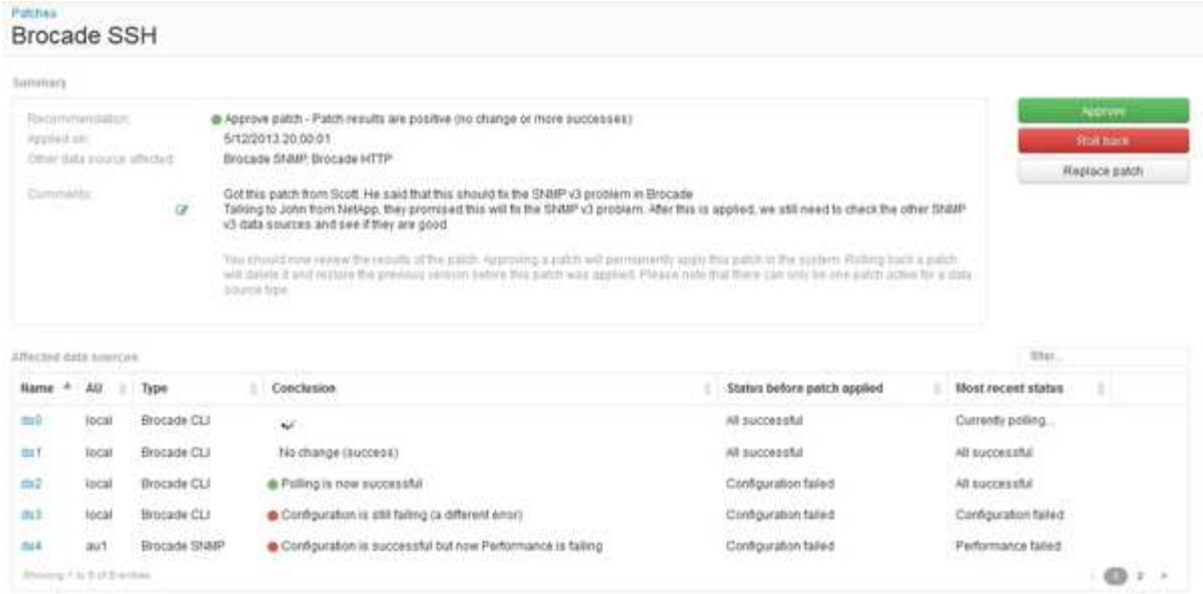
您已安裝修補程式、需要判斷修補程式是否成功且應獲得核准。

步驟

1. 在Insight工具列上、按一下*管理*。
2. 按一下*修補程式*。

   如果沒有安裝修補程式、目前正在審查的修補程式是空的。

3. 在*目前正在審查的修補程式*中、檢查目前正在套用的資料來源修補程式狀態。
4. 若要檢查與特定修補程式相關的詳細資料、請按一下該修補程式的連結名稱。
5. 在本例所示的「修補程式」摘要資訊中、請查看*建議*和*建議*、以評估修補程式的進度。



6. 查看*受影響的資料來源*表格、查看修補程式前後每個受影響資料來源的狀態。

   如果您擔心其中一個要修補的資料來源發生問題、請按一下「受影響的資料來源」表格中的「連結名稱」。

7. 如果您認為該修補程式應套用至該類型的資料來源、請按一下* Approve *。

   資料來源將會變更、並從目前正在審查的修補程式中移除修補程式。

復原資料來源修補程式

如果資料來源修補程式無法依照您預期的方式運作、您可以將其復原。復原修補程式會刪除它、並還原先前套用此修補程式之前的版本。

步驟

1. 在Insight工具列上、按一下*管理*。
2. 按一下*修補程式*。
3. 在*目前正在審查的修補程式*中、按一下看起來不成功的修補程式連結名稱。
4. 在資料來源的「修補程式」頁面上、檢查下列資訊：
   - *摘要*說明何時套用修補程式、受影響的資料來源、以及您或團隊其他成員對修補程式的意見。
   - *受影響的資料來源*會列出所有要修補的資料來源、並會比較修補狀態的「之前」和「之後」。
5. 若要顯示未成功處理修補程式之資料來源的詳細資料、請按一下連結的*名稱*。
   a. 查看摘要資訊。
   b. 請查看*事件時間表*、查看可能影響此資料來源的任何組態或效能資料。
6. 如果您認為修補程式將不會成功、請按一下瀏覽器的「上一步」箭頭、返回「修補程式」摘要頁面。
7. 按一下*回復*以移除該修補程式。

   如果您知道更有可能成功的其他修補程式、請按一下「取代修補程式」、然後上傳新的修補程式。

裝置解析度

您需要探索OnCommand Insight 所有想要用NetApp監控的裝置。為了準確追蹤環境中的效能與庫存、探索是必要的。一般而言、環境中大部分的裝置都是透過自動裝置解析功能來探索。

> 如果您正在執行升級、且升級時所在的系統中有非作用中的自動解決規則、則這些規則將會在升級期間刪除。若要保留非作用中的自動解決規則、請在執行升級之前先啟動規則（勾選方塊）。

在您安裝及設定資料來源之後、系統會識別環境中的裝置、包括交換器、儲存陣列、以及Hypervisor和VM的虛擬基礎架構。不過、這通常無法識別環境中100%的裝置。

在設定資料來源類型裝置之後、最佳做法是運用裝置解決規則來協助識別環境中剩餘的未知裝置。裝置解析度可協助您解決下列裝置類型的未知裝置：

- 實體主機
- 儲存陣列
- 磁帶
- 交換器

在裝置解析度之後、仍為「未知」的裝置會被視為一般裝置、您也可以在查詢和儀表板上顯示這些裝置。

接著建立的規則會在新增至環境時、自動識別具有類似屬性的新裝置。在某些情況下、裝置解析功能也允許手動識別、繞過Insight中未發現裝置的裝置解析規則。

不完整的裝置識別可能導致下列問題：

- 路徑不完整
- 未識別的多重路徑連線
- 無法將應用程式分組
- 拓撲視圖不準確
- 資料倉儲和報告中的資料不準確

「裝置解析度」功能（管理>*裝置解析度*）包含下列索引標籤、每個索引標籤在裝置解析度規劃和檢視結果中扮演著重要角色：

- 「FC identify」（FC識別）包含未透過自動裝置解析解決的光纖通道裝置WWN清單和連接埠資訊。此索引標籤也會識別已識別的裝置百分比。
- 「IP identify」（IP識別）包含存取CIFS共用和NFS共用的裝置清單、這些裝置無法透過自動裝置解析來識別。此索引標籤也會識別已識別的裝置百分比。
- 「自動解析規則」包含執行光纖通道裝置解析時所執行的規則清單。您可以建立這些規則來解析未識別的光纖通道裝置。
- 「偏好設定」提供組態選項、可讓您針對環境自訂裝置解析度。

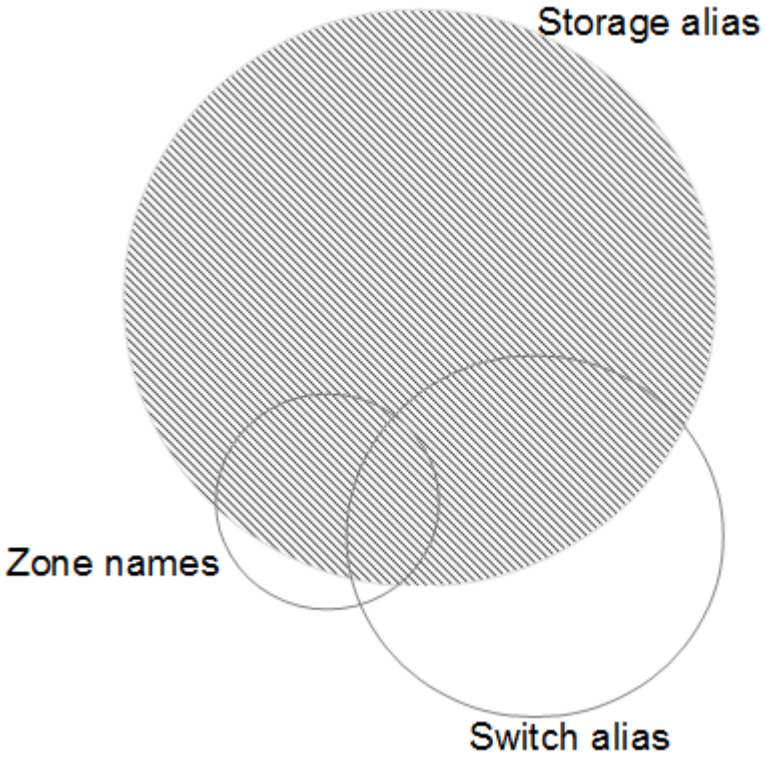
開始之前

在定義識別裝置的規則之前、您必須先瞭解環境的設定方式。您對環境的瞭解越多、識別裝置就越容易。

您需要回答類似下列的問題、以協助您建立正確的規則：

- 您的環境是否具有區域或主機的命名標準、其中有多少百分比是正確的？
- 您的環境是否使用交換器別名或儲存別名、而且它們是否與主機名稱相符？
- 您的環境是否使用SRM工具、您可以使用它來識別主機名稱？SRM提供哪些涵蓋範圍？
- 您環境中的命名配置多久會改變一次？
- 是否有任何併購或合併引進不同的命名方案？

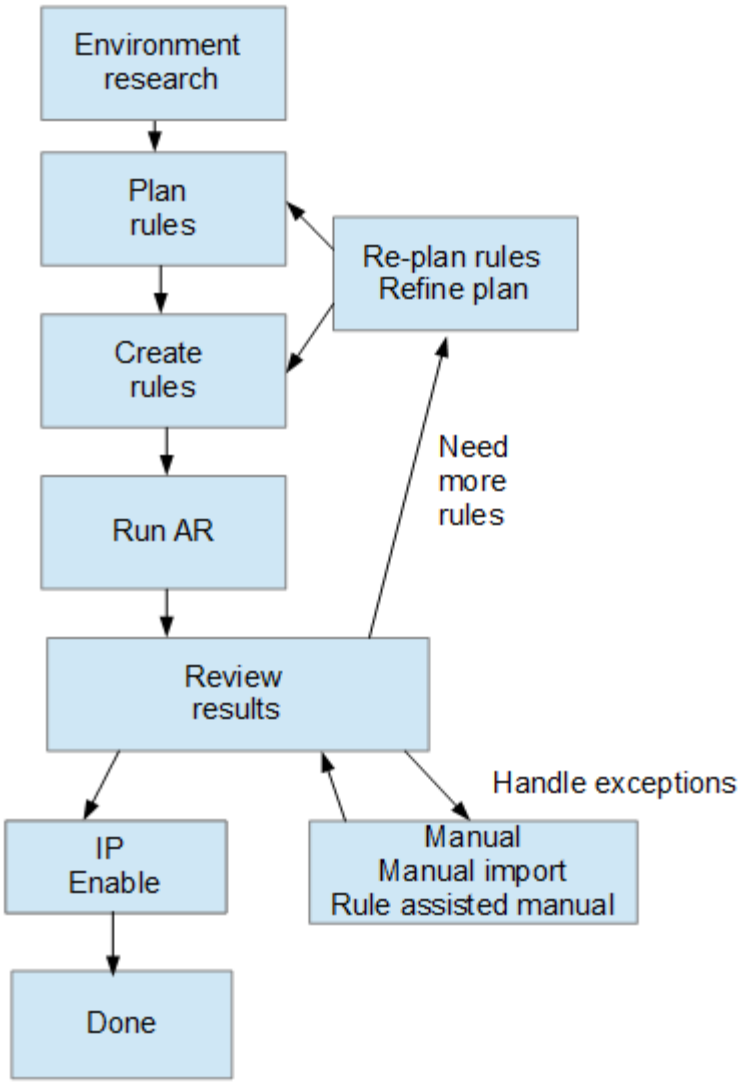
在分析環境之後、您應該能夠識別出哪些命名標準可以讓您預期在可靠性方面會遇到什麼問題。您收集到的資訊可能會以圖形呈現、如下圖所示：



在此範例中、儲存別名可可靠地代表最大數量的裝置。使用儲存別名識別主機的規則應先寫入、使用交換器別名的規則應在下一步寫入、最後建立的規則應使用區域別名。由於區域別名和交換器別名的使用重疊、部分儲存別名規則可能會識別其他裝置、因此區域別名和交換器別名所需的規則較少。

定義環境中裝置的步驟

一般而言、您會使用類似下列的工作流程來識別環境中的裝置。識別是一種迭代的程序、可能需要多個步驟來規劃和完善規則。



> 如果您的環境中有未識別的裝置（也稱為「未知」或一般裝置）、而您隨後設定了在輪詢時識別這些裝置的資料來源、則這些裝置將不再顯示或被視為一般裝置。

規劃環境的裝置解決規則

使用規則來識別環境中的裝置、通常是一種反覆的程序、需要徹底分析環境、並建立多個規則來識別盡可能多的裝置。最佳案例是設定目標、以識別環境中100%的裝置。

規則的最有效順序是先設定最嚴格的規則、導致大部分的項目不符合模式、而流程則是限制較少的規則。這可讓Insight在每個項目中套用更多模式、增加模式相符和主機識別正向的可能性。

建立規則時、您的目標應該是建立規則、以因應最多的未識別裝置。例如、建立遵循類似下列範圍模式的規則、會比建立30條涵蓋範圍百分比較低的規則更有效率：

規則	涵蓋範圍百分比
規則1.	60%

第2條	25%
規則3.	8%
第4條	4%
第5條	1%

建立裝置解決規則

您可以建立裝置解析規則、以識別OnCommand Insight 目前無法自動識別的主機、儲存設備和磁帶。您所建立的規則可識別環境中目前的裝置、並可識別新增至環境中的類似裝置。

關於這項工作

當您建立規則時、首先要識別規則執行的資訊來源、擷取資訊的方法、以及是否將DNS查詢套用至規則的結果。

用於識別裝置的來源
• 主機的SRM別名 • 包含內嵌主機或磁帶名稱的儲存別名 • 包含內嵌主機或磁帶名稱的交換器別名 • 包含內嵌主機名稱的區域名稱
從來源擷取裝置名稱的方法
• 原點（從SRM擷取名稱） • 分隔符號 • 規則運算式
DNS查詢
指定您是否使用DNS驗證主機名稱。

您可以在「自動解決規則」索引標籤中建立規則。下列步驟說明規則建立程序。

步驟

1. 按一下「管理>*裝置解析度*」
2. 在*自動解決規則*索引標籤中、按一下「**+**新增」

隨即顯示New Rule（新規則）畫面。

「新規則」畫面包含*？*圖示、提供建立規則運算式的說明和範例。

3. 在*類型*清單中、選取您要識別的裝置。

   您可以選取主機或磁帶。

4. 在*來源*清單中、選取您要用來識別主機的來源。

   根據您選擇的來源、Insight會顯示下列回應：

   - 區域列出Insight需要識別的區域和WWN。
   - SRM列出Insight需要識別的不明別名
   - 儲存別名列出需要Insight識別的儲存別名和WWN
   - 交換器別名列出Insight需要識別的交換器別名

5. 在「方法」清單中、選取您要用來識別主機的方法。

來源	方法
SRM	「as is」、「delimiters'」、「regular Expressions」
儲存別名	「刪除者」或「正則表達式」
交換器別名	「刪除者」或「正則表達式」
區域	「刪除者」或「正則表達式」

   - 使用「限制者」的規則需要分隔符號和主機名稱的最小長度。

     主機名稱的最小長度為Insight用於識別主機的字元數。Insight只會針對這麼長或更長的主機名稱執行DNS查詢。

     對於使用分隔符號的規則、輸入字串會以分隔符號標記、並會建立多個鄰近標記組合的主機名稱候選清單。然後將清單排序、從最大到最小。例如、對於vipsnq03_hba3_emc3_12ep0、清單會產生下列結果：

     - vipsnq03_hba3_emc3_12ep0
     - vipsnq03_hba3_emc3
     - hba3 emc3_12ep0
     - vipsnq03_hba3
     - emc3_12ep0
     - hba3_emc3
     - vipsnq03

        - 12ep0
        - emc3.
        - Hba3.
    - 使用「regular expression'」的規則需要規則運算式、格式和大小寫敏感度選擇。
6. 按一下 ▶ Run AR 若要執行所有規則、或按一下按鈕中的向下箭號、以執行您建立的規則（以及自上次完整執行AR之後所建立的任何其他規則）。

結果

規則執行的結果會顯示在FC識別索引標籤中。

開始自動更新裝置解析度

裝置解析度更新會認可自上次執行全自動裝置解析以來所新增的手動變更。執行更新只能用來提交及執行新的手動項目、以供裝置解析度組態使用。不會執行完整的裝置解析度執行。

步驟

1. 登入Insight Web UI。
2. 按一下「管理>*裝置解析度*」
3. 在*設備分辨率*屏幕中，單擊*運行AR*按鈕中的向下箭頭。
4. 按一下「更新」開始更新。

規則輔助手動識別

此功能適用於您想要執行特定規則或規則清單的特殊情況（無論是否需要一次性重新排序）、以解析未知主機、儲存設備及磁帶裝置或群組。

開始之前

您有許多尚未識別的裝置、也有多個規則可成功識別其他裝置。

關於這項工作

> 如果來源僅包含主機或裝置名稱的一部分、請使用規則運算式規則並加以格式化、以新增遺失的文字。

步驟

1. 登入OnCommand Insight 到The W不明 網路UI。
2. 按一下「管理>*裝置解析度*」
3. 按一下「* FC identi*」索引標籤。

   系統會顯示已識別和未識別的裝置。

4. 選取多個未識別的裝置。
5. 按一下*識別*>*設定主機解析度*或*>設定磁帶解析度*

   系統會顯示識別畫面、其中包含已成功識別裝置的所有規則清單。

6. 將規則順序變更為符合您需求的訂單。

   規則順序會在識別畫面中變更、但不會全域變更。

7. 選取符合您需求的方法。

   從最上層開始、執行主機解析程序的順序OnCommand Insight 。

   遇到適用的規則時、規則名稱會顯示在規則欄中、並標示為手動。

Fibre Channel裝置解析度

FC識別畫面會顯示光纖通道裝置的WWN和WWPN、這些裝置的主機尚未透過自動裝置解析來識別。此畫面也會顯示已手動解決裝置問題的所有裝置。

已手動解析的裝置狀態為「OK」、並識別用於識別裝置的規則。遺失的裝置狀態為「Unidentified」（未識別）。本頁列出識別裝置的總涵蓋範圍。

您可以在FC識別畫面左側選取多個裝置、以執行大量動作。將游標移到裝置上、然後選取清單最右側的識別或取消識別按鈕、即可在單一裝置上執行動作。

「Total overage（總涵蓋範圍）」連結會顯示您組態的「Number of devices identified / Number of devices Available（已識別的裝置數量/可用的裝置數量）」清單：

- SRM別名
- 儲存別名
- 交換器別名
- 區域
- 使用者定義

手動新增**Fibre Channel**裝置

您可以OnCommand Insight 使用「裝置解析度FC識別」索引標籤中的手動新增功能、將

光纖通道裝置手動新增至支援功能。此程序可用於預先識別預期未來會探索的裝置。

開始之前

若要成功將裝置識別新增至系統、您必須知道WWN或IP位址和裝置名稱。

關於這項工作

您可以手動新增主機、儲存設備、磁帶或未知的光纖通道裝置。

步驟

1. 登入Insight Web UI
2. 按一下「管理>*裝置解析度*」
3. 按一下「* FC identi*」索引標籤。
4. 按一下「新增」按鈕。

   隨即顯示Add Device（新增裝置）對話方塊

5. 輸入WWN或IP位址、裝置名稱、然後選取裝置類型。

結果

您輸入的裝置會新增至FC識別索引標籤中的裝置清單。「Rule」被識別為「Manual」（手動）。

從**CSV**檔案匯入**Fibre Channel**裝置識別

您可以使用OnCommand Insight CSV檔案中的裝置清單、將光纖通道裝置識別碼手動匯入到「物件解析」功能。

開始之前

您必須擁有正確格式的CSV檔案、才能將裝置識別碼直接匯入裝置解析度功能。適用於Fibre Channel裝置的CSV檔案需要下列資訊：

WWN
IP
名稱
類型

> 最佳實務做法是先將FC識別資訊匯出至CSV檔案、對該檔案進行所需的變更、然後再將檔案匯入FC識別。如此可確保預期的欄位以適當的順序出現。

若要匯入FC識別資訊：

步驟

1. 登入Insight Web UI。
2. 按一下「管理>*裝置解析度*」
3. 選取「* FC identify 」（ FC識別*）標籤。
4. 按一下*識別*>*識別檔案* .
   a. 瀏覽至包含您要匯入之CSV檔案的資料夾、然後選取所需的檔案。

   您輸入的裝置會新增至FC識別索引標籤中的裝置清單。「規則」被識別為「手動」。

將**Fibre Channel**裝置識別碼匯出至**CSV**檔案

您可以從OnCommand Insight 「無法分辨」功能將現有的Fibre Channel裝置識別碼匯出至CSV檔案。您可能想要匯出裝置識別碼、以便加以修改、然後再將其匯入Insight、然後再將其用於識別與原先與匯出識別碼相符的裝置。

關於這項工作

當裝置具有類似屬性、可在CSV檔案中輕鬆編輯、然後匯入系統時、可能會使用此案例。

當您將光纖通道裝置識別匯出至CSV檔案時、檔案會依照所示順序包含下列資訊：

WWN
IP
名稱
類型

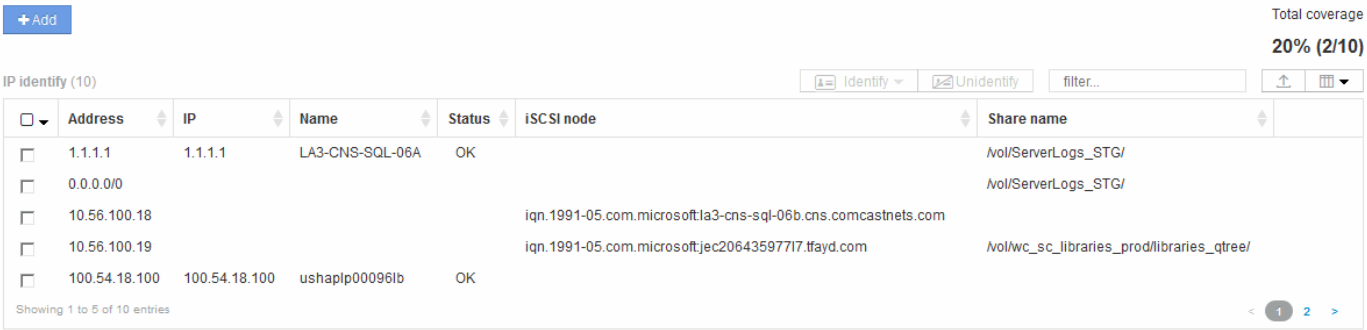
步驟

1. 登入Insight Web UI。
2. 按一下「管理>*裝置解析度*」
3. 選取「* FC identify 」（ FC識別*）標籤。
4. 選取您要匯出其識別碼的光纖通道裝置。
5. 按一下匯出 圖示。
6. 如果您要開啟CSV檔案或儲存檔案、請選擇此選項。

IP裝置解析度

IP識別畫面會顯示所有已透過自動裝置解析或手動裝置解析識別的iSCSI和CIFS或NFS共用。也會顯示未識別的裝置。此畫面包含裝置的IP位址、名稱、狀態、iSCSI節點和共用名

稱。也會顯示已成功識別的裝置百分比。



手動新增**IP**裝置

您可以OnCommand Insight 使用IP識別畫面中的手動新增功能、將IP裝置手動新增至支援功能。

步驟

1. 登入Insight Web UI。
2. 按一下「管理>*裝置解析度*」
3. 按一下「* IP識別*」索引標籤。
4. 按一下「新增」按鈕。

   隨即顯示Add Device（新增裝置）對話方塊

5. 輸入位址、IP位址和唯一的裝置名稱。

結果

您輸入的裝置會新增至「IP識別」索引標籤中的裝置清單。

從**CSV**檔案匯入**IP**裝置識別

您可以使用CSV檔案中的裝置識別清單、將IP裝置識別碼手動匯入「裝置解析度」功能。

開始之前

您必須擁有正確格式的CSV檔案、才能匯入裝置識別碼。IP裝置的CSV檔案需要下列資訊：

地址
IP
名稱

> 最佳實務做法是先將IP識別資訊匯出至CSV檔案、在該檔案中進行所需的變更、然後再將檔案匯入IP識別。如此可確保預期的欄位以適當的順序出現。

若要匯入IP識別資訊：

步驟

1. 登入Insight Web UI。
2. 按一下「管理>*裝置解析度*」
3. 選取「* IP識別*」索引標籤。
4. 按一下*識別*>*識別檔案* .
   a. 瀏覽至包含您要匯入之CSV檔案的資料夾、然後選取所需的檔案。

   您輸入的裝置會新增至「IP識別」索引標籤中的裝置清單。

將**IP**裝置識別匯出至**CSV**檔案

您可以使用裝置解析功能、從Insight匯出現有的IP裝置識別碼。您可能想要匯出裝置識別碼、以便加以修改、然後將其匯入Insight、以便用來識別與匯出識別碼類似的裝置。

關於這項工作

當您將IP裝置識別碼匯出至CSV檔案時、檔案會依照所示順序包含下列資訊：

地址
IP
名稱

步驟

1. 登入Insight Web UI。
2. 按一下「管理>*裝置解析度*」
3. 選取「* IP識別*」索引標籤。
4. 選取您要匯出識別碼的IP裝置。
5. 按一下匯出 ⬆ 圖示。
6. 如果您要開啟CSV檔案或儲存檔案、請選擇此選項。

設定選項

裝置解析偏好選項索引標籤可讓您建立自動解析排程、指定儲存設備和磁帶供應商以納入或排除識別、以及設定DNS查詢選項。

自動解決排程

自動解決排程可指定何時執行自動裝置解決方案：

選項	說明
每個	使用此選項可在天數、小時數或分鐘的時間間隔內執行自動裝置解析。
每天	使用此選項可在特定時間每天執行自動裝置解析。
手動	使用此選項只能手動執行自動裝置解析。
每個環境都會發生變化	使用此選項可在環境發生變更時執行自動裝置解析。

如果您手動指定、夜間自動裝置解析功能將會停用。

DNS處理選項

DNS處理選項可讓您選取下列功能：

- 啟用DNS查詢結果處理時、您可以新增DNS名稱清單以附加至已解析的裝置。
- 您可以選取「IP的自動解析：」、以便使用DNS查詢功能、自動為存取NFS共用的iSCSI啟動器和主機解析主機。如果未指定此選項、則只會執行FC型解析度。
- 您可以選擇允許在主機名稱中使用底線、並使用「已連線至」別名、而非結果中的標準連接埠別名。

包括或排除特定的儲存設備和磁帶廠商

您可以納入或排除特定的儲存設備和磁帶廠商、以便自動解決。例如、如果您知道某個特定主機將成為舊主機、而且應該排除在新環境之外、您可能會想排除特定廠商。您也可以重新新增先前排除但不再想排除的廠商。

磁帶的裝置解決規則僅適用於WWN、其中WWN廠商的偏好設定為*僅限磁帶*。

規則運算式範例

如果您已選擇規則運算式方法作為來源命名策略、則可使用規則運算式範例作為OnCommand Insight 參考指南、以供您在自動解析方法中使用自己的運算式。

格式化規則運算式

建立用於OnCommand Insight 自動解析的規則運算式時、您可以在名為的欄位中輸入值來設定輸出格式 `FORMAT`。

預設設定為 `\1`這表示符合規則運算式的區域名稱會被正規表示式所建立的第一個變數內容所取代。在規則運算式中、變數值是由插入的實質陳述式所建立。如果出現多個實質陳述式、則會以數字方式從左到右參照變數。這些變數可依任何順序在輸出格式中使用。您也可以將固定文字新增至、將其插入輸出中 `FORMAT` 欄位。

例如、此區域命名慣例可能有下列區域名稱：

```
[Zone number]_[data center]_[hostname]_[device type]_[interface number]
```

- S121_Miami主機名1_filer_FC1
- S14_Tampa_hostname2_switch_FC4
- S3291_波士頓 主機名3_windows2K_FC0
- S44_Raleigh_hostname4_solaris _FC1

您可能希望輸出採用下列格式：

```
        [hostname]-[data center]-[device type]
```

為達成此目的、您需要擷取變數中的主機名稱、資料中心和裝置類型欄位、並在輸出中使用這些欄位。下列規則運算式會執行此動作：

```
.*?_([a-zA-Z0-9]+)_([a-zA-Z0-9]+)_([a-zA-Z0-9]+)_.*
```

因為有三組括弧、所以這些變數 `\1`、 `\2` 和 `\3` 將會填入。

然後您可以使用下列格式接收偏好的輸出格式：

```
\2-\1-\3
```

您的輸出內容如下：

```
hostname1-Miami-filer
hostname2-Tampa-switch
hostname3-Boston-windows2K
hostname4-Raleigh-solaris
```

變數之間的連字號可提供插入格式化輸出中的固定文字範例。

範例**1**顯示區域名稱

在此範例中、您可以使用規則運算式從區域名稱擷取主機名稱。如果您有類似於下列區域名稱的內容、可以建立規則運算式：

- S0032_myComputer1Name-HBA0
- S0434_myComputer1Name-HBA1
- S0432_myComputer1Name-HBA3

您可以用來擷取主機名稱的規則運算式如下：

```
S[0-9]+_([a-zA-Z0-9]*)[_-]HBA[0-9]
```

結果會比對所有以S開頭的區域、然後是任何數字組合、接著是底線、英數字元主機名稱（myComputer1Name）、底線或連字號、大寫字母HBA和單一數字（0-9）。單一主機名稱就會儲存在*\1*變數中。

規則運算式可細分為其元件：

- 「s」代表區域名稱、並開始運算式。這只會比對區域名稱開頭的「S」。
- 方括弧中的字元[0-9]表示「S」後面的數字必須介於0到9之間（含）。
- +號表示前方括弧中的資訊必須存在1次以上。
- _（底線）表示S後的數字必須緊接著區域名稱中的底線字元。在此範例中、區域命名慣例會使用底線來分隔區域名稱與主機名稱。
- 在所需的底線之後、括弧會指出內含的模式將儲存在\1變數中。
- 方括弧內的字元[A-zA-Z0-9]表示要比對的字元為所有字母（不論大小寫）和數字。
- 方括弧後面的*（星號）表示方括弧內的字元出現0次以上。
- 方括弧內的字元[_-]（底線和破折號）表示字母數字型式必須後面加上底線或破折號。
- 規則運算式中的字母HBA表示區域名稱中必須有此確切的字元順序。
- 最後一組方括弧內的字元[0-9]會比對從0到9（含）的單一位數。

範例 **2.**

在此範例中、跳到第一個底線「」、然後比對*E*及其後的所有項目、直到第二個「」、然後跳過之後的所有項目。

區域： `Z_E2FHDBS01_E1NETAPP`

主機名稱： `E2FHDBS01`

- RegExp:* `.?(E.?).*?`

範例**3.**

正則運算式（下方）最後一節的括弧「（）」可識別哪個部分是主機名稱。如果您想要VSAN3做為主機名稱、應該是：_（[A-zA-Z0-9]）。*

區域： `A_VSAN3_SR48KENT_A_CX2578_SPA0`

主機名稱： `SR48KENT`

- RegExp:* `_[a-zA-Z0-9]+_([a-zA-Z0-9]).*`

範例**4**顯示較複雜的命名模式

如果您有類似於下列區域名稱的內容、可以建立規則運算式：

- myComputerName123-HBA1_Symm1_FA3
- myComputerName123-HBA2_Symm1_FA5
- myComputerName123-HBA3_Symm1_FA7

您可以用來擷取這些資料的規則運算式如下：

```
([a-zA-Z0-9]*)_.*
```

。 `\1` 變數僅包含 `myComputerName123` 使用此運算式進行評估之後。

規則運算式可細分為其元件：

- 括弧表示內含的模式將儲存在\1變數中。
- 方括弧內的字元[A-zA-Z0-9]表示任何字母（不論大小寫）或數字都會相符。
- 方括弧後面的*（星號）表示方括弧內的字元出現0次以上。
- 規則運算式中的_（底線）字元表示區域名稱必須在字母數字字串後面加上底線、且前面的方括弧必須相符。
- 。（句點）符合任何字元（萬用字元）。
- *（星號）表示前一個句點的萬用字元可能出現0次以上。

  也就是說、組合.*代表任何字元、任意次數。

範例**5**顯示不含模式的區域名稱

如果您有類似於下列區域名稱的內容、可以建立規則運算式：

- myComputerName_HBA1_Symm1_FA1
- myComputerName123_HBA1_Symm1_FA1

您可以用來擷取這些資料的規則運算式如下：

```
(.*?)_.*
```

1變數會包含_myComputerName_（在第一個區域名稱範例中）或_myComputerName123_（在第二個區域名稱範例中）。因此、此規則運算式會比對第一個底線之前的所有項目。

規則運算式可細分為其元件：

- 括弧表示內含的模式將儲存在\1變數中。
- .*（句點星號）會比對任何字元、任意次數。
- 方括弧後面的*（星號）表示方括弧內的字元出現0次以上。
- ？字元可讓比對變得無貪度。這迫使它在第一個底線而非最後一個底線停止比對。
- 字元_.*符合找到的第一個底線及其後的所有字元。

範例**6**顯示具有模式的電腦名稱

如果您有類似於下列區域名稱的內容、可以建立規則運算式：

- storage1_Switch1_myComputerName123A_A1_FC1
- Storage2_Switch2_myComputerName123B_A2_FC2
- Storage3_Switch3_myComputerName123T_A3_FC3

您可以用來擷取這些資料的規則運算式如下：

```
.*?_.*?_([a-zA-Z0-9]*[ABT])_.*
```

由於區域命名慣例具有更多的模式、因此我們可以使用上述運算式、將主機名稱（範例中為myComputerName）的所有執行個體、以A、A B或T結尾、並將該主機名稱置於\1變數中。

規則運算式可細分為其元件：

- .*（句點星號）會比對任何字元、任意次數。
- ？字元可讓比對變得無貪度。這迫使它在第一個底線而非最後一個底線停止比對。
- 底線字元符合區域名稱中的第一個底線。
- 因此、第一個.*?組合會符合第一個區域名稱範例中的字元*_storage1_*。
- 第二個.*？_組合的行為與第一個區域的名稱範例類似、但與_Switch1__相符。
- 括弧表示內含的模式將儲存在\1變數中。
- 方括弧內的字元[A-zA-Z0-9]表示任何字母（不論大小寫）或數字都會相符。
- 方括弧後面的*（星號）表示方括弧內的字元出現0次以上。
- 規則運算式[ABT]中的方括弧字元會比對區域名稱中必須為A、B或T的單一字元
- 括弧後面的_（底線）表示必須在[ABT]字元相符之後加上底線。
- .*（句點星號）會比對任何字元、任意次數。

因此、此結果會導致\1變數包含下列任何英數字元字串：

- 前面有一些英數字元和兩個底線
- 後面加上底線（然後是任意數量的英數字元）
- 在第三個底線之前、有A、B或T的最終字元。

範例**7.**

區域：`myComputerName123_HBA1_Symm1_FA1`

主機名稱：`myComputerName123`

- RegExp:* `([a-zA-Z0-9]+)_.*`

範例**8.**

此範例會找出第一個_之前的所有項目。

區域： `MyComputerName_HBA1_Symm1_FA1`

`MyComputerName123_HBA1_Symm1_FA1`

主機名稱： `MyComputerName`

- RegExp:* `(.?)_.`

範例**9.**

此範例會找出第1 個之後的所有項目、直到第二個。

區域： `Z_MyComputerName_StorageName`

主機名稱： `MyComputerName`

- RegExp:* `.?(.?).*?`

範例**10.**

此範例從區域範例中擷取「MyComputerName123」。

區域： `Storage1_Switch1_MyComputerName123A_A1_FC1`

`Storage2_Switch2_MyComputerName123B_A2_FC2`

`Storage3_Switch3_MyComputerName123T_A3_FC3`

主機名稱： `MyComputerName123`

- RegExp:* `.?.?([a-zA-Z0-9]+)[ABT]_.`

範例**11.**

區域： `Storage1_Switch1_MyComputerName123A_A1_FC1`

主機名稱： `MyComputerName123A`

- RegExp:* `.?.?([a-zA-z0-9]+).*?`

範例**12**

｛caret｝（cinserflext或caret）*內部方括弧*會否定運算式、例如、[｛caret｝FF]表示大寫或小寫F以外的任何項目、而[｛caret｝A-z]則表示除小寫a到z以外的所有項目、在上述情況下則為_以外的任何項目。format陳述式會在輸出主機名稱中加入"-"。

區域： `mhs_apps44_d_A_10a0_0429`

主機名稱： `mhs-apps44-d`

- RegExp:* `([^_])_([AB]).*`+格式OnCommand Insight ：

`([^_])_().*`格式OnCommand Insight ：

範例**13**

在此範例中、儲存別名以「\」分隔、運算式需要使用「\」來定義字串中實際使用的是「\」、而這些不是運算式本身的一部分。

儲存別名： `\Hosts\E2DOC01C1\E2DOC01N1`

主機名稱： `E2DOC01N1`

- RegExp:* `\\.?\\.?\\(.*?)`

範例**14**

此範例從區域範例中擷取「PD-RV-W-AD-2」。

區域： `PD_D-PD-RV-W-AD-2_01`

主機名稱： `PD-RV-W-AD-2`

- RegExp:* `[^-]-(.-\d+).+`

範例**15**

在此案例中的格式設定會將「US-BV-」新增至主機名稱。

區域： `SRV_USBVM11_F1`

主機名稱： `US-BV-M11`

- RegExp:* `SRV_USBV([A-Za-z0-9]+)_F[12]`

格式： `US-BV-\1`

維持洞見

無論您是Insight新手、需要設定新系統、或是系統已運作一段時間、您都必須採取步驟來維持Insight和網路的順暢運作。主要的維護概念是、在Insight中通常需要調整網路的變更。

以下是最常見的維護工作：

- 維護Insight備份
- 正在更新過期的Insight授權

- 協調資料來源修補程式
- 更新所有擷取單位的Insight版本
- 從Insight刪除移除的資料來源

管理Insight

此功能可監控您的環境、讓您在報告危機之前就能研究潛在問題OnCommand Insight 。資產儀表板提供摘要圓形圖、IOPS熱圖、以及前10大使用儲存資源池的互動式圖表。

步驟

1. 開啟Insight資產儀表板*、並將游標移到圓形圖上、以查看這三個圖表中的資產分配：
   - 「容量（依廠商）」會顯示各廠商的儲存總原始容量。
   - 「容量（依層級）」顯示每個儲存層的總可用容量。
   - 「交換器連接埠」圓形圖顯示連接埠製造商、並顯示使用的連接埠百分比。
2. 檢視*環境相關資料*以查看環境的已用容量、容量效率、已用FC資源及虛擬基礎架構統計資料。
3. 將游標放在*前10大使用資源池*圖表中的儲存資源池列上、以檢視儲存資源池的已使用和未使用容量。
4. 按一下* Storage IOP*熱圖中以大文字顯示的任何資產名稱（表示該資產有問題）、即可顯示摘要說明該資產目前狀態的頁面。
5. 在*資產儀表板*右下角、按一下*虛擬機器IOP*熱圖中以大文字顯示的任何資產名稱（表示資產有問題）、即可顯示摘要說明資產目前狀態的頁面。
6. 在Insight工具列上、按一下*管理*。
7. 請注意任何顯示純紅色圓圈的區域。

   在「視覺」UI中OnCommand 、潛在的問題會以紅色圓圈標示。

8. 按一下*資料來源*以檢查所有受監控資料來源的清單。

   使用*狀態*欄檢查任何資料來源、其中含有紅色圓圈的訊息、且*影響*列示為高或中。這些都在表格頂端。這些資料來源的問題會影響網路中相當大的一部分、您需要解決這些問題。

9. 按一下「擷取單位」以記錄執行Insight的每個IP位址狀態、並視需要重新啟動擷取單位
10. 按一下「健全狀況」以查看Insight伺服器的高層執行個體監控。

監控OnCommand Insight 系統健全狀況

您應該定期查看健全狀況頁面、查看Insight系統元件的目前狀態、該頁面會顯示每個元件的狀態、並在發生問題時發出警示。

步驟

1. 登入InsightWeb UI。
2. 按一下「管理」、然後選取「健全狀況」。

隨即顯示「健全狀況」頁面。

3. 在「詳細資料」欄中、檢視特別注意任何注意狀態的元件目前狀態摘要、此欄前面會出現一個紅色圓圈、指出需要您立即注意的問題。

「健全狀況」頁面會根據您的系統組態、顯示下列任何或所有Insight元件的相關資訊：

元件	測試	詳細資料	顯示
併購	庫存資料處理	本地擷取單位的狀態	如果並行輪詢資料來源數量少於執行集區上限的75%（預設上限為30）、則會顯示「OK」（確定）。若使用量大於75%、則「擷取作業正忙」、並建議增加輪詢時間間隔或新增更多遠端擷取單位。
DWH	備份	資料倉儲排程備份的狀態	若啟用DWH排程備份、「OK」和上次成功的DWH備份時間。否則、會顯示任何發現錯誤的相關資訊。
DWH	ETL	資料倉儲ETL狀態	如果沒有錯誤、「OK」和上次成功的DWH建置時間。否則、會顯示任何發現錯誤的相關資訊。
伺服器	ASUP	ASUP狀態	「已啟用ASUP」、以及上次成功的在家時間（若有）。如果已啟用電話主選項、但遇到問題、則會顯示「ASUP故障」。 +"備份目錄無效"。 +顯示上次成功的電話回覆時間、以及上次失敗嘗試的時間（若有）。 +「ASUP已停用」（如果電話主選項已停用）。

伺服器	自動解析	自動裝置解析狀態	如果沒有錯誤、請選擇「OK」。如果識別錯誤導致無法解決問題、則會出現「Auto resolution is blocked」（自動解決已遭封鎖）。 +「低成功率」、如果能識別出低於75%的一般裝置。
伺服器	彈性搜尋	彈性搜尋資料儲存區的狀態	如果沒有錯誤、請選擇「OK」。如果無法連線至彈性搜尋服務、則「服務無法使用」。 +「偵測到叢集模式」（如果偵測到多個節點）。 +"高記憶體使用率"（如果使用的堆空間超過85%）。 +"狀態：紅色"表示彈性搜尋報告的錯誤。顯示錯誤的相關資訊、並建議聯絡客戶支援部門。
伺服器	CPU	深入瞭解CPU使用率	如果CPU負載低於65%、則為「OK」。「系統CPU負載很高。減少CPU負載。」 如果CPU負載大於65%。
伺服器	磁碟空間	磁碟空間狀態	釋放磁碟空間、Insight使用中的磁碟空間、以及Insight所保留的建議磁碟空間。如果磁碟使用率超過80%、則會顯示「低磁碟空間」。
伺服器	事件匯流排	事件匯流排的狀態	如果事件匯流排佇列為空白、則「'EventBus is Empty'」（事件匯流排為空白）、否則會顯示事件匯流排佇列的狀態。

伺服器	庫存資料處理	Insight伺服器庫存資料處理功能的狀態	若Insight伺服器不忙碌、則為「OK」。如果伺服器在最後一個小時內至少有75%的時間處於忙碌狀態、則會顯示「伺服器忙碌中」。建議不要新增更多資料來源、並建議將環境分割至多個伺服器。
伺服器	MySQL	MySQL資料庫的狀態	若未偵測到問題、則為「OK」。「資料庫的效能問題。有些查詢的執行時間過長」（如果查詢速度緩慢超過5%）。 +「資料庫記錄檔在<size> 過去一小時成長超過了不只是單純的資料而已。如果錯誤日誌增長到20 KB以上、請查看MySQL記錄檔。
伺服器	效能歸檔	效能歸檔的狀態	「效能歸檔已啟用」或「效能歸檔未啟用」。
伺服器	實體記憶體	實體記憶體的狀態	如果記憶體使用率低於85%、則為「OK」。「我的使用量很高、如果記憶體使用率超過85%、則可減少整體記憶體佔用空間、以確保系統穩定性。
伺服器	Service Pack	Service Pack可用度	顯示Service Pack是否可供Insight使用。如果有可用的Service Pack、則會顯示指示。
伺服器	使用資訊	傳送使用資訊的狀態	顯示是否已啟用或停用傳送使用資訊給NetApp。建議停用時啟用。顯示上次嘗試或上次成功的傳送時間。 +顯示所遇到問題的相關資訊。

伺服器	違規	未處理違規的狀態	若未處理的違規數量少於違規上限的75%、則為「OK」。如果未處理的違規數量超過違規上限的75%、則「允許的最大未決違規數是<number>指不允許的數量。」建議檢閱效能原則組態。 +「違規管理程式已封鎖」（如果未處理的違規數量達到違規上限）。 +請注意、違規管理程式無法建立新的違規、建議您檢閱效能原則組態。
伺服器	每週備份	每週備份狀態	如果啟用每週備份、「'OK'」會顯示「每週備份未啟用」。

刪除非使用中的裝置

刪除非作用中的裝置、有助於保持資料更乾淨、更容易瀏覽。

關於這項工作

若要從Insight刪除非使用中的裝置、請執行下列步驟：

步驟

1. 建立新查詢或開啟現有查詢。
2. 選擇_通用設備_、*host*、_storage _、_switch_或_tape _資產類型。
3. 新增*為作用中*的篩選條件、並將篩選條件設為*否*。

   結果表僅顯示未啟用的資產。

4. 選取您要刪除的裝置。
5. 按一下「動作」按鈕、然後選取「刪除非使用中的裝置」。

   您的非使用中裝置將會刪除、而不會再顯示在Insight中。

稽核系統與使用者活動

如果您想找到非預期的變更、可以檢視OnCommand Insight 有關該系統及其使用者活動的稽核記錄。除了顯示在「稽核」頁面之外、您也可以選擇將稽核記錄訊息傳送至syslog。

關於這項工作

Insight會針對任何影響儲存網路或其管理的使用者活動、產生稽核項目、包括：

- 登入
- 授權或取消授權路徑
- 更新授權路徑
- 設定全域原則或臨界值
- 新增或移除資料來源
- 啟動或停止資料來源
- 正在更新資料來源內容
- 新增、編輯或刪除工作
- 移除應用程式群組
- 識別或變更裝置的識別碼
- 建立使用者
- 刪除使用者
- 使用者角色變更
- 修改使用者（訪客 à 管理）
- 登出使用者（強制登出或手動登出）
- 刪除擷取單位
- 更新授權
- 正在啟用備份
- 正在停用備份
- 啟用ASUP（稽核記錄中會報告啟用同一頁的Proxy）
- 停用ASUP（稽核記錄中會報告在同一頁上停用Proxy）
- 安全性-重新輸入、變更系統密碼。
- 移除/新增資產附註
- CAC使用者登入/登出
- CAC使用者工作階段逾時

步驟

1. 在瀏覽器中開啟Insight。
2. 按一下「管理」、然後選取「稽核」。

   「稽核」頁面會在表格中顯示稽核項目。

3. 您可以在表格中檢視下列詳細資料：

- 時間

  進行變更的日期和時間

- 使用者

  與稽核項目相關聯的使用者名稱

- 角色

  使用者帳戶的角色、即來賓、使用者或系統管理員

- * IP*

  與稽核項目相關的IP位址

- 行動

  稽核項目中的活動類型

- 詳細資料

  稽核項目的詳細資料

  如果有使用者活動會影響資源、例如資料來源或應用程式、則詳細資料會包含資源登陸頁面的連結。

> 刪除資料來源時、與資料來源相關的使用者活動詳細資料將不再包含資料來源登陸頁面的連結。

4. 您可以選擇特定的期間（1小時、3小時、24小時、3天及7天）來顯示稽核項目、 Insight顯示所選期間最多1000次違規事件。

   如果資料超過單一頁面大小、您可以按一下表格下方的頁碼、逐頁瀏覽資料。

5. 您可以按一下欄標題中的箭號、將表格中欄的排序順序變更為遞增（向上箭頭）或遞減（向下箭頭）；若要回到預設的排序順序、請按一下任何其他欄標題。

   依預設、表格會以遞減順序顯示項目。

6. 您可以使用*篩選器*方塊、僅顯示您要在表格中顯示的項目。

   僅查看使用者的稽核項目 `izzyk`，鍵入 `izzyk` 在*篩選器*方塊中。

監控網路中的違規行為

當Insight因為效能原則中設定的臨界值而產生違規時、您可以使用違規儀表板來檢視違規。儀表板會列出網路中發生的所有違規事件、並可讓您找出問題並加以解決。

步驟

1. 在OnCommand Insight 瀏覽器中開啟

2. 在Insight工具列上、按一下*儀表板*、然後選取*違規儀表板*。

   隨即顯示違規儀表板。

3. 您可以使用*違反原則*的圓形圖、如下所示：
   - 您可以將游標放在圖表的任一片段上、以顯示特定原則或度量發生的違規總數百分比。
   - 您可以按一下圖表的某個部分來「放大」、如此一來、您就能將該分割區從圖表的其餘部分移開、以更仔細地強調及研究該分割區。
   - 您可以按一下 圖示、以全螢幕模式顯示圓形圖、然後按一下 再次將圓形圖最小化。圓形圖最多可包含五個分區、因此、如果您有六個產生違規的原則、Insight會將第五和第六個分區合併成「其他」分區。Insight會將最常發生的違規指派給第一層、第二層違規事件最多、依此類推。
4. 您可以使用*違反歷史記錄*圖表的下列方式：
   - 您可以將游標放在圖表上、以顯示特定時間發生的違規總數、以及每個指定度量總計中發生的次數。
   - 您可以按一下圖例標籤、從圖表中移除與圖例相關的資料。

     按一下圖例即可再次顯示資料。

   - 您可以按一下 圖示、以全螢幕模式顯示圖表、然後按一下 再次將圓形圖最小化。
5. 您可以使用*違規表*的方式如下：
   - 您可以按一下 圖示、以全螢幕模式顯示表格、然後按一下 再次將圓形圖最小化。

     如果您的視窗大小太小、則違規表格只會顯示三欄；不過、當您按一下時 、其他欄（最多七欄）會顯示。

   - 您可以顯示特定期間內的違規情況（* 1h*、* 3h*、* 24h*、* 3d*、* 7d*、 和* 30d*）、其中Insight顯示所選期間的違規上限為1000次。
   - 您可以使用*篩選器*方塊、僅顯示您想要的違規。
   - 您可以按一下欄標題中的箭號、將表格中欄的排序順序變更為遞增（向上箭頭）或遞減（向下箭頭）；若要回到預設的排序順序、請按一下任何其他欄標題。

     依預設、表格會以遞減順序顯示違規。

   - 您可以在ID欄中按一下違規、以顯示違規期間的資產頁面。
   - 您可以按一下「Description（說明）」欄中的資源連結（例如儲存資源池和儲存磁碟區）、以顯示與這些資源相關的資產頁面。
   - 您可以按一下「原則」欄中的效能原則連結、以顯示「編輯原則」對話方塊。

     如果您認為某個原則產生的違規數太少或太多、您可能會想要調整該原則的臨界值。

   - 如果資料超過單一頁面大小、您可以按一下頁碼、逐頁瀏覽資料。
   - 您可以按一下 以解除違規。

擷取單位狀態

擷取單位畫面提供您所有擷取單位的檢視、包括狀態和任何錯誤。

連線至伺服器的Insight採購單位狀態會顯示在*管理*>*擷取單位*表格中。下表顯示每個擷取單位的下列資訊：

- 名稱
- * IP*
- *狀態*是擷取單位的作業狀態。
- 上一次報告的資料來源是上次報告給擷取單位的時間。
- *附註*顯示使用者輸入的AU相關附註。

如果清單中的擷取單位有問題、「狀態」欄位會顯示一個紅色圓圈、並提供有關問題的簡短資訊。您應該調查任何擷取設備問題、因為這些問題可能會影響資料收集。

若要重新啟動擷取單位、請將游標移到單位上、然後按一下出現的「重新啟動擷取單位」按鈕。

若要新增文字附註、請將游標暫留在擷取單位上、然後按一下出現的「*Add note _*（新增附註）」按鈕。只會顯示最近輸入的附註。

還原**Insight**資料庫

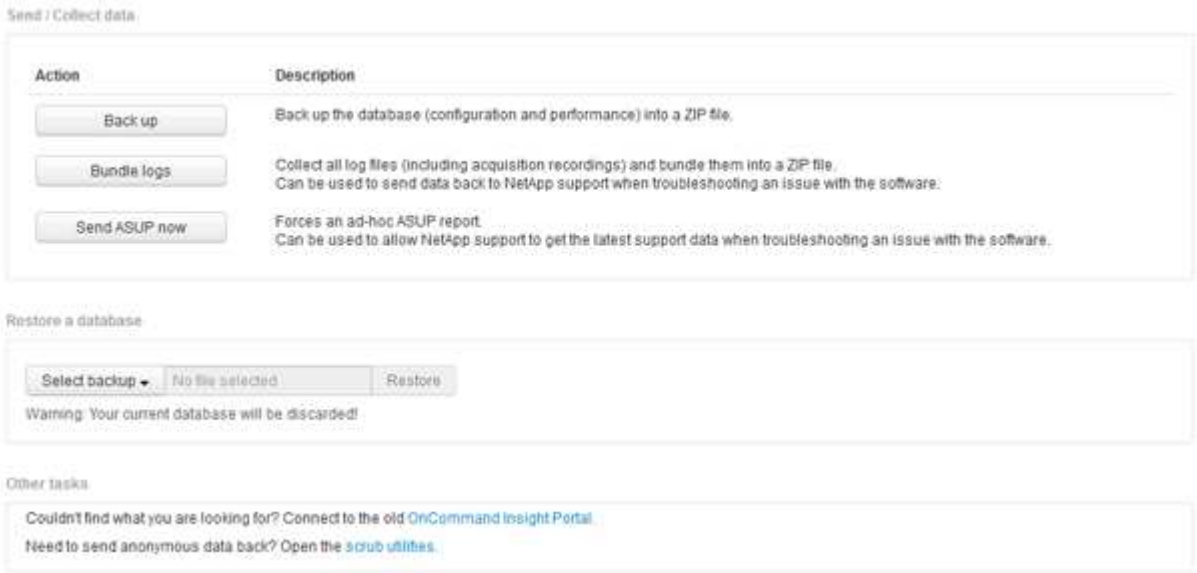
若要從通過驗證的備份檔案還原Insight資料庫、請使用疑難排解選項。這項作業完全取代您目前OnCommand Insight 的各項資料。

開始之前

最佳實務做法：**在還原OnCommand Insight 您的還原資料庫之前、請先使用手動備份程序來建立目前資料庫的複本。請檢查您打算還原的備份檔案、確定備份成功、其中包含您要還原的檔案。

步驟

1. 在Insight工具列上、按一下*管理*。
2. 按一下*疑難排解*。



3. 在「還原資料庫」區段中、從*選取備份*功能表中選取您要還原的備份檔案。

4. 按一下 * 還原 * 。
5. 在「所有資料都會被取代」的警告上、按一下「確定」

   還原活動的狀態會顯示在還原頁面上。

正在更新過期的授權

如果一個或多個Insight授權過期、您可以使用與原先安裝授權相同的程序來快速更新授權。

步驟

1. 在文字編輯器（例如「記事本」）中、開啟您從NetApp Support收到的新授權檔案、然後將授權金鑰文字複製到Windows剪貼簿。
2. 在OnCommand Insight 瀏覽器中開啟
3. 按一下工具列上的*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。

   此作業會將您的新授權新增至任何目前使用中的Insight授權。

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「使用率」區段中的「啟用傳送使用資訊給**NetApp**」方塊。您的環境必須正確設定並啟用Proxy。

授權不再符合法規要求

如果您在Insight授權頁面上看到「不合規」訊息、則Insight的管理TB數將超過貴公司授權的TB數。

「不合規」的訊息代表貴公司所支付的TB數低於Insight目前所管理的TB數。託管TB與授權TB數之間的差異會顯示在非法規遵循訊息旁。

Insight系統的運作不受影響、但您應聯絡NetApp代表以增加授權範圍並更新適當的授權。

取代舊版**Insight**的授權

如果您購買的新Insight版本與舊版產品不相容、則必須以新授權取代舊版授權。

安裝新授權時、您必須先選取*取代*作業、然後再儲存授權金鑰文字。

套用**Service Pack**

定期提供Service Pack、您可以申請使用這些Service Pack來修復OnCommand Insight 及增強功能。

開始之前

- 您必須已下載Service Pack檔案（例如、 `7.2service_pack_1.patch`）從NOW站點開始。
- 您必須已核准所有修補程式。

步驟

1. 在Insight工具列上、按一下*管理*。
2. 按一下*修補程式*。
3. 從「動作」按鈕選取*「套用修補程式」*。
4. 在「套用資料來源修補程式」對話方塊中、按一下「瀏覽」以找出Service Pack檔案。
5. 請查看*修補程式名稱*、說明、受影響的資料來源類型、其中顯示是否有任何資料來源受到影響、以及*詳細資料*、其中說明Service Pack所含的增強功能。
6. 如果選取的Service Pack正確、請按一下*套用修補程式*。

   Service Pack會自動核准、不需要採取進一步行動。

準備特殊的疑難排解報告

Insight會透過安裝軟體後所設定的ASUP系統、自動將資訊傳送給NetApp客戶支援部門。不過、您可能想要建立疑難排解報告、並向支援團隊開啟特定問題的案例。

您可以使用Insight中的工具來執行手動Insight備份、將記錄套用、然後將該資訊傳送給NetApp客戶支援部門。

手動備份**OnCommand Insight** 支援資料庫

如果您啟用OnCommand Insight 每週的還原資料庫備份、您會自動產生複本、以便在必要時還原資料庫。如果您需要在還原作業之前建立備份、或是傳送給NetApp技術支援以尋求協助、您可以建立備份 `.zip` 手動檔案。

步驟

1. 在Insight工具列上、按一下*管理*。
2. 按一下*疑難排解*。
3. 在「傳送/收集資料」區段中、按一下「備份」。
4. 按一下*儲存檔案*。
5. 按一下「確定」。

將記錄套用以取得支援

疑難排解Insight軟體的問題時、您可以快速產生記錄的壓縮檔（使用「gz」格式）、並將擷取記錄傳送給NetApp客戶支援。

步驟

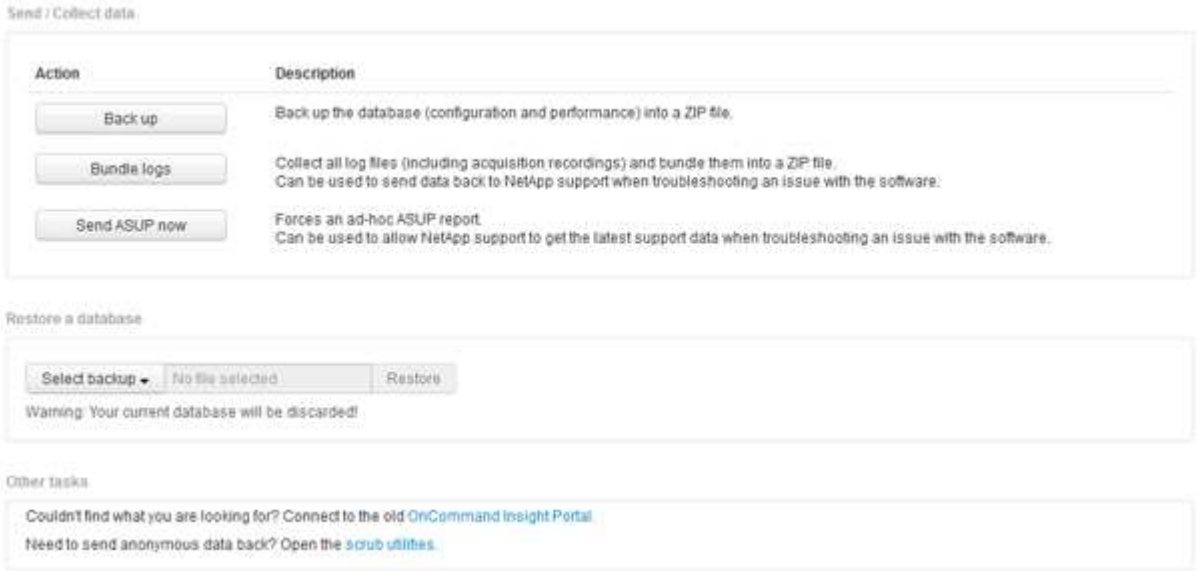
1. 在Insight工具列上、按一下*管理*。
2. 按一下*疑難排解*。
3. 在「傳送/收集資料」區段中、按一下「產品組合記錄」。
4. 按一下*儲存檔案*。
5. 按一下「確定」。

傳送資訊給**NetApp**支援部門

NetApp自動化支援（ASUP）機構會將疑難排解資訊直接傳送給NetApp客戶支援團隊。您可以強制傳送特殊報告。

步驟

1. 在Insight工具列上、按一下*管理*。
2. 按一下*設定*。
3. 單擊*備份/ASUP*選項卡。
4. 在「傳送/收集資料」區域中、按一下*「立即傳送ASUP」*、將您的記錄、錄音及備份提交給NetApp支援部門。



資料清理、以便傳輸至支援部門

擁有安全環境的客戶需要與NetApp客戶服務部門溝通、以便在不影響資料庫資訊的情況下疑難排解所產生的問題。利用此功能、您可以OnCommand Insight 設定完整的關鍵字與模

式字典、以便「清除」敏感資料、並將清理的檔案傳送給客戶支援部門。

步驟

1. 在Web UI中、按一下「管理」、然後選取「疑難排解」。
2. 在頁面底部的「其他工作」區域中、按一下「清理公用程式」連結。

   有幾個清理區段：在「Dictionary」、「清理資料」及「建置dictionary」、「Custom keywords」及「Regular Expressions」中查詢。

.

+ .. 在「**在目錄中查詢」區段中、輸入要顯示其所取代值的程式碼、或輸入值以查看取代該程式碼的程式碼。附註：您必須先*建置*字典、才能從支援資料中找出要清理的值。

1. 若要從支援資料新增您自己的關鍵字以清理、請在*自訂關鍵字*區段中、按一下功能表：動作[新增自訂關鍵字]。輸入關鍵字、然後按一下*「Save*（儲存*）」。關鍵字即會新增至該字典。
2. 展開*模式（regexp）。按一下「*新增」以取得用於輸入新模式的對話方塊。
3. 若要使用規則運算式來識別要清理的字詞或片語、請在*規則運算式*區段中輸入模式或模式。按一下功能表：「Actions（動作）」[「Add regular expression]（新增規則運算式）」、在欄位中輸入模式名稱和規則運算式、然後按一下「* Save（儲存）」。資訊已新增至該字典。

   模式必須包含圓括弧、以識別規則運算式擷取群組。

4. 在「***Build D**彙 編」一節中、按一下「*建置」、即可開始編譯OnCommand Insight 從該資料庫中辨識為敏感的所有字詞。

   完成後、您會看到提示、通知您有可用的修訂版字典。資料庫說明包含一行、指出該字典中有多少關鍵字。檢查您在字典中的關鍵字是否正確。如果您發現問題並想要重新建置該字典、請按一下資料庫區塊上的*重設*、從OnCommand Insight 該字典中移除從該資料庫收集的所有關鍵字。根據提示、不會刪除其他關鍵字。返回清理公用程式、然後再次輸入您的自訂關鍵字。

5. 建立清理字典之後、您可以使用它來清理記錄、XML或其他文字檔、使資料成為匿名。
6. 若要清理記錄檔、XML或其他文字檔、請在*清理資料*區段中、瀏覽找出檔案、然後按一下*清理檔案*。

進階疑難排解

若要完成OnCommand Insight 您的不完整組態、您必須使用進階疑難排解工具。這些工具會在瀏覽器中執行、並從*管理*>*疑難排解*頁面開啟。

若要在瀏覽器中開啟進階疑難排解工具、請按一下頁面底部的*進階疑難排解*連結。

進階疑難排解工具可讓您檢視各種報告、系統資訊、安裝的套件和記錄、以及執行許多動作、例如重新啟動伺服器或擷取單位、更新DWH註釋、以及匯入註釋。

請參閱「進階疑難排解」頁面以取得所有可用選項。

設定忽略動態資料的小時數

您可以設定OnCommand Insight 不更新動態資料（例如已用容量）的時候數。如果使用預設的六小時、但未發生任何組態變更、則在預設的時數之後、報告才會以動態資料更新。此選項可改善效能、因為此選項只會在動態資料變更時延遲更新。

關於這項工作

如果為此選項設定值、OnCommand Insight 則會根據下列規則更新動態資料：

- 如果沒有發生組態變更、但容量資料有所變更、則不會更新資料。
- 只有在此選項中指定的逾時後、才會更新動態資料（組態變更除外）。
- 如果發生組態變更、則會更新組態和動態資料。

受此選項影響的動態資料包括：

- 容量違規資料
- 檔案系統已配置容量和已用容量
- Hypervisor
  - 虛擬磁碟使用容量
  - 虛擬機器使用容量
- 內部Volume
  - 資料分配容量
  - 資料使用容量
  - 重複資料刪除技術的節省
  - 上次已知存取時間
  - 上次Snapshot時間
  - 其他已用容量
  - Snapshot計數
  - Snapshot已用容量
  - 總使用容量
- iSCSI工作階段啟動器IP、目標工作階段ID和啟動器工作階段ID
- qtree配額已使用容量
- 配額已用檔案和已用容量
- 儲存效率技術、獲利/損失及潛在獲利/損失
- 儲存資源池
  - 資料使用容量
  - 重複資料刪除技術的節省
  - 其他已用容量

    - Snapshot已用容量
    - 總使用容量
- Volume
    - 重複資料刪除技術的節省
    - 上次已知存取時間
    - 已用容量

步驟

1. 在Insight工具列上、按一下*管理*、然後選取*疑難排解*。
2. 在頁面底部的「其他工作」區域中、按一下「進階疑難排解」連結。
3. 按一下「進階設定」索引標籤、在「擷取動態屬性」區段中、輸入OnCommand Insight 應忽略「擷取動態屬性」動態資料的小時數。
4. 按一下「 * 儲存 * 」。
5. （選用）若要重新啟動擷取單位、請按一下*重新啟動擷取單位*連結。

   重新建立本機擷取單元會重新載入OnCommand Insight 所有的「不景點資料來源」視圖。此變更會在下次輪詢期間套用、因此您不需要重新啟動擷取設備。

為客戶支援產生記錄

如果客戶支援部門要求、請產生伺服器、擷取或遠端記錄、以供疑難排解之用。

關於這項工作

如果NetApp客戶支援要求、請使用此選項來產生記錄。

步驟

1. 在Insight工具列上、按一下*管理*、然後選取*疑難排解*。
2. 在頁面底部的「其他工作」區域中、按一下「進階疑難排解」。
3. 在「進階」功能表的下一頁、按一下「疑難排解」連結。
4. 按一下「記錄」索引標籤、然後選取要下載的記錄檔。

   此時會開啟一個對話方塊、讓您開啟記錄檔或將記錄儲存在本機。

顯示系統資訊

您可以顯示OnCommand Insight 部署了該伺服器之系統的Microsoft Windows IP組態資訊。

步驟

1. 在Insight工具列上、按一下*管理*、然後選取*疑難排解*。

2. 在頁面底部的「其他工作」區域中、按一下「進階疑難排解」連結。
3. 在「進階疑難排解」頁面上、按一下「報告」索引標籤。
4. 按一下*系統資訊*。

   Windows IP組態包括主機名稱、DNS、IP位址、子網路遮罩、作業系統資訊、 記憶體、開機裝置和連線名稱。

列出安裝**OnCommand Insight** 的元件

您可以顯示已安裝OnCommand Insight 的各種元件清單、包括庫存、容量、尺寸、 以及資料倉儲檢視。客戶支援部門可能會要求您提供此資訊、或者您可能想要查看安裝的軟體版本及安裝時間。

步驟

1. 在Insight工具列上、按一下*管理*、然後選取*疑難排解*。
2. 在頁面底部的「其他工作」區域中、按一下「進階疑難排解」連結。
3. 在「進階疑難排解」頁面上、按一下「報告」索引標籤。
4. 按一下*安裝的軟體套件*。

計算資料庫物件數目

若要判斷OnCommand Insight 還原資料庫中的物件數量、請使用「計算比例」功能。

步驟

1. 在Insight工具列上、按一下*管理*、然後選取*疑難排解*。
2. 在頁面底部的「其他工作」區域中、按一下「進階疑難排解」連結。
3. 在「進階疑難排解」頁面上、按一下「報告」索引標籤。
4. 按一下*計算比例*。

重新啟動**OnCommand Insight** 伺服器

當您重新啟動OnCommand Insight 伺服器時、請重新整理頁面、OnCommand Insight 然後再次登入此功能。

關於這項工作

> 這兩種選項僅應在NetApp客戶支援部門提出要求時使用。重新啟動之前不會進行任何確認。

步驟

1. 在Insight工具列上、按一下*管理*、然後選取*疑難排解*。
2. 在頁面底部的「其他工作」區域中、按一下「進階疑難排解」連結。

3. 在「進階」功能表的下一頁、按一下「動作」索引標籤。
4. 按一下*重新啟動伺服器*。

使用移轉選項移動**MySQL**資料

您可以使用將MySQL資料目錄移轉到不同的目錄。您可以保留目前的資料目錄。您可以使用疑難排解功能表上的移轉選項、也可以使用命令列。本程序說明如何使用*疑難排解*>*移轉MySQL資料*選項。

關於這項工作

如果您保留目前的資料目錄、它將保留為備份並重新命名。

步驟

1. 在Web UI中、按一下「管理」、然後選取「疑難排解」。
2. 按一下*進階疑難排解*。
3. 選擇* Actions （操作）選項卡
4. 選擇*移轉MySQL Data*。
5. 輸入您要移轉資料的路徑。
6. 若要保留現有的資料目錄、請勾選*保留現有的資料目錄。*
7. 按一下*移轉*。

使用命令列移動**MySQL**資料

您可以使用將MySQL資料目錄移轉到不同的目錄。您可以保留目前的資料目錄。您可以使用疑難排解功能表上的移轉選項、也可以使用命令列。本程序說明如何使用命令列。

關於這項工作

如果您保留目前的資料目錄、它將保留為備份並重新命名。

您可以使用「移轉MySQL資料」公用程式、也可以使用 `java -jar mysqldatamigrator.jar` 選項OnCommand Insight `\bin\mysqldatamigrator` 應使用下列參數的位置：

- 必要參數
  - 路徑

    將複製資料資料夾的新資料路徑。
- 選用參數
  - * myCnf <my .cnf file> Set*
  - 備份

    如果設定此旗標、則會重新命名目前的資料資料夾、但不會刪除。

步驟

1. 請至此處存取命令列工具： `<installation path>` \bin\mysqldatamigator\mysqldatamigator.jar`

使用範例

```
java -jar mysqldatamigrator.jar -path "C:\<new path>" -doBackup
```

強制註釋更新

如果您已變更註釋並想要立即在報告中使用註釋、請使用其中一個強制註釋選項。

步驟

1. 在Web UI中、按一下「管理」、然後選取「疑難排解」。
2. 在頁面底部、按一下「進階疑難排解」連結。
3. 按一下「動作」索引標籤。
4. 選取下列其中一個選項：
   - 更新**DWH**附註、強制更新資料倉儲中的附註、以供報告使用。
   - *更新DWH附註（包括刪除）*強制更新資料倉儲中的註釋（包括刪除的物件）以供報告使用。

檢查伺服器資源的狀態

此選項會顯示OnCommand Insight 支援伺服器的資訊、包括伺服器記憶體、磁碟空間、作業系統、以及CPU和OnCommand Insight 包含InnoDB資料大小和資料庫所在磁碟可用空間等資料庫資訊。

步驟

1. 在Insight工具列上、按一下*管理*、然後選取*疑難排解*。
2. 在頁面底部的「其他工作」區域中、按一下「* OnCommand Insight 」「Portal *」連結。
3. 在「進階」功能表的下一頁、按一下「疑難排解」連結。
4. 按一下*伺服器資源狀態*。

   *對於進階OnCommand Insight 版的支援對象：*系統管理員可以執行一些SQL測試、從資訊摘要結尾的按鈕檢查資料庫和伺服器的回應時間。如果伺服器資源不足、此選項會顯示警告。

尋找重影資料來源

如果您已移除裝置、但仍保留裝置資料、您可以找到任何重影資料來源、以便將其移除。

步驟

1. 在Web UI中、按一下「管理」、然後選取「疑難排解」。

2. 在頁面底部的「其他工作」區域中、按一下「進階疑難排解」連結。
3. 在* Reports*（報告）選項卡上，單擊* Ghost* Data Sources"（*重影資料來源）鏈接。

   用自己的裝置資訊製作一份原創者清單OnCommand Insight 。

新增遺失的磁碟機型

如果擷取因為不明的磁碟機型而失敗、您可以將遺失的磁碟機型新增至 `new_disk_models.txt` 歸檔並再次執行擷取。

關於這項工作

在以不完整的擷取方式輪詢儲存設備OnCommand Insight 時、會讀取儲存設備上的磁碟機型。如果廠商在陣列中新增Insight不知道的新磁碟機型、或是Insight尋找的型號與儲存裝置傳回的型號不符、則取得該資料來源將會失敗並顯示錯誤。為了避免這些錯誤、必須更新Insight已知的磁碟機型資訊。Insight新增了新的磁碟機型、提供更新、修補程式和維護版本。不過、您可能決定手動更新此資訊、而非等待修補程式或更新。

由於每五分鐘就會讀取磁碟模型檔案、因此您輸入的任何新資料模型資訊都會自動更新OnCommand Insight 。您不需要重新啟動伺服器、變更才會生效、但您可以選擇重新啟動伺服器、以及任何遠端擷取設備（Raus）、讓變更在下次更新之前生效。

磁碟模型更新會新增至 `new_disk_models.txt` 檔案位於`<SANScreenInstallDir>\wildfly\standalone\deployments\datasources.war` 目錄。在更新之前、請先瞭解描述新磁碟模型所需的資訊 `new_disk_models.txt` 檔案：檔案中的資訊不準確會產生不正確的系統資料、並可能導致擷取失敗。

請依照下列指示手動更新Insight磁碟機型：

步驟

1. 找出適用於您磁碟機型的適當資訊。
2. 使用文字編輯器開啟 `new_disk_models.txt` 檔案：
3. 新增新資料來源的必要資訊。
4. 將檔案儲存在中`<SANScreenInstallDir>\wildfly\standalone\deployments\datasources.war` 目錄。
5. 備份 `new_disk_models.txt` 檔案移至安全位置。在後續OnCommand Insight 任何的版本更新中、此檔案將會被覆寫。如果升級後的檔案中沒有您的磁碟機型資訊、您必須重新輸入。

找出新磁碟機型所需的資訊

若要找出磁碟機型資訊、請識別廠商和型號、然後執行網際網路搜尋。

關於這項工作

尋找磁碟機型資訊就像執行網際網路搜尋一樣簡單。搜尋前、請務必記下廠商名稱和磁碟機型號。

步驟

1. 建議您使用進階網際網路搜尋廠商、機型及文件類型「PDF」、以尋找廠商的資料表及/或磁碟機安裝指南。這些資料表通常是廠商磁碟資訊的最佳來源。
2. 廠商規格並不一定會根據完整的機型編號提供所有必要資訊。在廠商網站上搜尋模型編號字串的不同部分、以找出所有資訊、通常很有用。
3. 找到磁碟廠商名稱、完整型號、磁碟大小和速度、以及介面類型、以便在OnCommand Insight 支援中定義新的磁碟機型。您可以使用下表作為指南、在找到這些資訊時予以注意：

針對此欄位：	這是：	請輸入：
機型編號（又稱為Key）	必要	
廠商	必要	
磁碟速度（RPM）	必要	
大小（單位：GB）	必要	
介面類型（選取一項）	必要	ATA、SATA、SATA2、SATA3、FC、 SAS、FATA、SSD、其他
搜尋時間（毫秒）	選用	
最大傳輸率（單位：MB/sec）	選用	
介面傳輸率（以MB/秒為單位）	選用	
連結至廠商/機型資訊	選用但建議使用	

4. 在中輸入該資訊 `new_disk_models.txt` 檔案：請參閱 "new_disk_models.txt檔案的內容" 格式、順序和範例。

new_disk_models.txt檔案的內容

- `new_disk_models.txt` 檔案有必填欄位和選用欄位。這些欄位以逗號分隔、因此請勿在欄位中使用逗號_within。

除了搜尋時間、傳輸率和其他資訊以外、所有欄位都是必填欄位。如果有、請在「add_info」欄位中加入廠商/機型網站連結。

使用文字編輯器、針對您要新增的每個新磁碟機型、依此順序輸入下列資訊（以逗號分隔）：

1. 金鑰：使用機型編號（必填）
2. 廠商：名稱（必填）
3. 型號：完整數字（通常與「key」（機碼）相同）（必填）

4. 磁碟*的* rpm：例如10000或15000（必要）
5. 大小：容量（單位：GB）（必填）
6. 介面類型：ATA、SATA、FC、SAS、FATA、 SSD、其他（必要）
7. 搜尋時間：單位為毫秒（選用）
8. 潛在傳輸率：可能的傳輸率（以MB/秒為單位）磁碟本身的最大傳輸率。（選用）
9. 介面傳輸率：主機往返主機的速率（以MB/秒為單位）（選用）。
10. 其他資訊：您想要擷取的任何其他資訊。最佳實務做法是輸入找到規格的廠商頁面連結、以供參考（選用）

對於任何保留空白的選用欄位、請務必包含逗號。

範例（每一行均無空格）：

```
ST373405,Seagate,ST373405,10000,73,FC,5.3,64,160,http://www.seagate.com/staticfil
es/support/disc/manuals/enterprise/cheetah/73(LP)/100109943e.pdf

SLR5B-M400SS,HITACHI,SLR5B-M400SS,1000000,400,SSD,,,,

X477_THARX04TA07,TOSHIBA,X477_THARX04TA07,7200,4000,SATA,9.5,,,https://storage.to
shiba.eu/export/sites/toshiba-sdd/media/products/datasheets/MG03ACAxxxY.pdf
```

監控環境

Insight可協助您預防環境中的問題、並快速疑難排解潛在問題。

資產頁面資料

資產頁面提供效能疑難排解資料、並提供基礎資產（例如虛擬機器或磁碟區）及其使用的相關資產（例如儲存資源池、儲存節點及連接的交換器連接埠）的摘要資訊、以及其他資訊的連結。

從功能完整的7.3.1開始OnCommand Insight 、所有資產頁面都有*主*頁面和*其他資料*頁面。在主頁上、摘要列出資產、以及圖表、拓撲和其他資訊的不同區段。「其他資料」頁面可讓您針對目前的資產類型設定可自訂的儀表板頁面。

資產頁面主索引標籤上的行或訊息旁會出現紅色圓圈、表示受監控環境可能發生問題。

資產頁面類型

資產頁面會摘要說明資產的目前狀態、並包含資產及其相關資產的其他資訊連結。

提供下列資產的資產頁面OnCommand Insight ：

- 虛擬機器
- Volume
- 內部Volume

- 實體主機
- 儲存資源池
- 儲存設備
- 資料存放區
- Hypervisor
- 應用程式
- 儲存節點
- qtree
- 磁碟
- VMDK
- 連接埠
- 交換器
- 網路
- 物件儲存（例如、Atmos、Centera、Amazon S3）
- 區域

對應與遮罩資訊可在「區域」、「Volume」、「VM」和「主機/ Hypervisor」資產頁面的表格中檢視。

> 摘要資訊可用於物件儲存資產、不過您只能從「資料來源詳細資料」頁面存取此資訊。

搜尋環境中的特定資產

您可以使用搜尋工具來尋找特定資產的相關資訊。例如、如果系統使用者聯絡儲存管理員、並對特定伺服器提出抱怨、則管理員可以搜尋伺服器名稱、並顯示資產頁面、摘要說明狀態並提供其他連結資訊。

步驟

1. 開啟OnCommand 「視覺瀏覽」UI。
2. 在工具列上、按一下 。

   此時會顯示「搜尋資產」方塊。

3. 輸入資產名稱或部分名稱。
4. 從搜尋結果中選取所需的資源。

   隨即顯示該資源的資產頁面。

進階搜尋技術

您可以使用多種搜尋技術來搜尋監控環境中的資料或物件。

萬用字元搜尋

您可以使用*字元執行多個字元的萬用字元搜尋。例如、_applic* n_會傳回應用程式。

用於搜尋的詞彙

片語是一組字詞、以雙引號括住、例如「paw VNX LUN 5」。您可以使用雙引號來搜尋名稱或屬性中含有空格的文件。

布林運算子

使用布林運算子、您可以合併多個字詞、形成更複雜的查詢。

- 或
  - OR運算子是預設的聯合運算子。

    如果兩個詞彙之間沒有布林運算子、則會使用OR運算子。

  - OR運算子會連結兩個詞彙、如果文件中有任一詞彙、就會找到相符的文件。

    例如、「'sorage or NetApp'」會搜尋含有「'sorage'」或「'NetApp'」的文件。

  - 對於符合大部分條款的文件、會給予高分。
- 和

  您可以使用AND運算子來尋找單一文件中同時存在兩個搜尋字詞的文件。例如、「'aurora and NetApp'」會搜尋同時包含「shorage'」和「'NetApp'」的文件。

  您可以使用符號&&取代詞AND。

- 不

  當您使用Not運算子時、搜尋結果中會排除所有包含「Not」字詞之後的文件。例如、「'sorage not NetApp'」會搜尋僅包含「shorage」而非「'NetApp'」的文件。

  您可以使用符號！而不是「不」這個字。

字首和字尾搜尋

- 一旦您開始輸入搜尋字串、搜尋引擎就會執行前置詞和後置字元搜尋、以找出最相符的字元。
- 完全符合的分數比前置詞或後置字元相符的分數高。分數是根據搜尋詞彙與實際搜尋結果之間的距離來計算。例如、我們有三個儲存室：「'aurora'」、「'aurora1'」和「'aurora11'」。搜尋「aur」將會傳回所有三個儲存室。不過、「'aurora'」的搜尋結果會獲得最高分數、因為它距離前置字元搜尋字串最近。
- 搜尋引擎也會以相反順序搜尋詞彙、讓您執行後置搜尋。例如、當您在搜尋方塊中輸入「'345」時、搜尋引擎會搜尋「'345」。
- 搜尋不區分大小寫。

使用索引詞彙進行搜尋

符合更多索引詞彙的搜尋結果會獲得較高的分數。

搜尋字串會依空格分割成不同的搜尋字詞。例如、搜尋字串「'sorage aurora NetApp'」分為三個關鍵字：「'torage'」、「'aurora'」和「'NetApp'」。搜尋是使用這三個詞彙來執行。大部分符合這些詞彙的文件將獲得最高分數。您提供的資訊越多、搜尋結果就越好。例如、您可以依儲存設備的名稱和模式來搜尋儲存設備。

UI會顯示各類別的搜尋結果、每個類別的結果最多三項。如果您找不到所需的文件、可以在搜尋字串中加入更多字詞、以改善搜尋結果。

下表提供可新增至搜尋字串的索引詞彙清單。

類別	索引詞彙
儲存設備	• 「太老了」 • 名稱 • 廠商 • 模型
StoragePool	• 「toragepool」 • 名稱 • 儲存設備名稱 • 儲存設備的IP位址 • 儲存設備的序號 • 儲存設備廠商 • 儲存模式 • 所有相關內部磁碟區的名稱 • 所有相關磁碟的名稱
內部Volume	• 「內部容量」 • 名稱 • 儲存設備名稱 • 儲存設備的IP位址 • 儲存設備的序號 • 儲存設備廠商 • 儲存模式 • 儲存資源池名稱 • 所有相關共用的名稱 • 所有相關應用程式和商業實體的名稱

Volume	• 「Volume」 • 名稱 • 標籤 • 所有內部磁碟區的名稱 • 儲存資源池名稱 • 儲存設備名稱 • 儲存設備的IP位址 • 儲存設備的序號 • 儲存設備廠商 • 儲存模式
儲存節點	• 「太過程式碼」 • 名稱 • 儲存設備名稱 • 儲存設備的IP位址 • 儲存設備序號 • 儲存設備廠商 • 儲存模式
主機	• 「主機」 • 名稱 • IP位址 • 所有相關應用程式和商業實體的名稱
資料存放區	• 「Datastore」 • 名稱 • 虛擬中心IP • 所有Volume的名稱 • 所有內部磁碟區的名稱

虛擬機器	• 「虛擬機器」 • 名稱 • DNS名稱 • IP位址 • 主機名稱 • 主機的IP位址 • 所有資料存放區的名稱 • 所有相關應用程式和商業實體的名稱
交換器（一般和NPV）	• 「女魔女」 • IP 位址 • WWN • 名稱 • 序號 • 模型 • 網域ID • 網路名稱 • 網路的WWN
應用程式	• 「應用程式」 • 名稱 • 租戶 • 業務線 • 業務單位 • 專案
磁帶	• 「'tape」 • IP 位址 • 名稱 • 序號 • 廠商
連接埠	• 「'port'」 • WWN • 名稱

網路	• 「Fabric」 • WWN • 名稱

變更顯示資料的時間範圍

依預設、資產頁面會顯示過去24小時的資料；不過、您可以選取其他固定時間或自訂時間範圍來變更所顯示的資料區段、以檢視較少或更多的資料。

關於這項工作

無論資產類型為何、您都可以使用位於每個資產頁面的選項來變更顯示資料的時間區段。

步驟

1. 登入OnCommand 到「無法使用者介面」。
2. 執行下列其中一項動作、找出資產頁面：
   - 在Insight工具列上、按一下 ，輸入資產名稱，然後從清單中選取資產。
   - 按一下*儀表板*、選取*資產儀表板*、找出資產名稱、然後按一下。隨即顯示「資產」頁面。
3. 在頁面左上角、按一下下列任一時間圖示、以變更所顯示的資料區段：
   - * 3小時*

     顯示過去三小時的資料。
   - * 24小時*

     顯示過去24小時的資料。
   - * 3D *

     顯示過去三天的資料。
   - * 7d*

     顯示過去七天的資料。
   - * 30d*

     顯示過去30天的資料。
   - 自訂

     顯示對話方塊、讓您選擇自訂時間範圍。您一次最多可顯示31天的資料。
4. 如果您選擇*自訂*、請執行下列動作：
   a. 按一下日期欄位、然後選取開始日期的月份、日期和年份。

b. 按一下時間清單、然後選取開始時間。

c. 針對結束資料和時間重複步驟a和b。

d. 按一下 ✔ 。

判斷資料來源擷取狀態

由於資料來源是Insight的主要資訊來源、因此您必須確保資料來源保持在執行中狀態。

您可以在每個資產頁面上、查看直接取得的所有資產的資料來源擷取狀態。可能發生下列任一擷取案例、狀態會顯示在資產頁面的右上角：

- 已成功從資料來源取得

  顯示「擷取」狀態 `xxxx``", where `xxxx` 指出資產資料來源最近的擷取時間。

- 發生擷取錯誤。

  顯示「擷取」狀態 `xxxx``", where `xxxx` 指出資產的一或多個資料來源最近使用的擷取時間 ⚠ 。當您按一下時 ⚠ 、視窗會顯示資產的每個資料來源、資料來源狀態、以及上次擷取資料的時間。按一下資料來源會顯示資料來源的詳細資料頁面。

如果資產並非直接取得、則不會顯示任何狀態。

資產頁面區段

資產頁面會顯示數個區段、其中包含與資產相關的資訊。您所看到的區段取決於資產類型。

摘要

資產頁面上的「摘要」區段會顯示特定資產的相關資訊摘要、並顯示與資產相關的問題、以紅色圓圈表示、並提供超連結、可連結至相關資產的其他資訊、以及指派給該資產的任何效能原則。

以下範例顯示虛擬機器資產頁面的「摘要」區段中可用的部分資訊類型。旁邊有一個紅色圓圈的任何項目、都表示受監控環境可能發生問題。

Summary

Power state:	On
Guest state:	Running
Datastore:	DS_SP1_1
CPU:	41.05%
Memory:	51% (1,047 / 2,048 MB)
Capacity:	10% (19.5 / 195.3 GB)
Latency:	1.93 ms (6.00 ms max)
IOPS:	1,317.33 IO/s (4,964.00 IO/s max)
Throughput:	38.79 MB/s (142.00 MB/s max)
DNS name:	VM_Cs_travBookcomp.com
IP:	10.97.133.23
OS:	Microsoft Windows Server 2008 R2(64-bit)
Processors:	4
FC Fabrics Connected:	1
Performance Policies:	VM Latency-Critical VM Latency-Warning Comp Corp.Customer Support SLA latency Exchange SL0

使用「摘要」區段

您可以檢視「摘要」區段、查看資產的一般資訊。具體而言、查看是否有任何指標（例如記憶體、容量和延遲）或任何效能原則引起疑慮、OnCommand Insight 而這些指標會在指標或效能原則旁顯示紅色圓圈、以表示此問題。

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、找出資產頁面：
   - 在Insight工具列上、按一下 ，輸入資產名稱，然後從清單中選取資產。
   - 按一下*儀表板*、選取*資產儀表板*、找出資產名稱、然後按一下。隨即顯示「資產」頁面。

     摘要區段中顯示的資訊取決於您所檢視的資產頁面類型。
3. 您可以按一下任何資產連結來檢視其資產頁面。

   例如、如果您正在檢視儲存節點、可以按一下連結來檢視與其相關聯之儲存設備的資產頁面、或按一下以檢視HA合作夥伴的資產頁面。
4. 您可以檢視與資產相關的指標。

   指標旁的紅色圓圈表示您可能需要診斷並解決潛在問題。

您可能會注意到、部分儲存資產的Volume容量可能顯示超過100%。這是因為與磁碟區容量相關的中繼資料、是資產所報告之已用容量資料的一部分。

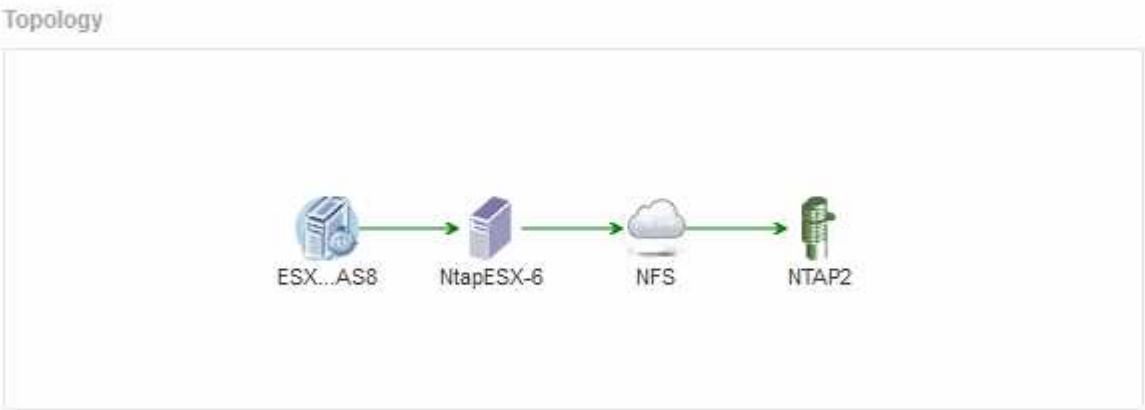
5. 如果適用、您可以按一下效能原則連結、檢視與資產相關的效能原則或原則。

   如果效能原則旁邊出現紅色圓圈、表示資產已超過效能原則定義的臨界值。您應該檢查效能原則、以進一步診斷問題。

拓撲

拓撲區段（若適用於資產）可讓您查看基礎資產與其相關資產的連線方式。

以下是虛擬機器資產頁面的「拓撲」區段可能顯示的範例。



如果資產的拓撲大於該部分所能容納的範圍、則會顯示*按一下連結以查看拓撲*超連結。

使用拓撲區段

「拓撲」區段可讓您檢視網路中的資產如何彼此連線、並顯示相關資產的相關資訊。

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、找出資產頁面：
   - 在Insight工具列上、按一下 Q，輸入資產名稱，然後從清單中選取資產。
   - 按一下*儀表板*、選取*資產儀表板*、找出資產名稱、然後按一下。隨即顯示「資產」頁面。您可以在資產頁面的右上角找到「拓撲」區段。

   如果資產的拓撲大於該部分所需的範圍、請按一下*按一下連結以查看拓撲*超連結。

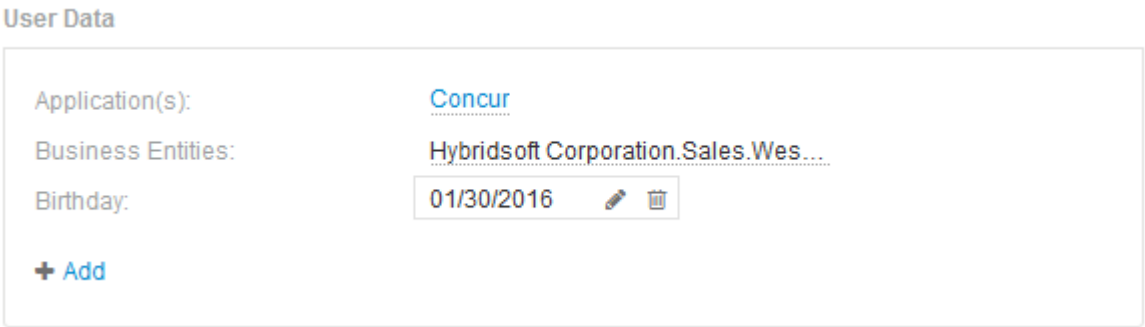
3. 若要檢視基礎資產相關資產的詳細資訊、請將游標放在拓撲中的相關資產上、然後按一下其名稱、即會顯示其資產頁面。

使用者資料

資產頁面的「使用者資料」區段隨即顯示、並可讓您變更任何使用者定義的資料、例如應

用程式、商業實體和註釋。

下列範例顯示當應用程式、企業實體及註釋指派給資產時、虛擬機器資產頁面的「使用者資料」區段可能會顯示的內容：



使用「使用者資料」區段來指派或修改應用程式

您可以將環境中執行的應用程式指派給特定資產（主機、虛擬機器、磁碟區、內部磁碟區和Hypervisor）。「使用者資料」區段可讓您變更指派給資產的應用程式、或將應用程式或其他應用程式指派給資產。

步驟

1. 登入OnCommand Insight 到The W不明 網路UI。
2. 執行下列其中一項動作、找出資產頁面：
   - 在Insight工具列上、按一下 ，輸入資產名稱，然後從清單中選取資產。
   - 按一下*儀表板*、選取*資產儀表板*、找出資產名稱、然後按一下。隨即顯示「資產」頁面。
3. 您可以執行下列動作：
   - 若要檢視應用程式的資產頁面、請按一下應用程式名稱。
   - 若要變更已指派的應用程式或指派應用程式或其他應用程式、請將游標放在應用程式名稱上方（如果已指派應用程式）、或將游標放在*無*上（如果未指派應用程式）、請按一下 下、輸入以搜尋應用程式、或從清單中選取應用程式、然後按一下 。

     如果您選擇與企業實體相關聯的應用程式、則該企業實體會自動指派給該資產。在這種情況下、當您將游標放在企業實體名稱上時、會顯示「推導」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。

   - 若要移除應用程式、請按一下 。

使用「使用者資料」區段來指派或修改商業實體

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。資產頁面的「使用者資料」區段可讓您變更指派給資產的企業實體、或是從資產中移除企業實體。

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、找出資產頁面：
   - 在Insight工具列上、按一下 ，輸入資產名稱，然後從清單中選取資產。
   - 按一下*儀表板*、選取*資產儀表板*、找出資產名稱、然後按一下。隨即顯示「資產」頁面。
3. 您可以執行下列動作：
   - 若要變更指派的實體或指派實體、請按一下 然後從清單中選取一個實體。
   - 若要移除企業實體、請按一下 。

     您無法移除從指派給資產的應用程式衍生的實體。

使用「使用者資料」區段來指派或修改附註

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。資產頁面的「使用者資料」區段會顯示指派給資產的附註、並可讓您變更指派給該資產的附註。

步驟

1. 登入OnCommand Insight 到The W不明 網路UI。
2. 執行下列其中一項動作、找出資產頁面：
   - 在Insight工具列上、按一下 ，輸入資產名稱，然後從清單中選取資產。
   - 按一下*儀表板*、選取*資產儀表板*、找出資產名稱、然後按一下。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 。

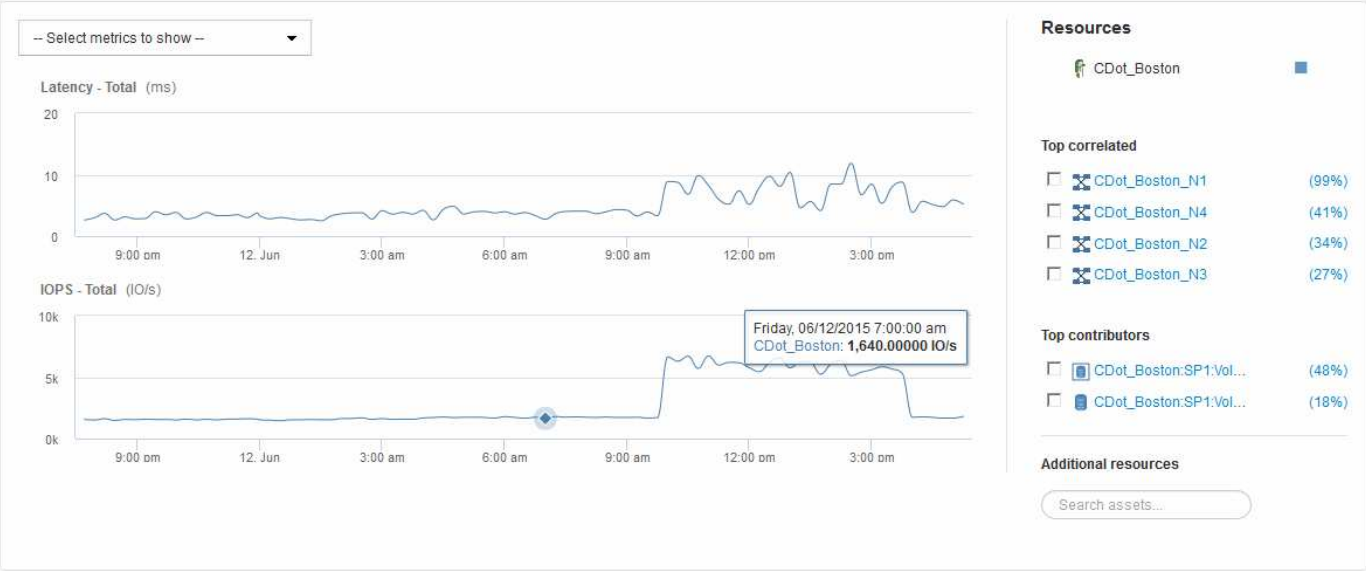
   此時會顯示「新增附註」對話方塊。
4. 按一下*註釋*、然後從清單中選取註釋。
5. 按一下*值*、然後根據您選取的註釋類型執行下列任一項：
   - 如果註釋類型為清單、日期或布林值、請從清單中選取一個值。
   - 如果註釋類型為文字、請輸入一個值。
6. 按一下「 * 儲存 * 」。

   註釋會指派給資產。您稍後可以使用查詢來篩選資產。
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。

資產頁面的「專家檢視」區段可讓您根據所選期間（3小時、24小時、3天、7天、 或自訂期間）。

以下是Volume資產頁面中「專家檢視」區段的範例：



您可以在效能圖表中選取所選期間內要檢視的指標。

「資源」區段會顯示基礎資產的名稱、以及效能圖表中代表基礎資產的色彩。如果Top Correlated區段未包含您想要在效能圖表中檢視的資產、您可以使用「其他資源」區段中的「搜尋資產」方塊來找出資產並將其新增至效能圖表。當您新增資源時、這些資源會顯示在「其他資源」區段中。

如適用、「資源」區段也會顯示下列類別中與基礎資產相關的任何資產：

- 最高關聯

  顯示與基礎資產有高關聯性（百分比）的資產、以及一或多個效能指標。

- 頂尖貢獻者

  顯示對基礎資產貢獻（百分比）的資產。

- 貪婪

  顯示透過共用相同資源（例如主機、網路和儲存設備）而從資產中移走系統資源的資產。

- 降級

  顯示因此資產而耗盡系統資源的資產。

Expert View度量定義

資產頁面的「專家檢視」區段會根據為資產選取的時間週期、顯示數個指標。每個指標都

會顯示在自己的效能圖表中。您可以根據想要查看的資料、從圖表中新增或移除指標和相關資產。

度量	說明
寬帶零接收器、傳輸器	在取樣期間、接收/傳輸緩衝區對緩衝區信用數轉換為零的次數。此度量代表連接埠因此連接埠超出信用額度而必須停止傳輸的次數。
BB積分零持續時間Tx	取樣時間間隔內、傳輸寬頻點數為零的時間（以毫秒為單位）。
快取命中率（總計、讀取、寫入）%	導致快取命中的要求百分比。點擊次數比存取磁碟區的次數越多、效能就越好。對於不收集快取命中率資訊的儲存陣列、此欄為空白。
快取使用率（總計）%	導致快取命中的快取要求總數百分比
類別3捨棄	3級光纖通道資料傳輸捨棄的計數。
CPU使用率（總計）%	作用中使用的CPU資源量、佔總可用（所有虛擬CPU）的百分比。
crc錯誤	在取樣期間、連接埠偵測到具有無效循環備援檢查（CRC）的框架數
影格速率	以每秒影格數（FPS）傳輸影格速率
平均影格大小（接收、傳輸）	流量與影格大小的比率。此度量可讓您識別網路中是否有任何高負荷框架。
影格大小太長	光纖通道資料傳輸框架過長的計數。
影格大小太短	光纖通道資料傳輸框架過短的計數。
I/O密度（總、讀取、寫入）	IOPS的數目除以Volume、內部Volume或Storage元素的已用容量（從最近的資料來源庫存輪詢中取得）。測量單位為每TB每秒I/O作業數。
IOPS（總計、讀取、寫入）	透過I/O通道傳遞的讀寫I/O服務要求數、或是每單位時間（以每秒I/O數為單位）該通道的一部分。

IP處理量（總計、讀取、寫入）	總計：傳輸和接收IP資料的彙總速率、單位為每秒MB。讀取：IP傳輸量（接收）：接收IP資料的平均速率、以百萬位元組/秒為單位。 寫入：IP傳輸量（傳輸）：傳輸IP資料的平均速率、以百萬位元組/秒為單位。
延遲（總計、讀取、寫入）	延遲（R&W）：資料在固定時間內讀取或寫入虛擬機器的速率。此值的測量單位為每秒百萬位元組。 延遲：資料儲存區中虛擬機器的平均回應時間。 最高延遲：資料儲存區中虛擬機器的最高回應時間。
連結失敗	連接埠在取樣期間偵測到的連結故障數。
連結重設接收器、傳輸	取樣期間的接收或傳輸連結重設次數。此度量表示連接埠對此連接埠發出的連結重設次數。
記憶體使用率（總計）%	主機使用的記憶體臨界值。
部分右/右（總計）%	一般而言、讀寫作業跨越RAID 5、RAID 1/0或RAID 0 LUN中任何磁碟模組的等量磁碟區界限的總次數、因為每個磁碟區交叉點都需要額外的I/O、所以這種情況並不有利低百分比表示有效率的等量磁碟區元素大小、表示磁碟區（或NetApp LUN）的對齊方式不正確。 對於CLARiiON、此值是等量磁碟區交叉數除以IOPS總數。
連接埠錯誤	取樣期間/指定時間範圍內的連接埠錯誤報告。
訊號遺失計數	訊號遺失錯誤數。如果發生訊號遺失錯誤、表示沒有電子連線、而且存在實體問題。
交換率（總速率、輸入速率、輸出速率）	取樣期間、記憶體從磁碟換入、移出或兩者都換入作用中記憶體的速率。此計數器適用於虛擬機器。
同步遺失計數	同步遺失錯誤數。如果發生同步遺失錯誤、硬體就無法判斷流量或鎖定流量。所有設備可能使用的資料速率不同、或光纖或實體連線品質不佳。每次發生此類錯誤後、連接埠都必須重新同步、這會影響系統效能。測量單位：kb/sec
處理量（總計、讀取、寫入）	在回應I/O服務要求時、資料在固定時間內傳輸、接收或兩者的速率（以每秒MB為單位）。

捨棄框架逾時- Tx	因逾時而捨棄的傳輸框架數。
流量（總計、讀取、寫入）	在取樣期間傳輸、接收或同時接收的流量、以每秒百萬位元組為單位。
流量使用率（總計、讀取、寫入）	取樣期間接收/傳輸/總流量與接收/傳輸/總容量的比率。
使用率（總計、讀取、寫入）%	傳輸（傳輸）和接收（接收）所用的可用頻寬百分比。
寫入擱置中（總計）	擱置中的寫入I/O服務要求數。

使用「專家檢視」區段

「專家檢視」區段可讓您根據所選期間內任何數量的適用指標、檢視資產的效能圖表、並新增相關資產、以便在不同時間期間比較及對照資產與相關資產的效能。

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、找出資產頁面：
   - 在Insight工具列上、按一下 Q，輸入資產名稱，然後從清單中選取資產。
   - 按一下*儀表板*、選取*資產儀表板*、找出資產名稱、然後按一下。隨即顯示「資產」頁面。根據預設、效能圖表會顯示針對資產頁面所選期間的兩項指標。例如、對於儲存設備、效能圖表預設會顯示延遲和總IOPS。「資源」區段會顯示資源名稱和其他資源區段、可讓您搜尋資產。視資產而定、您可能也會在「最高關聯者」、「最高貢獻者」、「貪度」和「降級」等區段中看到資產。
3. 您可以按一下*選取要顯示的度量*、然後選取要新增度量效能圖表的度量。

   系統會針對所選的度量新增效能圖表。圖表會顯示所選期間的資料。您可以按一下資產頁面左上角的其他時間段來變更時間週期。

   您可以再次執行步驟、然後按一下以清除度量。度量的效能圖表即會移除。
4. 您可以將游標放在圖表上、並視資產而定、按一下下列任一項目來變更顯示的度量資料：
   - 讀取*或*寫入
   - 預設為* Tx*或* Rx*總計。
5. 您可以將游標拖曳到圖表中的資料點上、以查看在所選期間內、度量值的變化情況。
6. 在「資源」區段中、您可以執行下列任一項動作（若適用）、將任何相關資產新增至效能圖表：
   - 您可以在「最高關聯」、「最高貢獻者」、「貪運算」或「降級」區段中選取相關資產、將該資產的資料新增至每個所選度量的效能圖表。資產必須有至少15%的關聯性或供款才能顯示。

     選取資產後、資產旁邊會出現一個色塊、表示圖表中資料點的色彩。

- 對於顯示的任何資產、您可以按一下資產名稱以顯示其資產頁面、或按一下資產與基礎資產相關或對其貢獻的百分比、以檢視有關與基礎資產相關的資產相關詳細資訊。

  例如、按一下頂端關聯資產旁的連結百分比會顯示資訊訊息、比較該資產與基礎資產之間的關聯類型。

- 如果最高關聯區段未包含您要在效能圖表中顯示以供比較的資產、您可以使用「其他資源」區段中的「搜尋資產」方塊來尋找其他資產。選取資產後、該資產會顯示在「其他資源」區段中。如果您不想再檢視資產的相關資訊、請按一下 。

相關資產

如果適用、資產頁面會顯示相關資產區段。例如、Volume Assets頁面可能會顯示儲存資源池、連接的交換器連接埠和運算資源等資產的相關資訊。每個區段都包含一個表格、其中列出該類別中的任何相關資產、以及其各自資產頁面的連結、以及與該資產相關的數個效能統計資料。

使用「相關資產」區段

「相關資產」區段可讓您檢視任何與基礎資產相關的資產。每項相關資產都會顯示在表格中、以及該資產的相關統計資料。您可以匯出資產資訊、在「專家檢視」效能圖表中檢視資產統計資料、或顯示僅顯示相關資產統計資料的圖表。

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、找出資產頁面：
   - 在Insight工具列上、按一下 ，輸入資產名稱，然後從清單中選取資產。
   - 按一下*儀表板*、選取*資產儀表板*、找出資產名稱、然後按一下。隨即顯示「資產」頁面。
3. 若要控制資產在表格中的顯示方式：
   - 按一下任何資產的名稱、即可顯示其資產頁面。
   - 使用「篩選」方塊僅顯示特定資產。
   - 如果資料表中有五項以上的資產、請按一下頁碼以逐頁瀏覽資產。
   - 按一下欄標題中的箭號、將表格中欄的排序順序變更為遞增（向上箭頭）或遞減（向下箭頭）。
   - 將游標放在相關資產上、然後按一下、即可將相關資產新增至「專家檢視」區段中的任何效能圖表 。
4. 可將表格中顯示的資訊匯出至 `.csv` 檔案：
   a. 按一下 。
   b. 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、或按一下「儲存檔案」、然後按一下「確定」、將檔案儲存至「下載」資料夾。

      目前選取要顯示之欄的所有物件屬性都會匯出至檔案。只會匯出顯示欄的屬性。請注意、只會匯出表格的前10、000列。

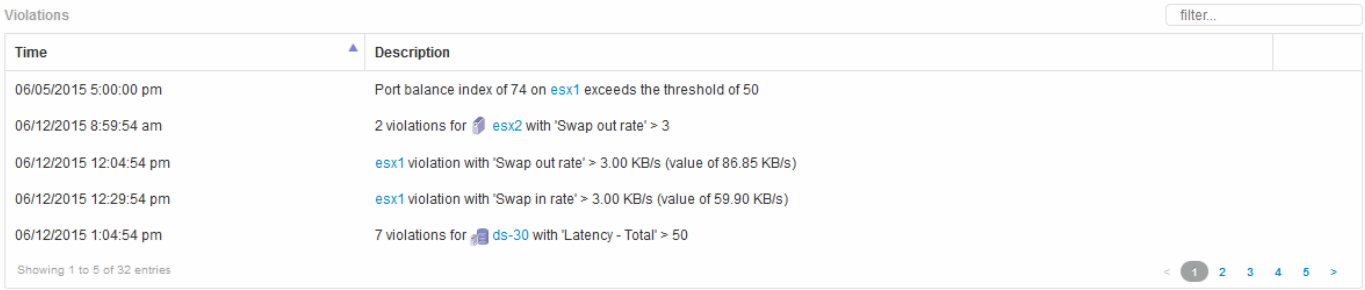
5. 若要在表格下方的圖表中顯示相關資產資訊、請按一下 並執行下列任何一項：
   - 按一下*讀取*、*寫入*或*總計*以變更顯示的度量資料。*總計*為預設值。

- 按一下 以選取不同的度量。
- 按一下 變更圖表類型。*折線圖*為預設值。
- 將游標移到圖表中的資料點上、查看在每項相關資產所選期間內、度量值的變化情況。
- 按一下圖表圖例中的相關資產、將其新增至圖表或從圖表中移除。
- 按一下相關資產表中的頁碼、即可檢視圖表中的其他相關資產。
- 按一下 以關閉圖表。

違規

您可以使用資產頁面的「違規」區段、查看指派給資產的效能原則所造成的環境違規（如果有）。效能原則可監控網路臨界值、並讓您立即偵測臨界值違規、識別其影響、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。

以下範例顯示Hypervisor資產頁面上顯示的「違規」區段：



使用「違規」區段

「違規」區段可讓您檢視及管理指派給資產的效能原則所造成的任何網路違規事件。

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、找出資產頁面：
   - 在Insight工具列上、按一下 ，輸入資產名稱，然後從清單中選取資產。
   - 按一下*儀表板*、選取*資產儀表板*、找出資產名稱、然後按一下。隨即顯示「資產」頁面。「違規」區段會顯示違規發生的時間、以及超過的臨界值說明、以及發生違規事件之資產的超連結（例如「2個違規事件符合DS-30的延遲時間-總計> 50」）。
3. 您可以執行下列任一選用工作：
   - 使用*篩選器*方塊僅顯示特定違規。
   - 如果表格中有五個以上違規、請按一下頁碼、瀏覽違規情形。
   - 按一下欄標題中的箭號、將表格中欄的排序順序變更為遞增（向上箭頭）或遞減（向下箭頭）。
   - 按一下任何說明中的資產名稱、即可顯示其資產頁面；紅色圓圈表示需要進一步調查的問題。

     您可以按一下顯示「編輯原則」對話方塊的效能原則、以檢閱效能原則、並視需要變更原則。

- 按一下 ✖ 如果您判斷問題不再是引起疑慮的原因、請從清單中移除違規行為。

可自訂的資產頁面

其他資料可顯示在每個資產頁面的可自訂小工具中。自訂資產頁面會將自訂套用至該類型所有資產的頁面。

您可以執行下列動作來自訂資產頁面小工具：

1. 新增小工具至頁面
2. 建立Widget的查詢或運算式、以顯示所需的資料
3. 如有需要、請選擇篩選條件
4. 選擇彙總或分組方法
5. 儲存小工具
6. 針對所有想要的小工具重複上述步驟
7. 儲存資產頁面

您也可以將變數新增至自訂資產頁面、以便進一步精簡小工具中的展示資料。除了一般變數之外、每種資產類型都可以使用一組「$this」變數來快速識別與目前資產直接相關的資源、例如、由裝載目前虛擬機器的同一個Hypervisor所託管的所有虛擬機器。

此自訂資產頁面對每位使用者以及每種資產類型而言都是獨一無二的。例如、如果使用者A為虛擬機器建立自訂資產頁面、則該使用者的任何虛擬機器資產頁面都會顯示該自訂頁面。

使用者只能檢視、編輯或刪除自己建立的自訂資產頁面。

Insight的匯出/匯入功能不包含自訂資產頁面。

瞭解「**$this**」變數

資產「額外資料」可自訂頁面上的特殊變數、可讓您輕鬆展示與目前資產直接相關的其他資訊。

關於這項工作

若要在資產的可自訂登陸頁面上的小工具中使用「$this」變數、請依照下列步驟操作。在此範例中、我們會新增表格小工具。

> 「$this」變數僅適用於資產的可自訂登陸頁面。其他Insight儀表板則無法使用。可用的「$this」變數會因資產類型而異。

步驟

1. 瀏覽至所選資產的資產頁面。在此範例中、我們來選擇「虛擬機器（VM）」資產頁面。查詢或搜尋VM、然後按一下連結前往該VM的資產頁面。

   此時會開啟VM的資產頁面。

2. 按一下「變更檢視：>*其他虛擬機器資料*」下拉式清單、前往該資產的可自訂登陸頁面。
3. 按一下「小工具」按鈕、然後選擇「表格小工具」。

   「表格」小工具隨即開啟以供編輯。根據預設、所有儲存都會顯示在表格中。

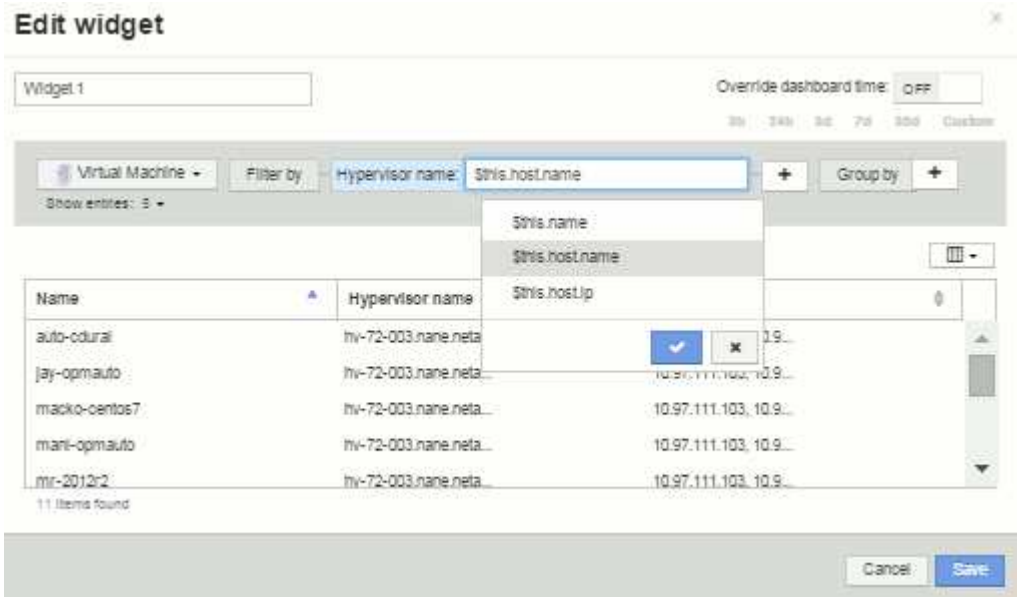
4. 我們想要顯示所有的虛擬機器。按一下資產選取器、並將* Storage 變更為 Virtual Machine *。

   所有虛擬機器現在都會顯示在表格中。

5. 按一下*欄選擇器*按鈕 並將* Hypervisor名稱*欄位新增至資料表。

   表中顯示每個VM的Hypervisor名稱。

6. 我們只關心裝載目前VM的Hypervisor。按一下*篩選條件*欄位的+按鈕、然後選取* Hypervisor名稱*。
7. 按一下「* any 」、然後選取「$this.host.name *」變數。按一下檢查按鈕以儲存篩選條件。



8. 下表顯示目前VM Hypervisor所託管的所有VM。按一下「 * 儲存 * 」。

結果

您為此虛擬機器資產頁面所建立的表格、將會顯示您所顯示的任何VM資產頁面。在小工具中使用*$this.host.name變數、表示表格中只會顯示目前資產Hypervisor所擁有的VM。

平衡網路資源

若要解決平衡問題、請使用資產頁面找出問題、並找出未充分使用的大容量磁碟區。

步驟

1. 在瀏覽器中開啟「資產儀表板」。
2. 在虛擬機器IOPS熱圖中、您會注意到虛擬機器在非常大的列印中的名稱、而該名稱通常會報告問題。

3. 按一下VM名稱以顯示資產頁面。
4. 檢查摘要中的錯誤訊息。
5. 請查看效能圖表、尤其是最重要的關聯資源、找出可能發生爭用的任何磁碟區。
6. 將磁碟區新增至效能圖表、以比較活動模式、並針對問題所涉及的其他資源顯示更多資產頁面。
7. 捲動至資產頁面底部、查看與VM相關的所有資源清單。請注意任何以大容量執行的VMDK。這可能會導致爭用。
8. 若要解決平衡問題、請找出使用率偏低的資源、以便從過度使用的資源接收負載、或是從使用率偏高的資源移除要求較低的應用程式。

檢查網路效能

您可以檢查儲存環境的效能、找出使用率過低和過度使用的資源、並在風險變成問題之前加以識別。

Insight可協助您解決或預防透過收集的儲存資料所揭露的效能與可用度問題。

您可以使用Insight來執行下列效能管理工作：

- 監控整個環境的效能
- 找出影響其他裝置效能的資源

連接埠的重要性

Insight Server和Data倉儲（DWH）伺服器可能需要大量的TCP連接埠才能正常運作、以確保可靠運作。其中有些連接埠僅用於繫結至localhost介面卡（127.0.0.1）的處理程序、但核心服務仍需可靠運作。所需的連接埠數量是跨網路使用的連接埠的超集合。

Insight伺服器連接埠

Insight Server可以安裝軟體防火牆。需要開啟的「孔」如下所述。

傳入**HTTPS 443**-假設您在TCP 443上執行Insight WebUI、您必須揭露此資訊、以允許下列任何及所有使用者：

- WebUI的深入分析使用者
- 尋求連線至Insight伺服器的遠端擷取單位
- OCI DWH伺服器搭配此Insight伺服器的連接器。
- 與Insight REST API的任何程式化互動

對於任何想要實作Insight伺服器主機層級防火牆的人、我們的一般建議是允許HTTPS存取所有公司網路IP區塊。

傳入**MySQL**（**TCP 3306**）。此連接埠僅需暴露於任何具有連接器的Insight DWH伺服器

雖然Insight擁有數十個資料收集器、但它們都是以輪詢為基礎的、但Insight會讓收購單位（Aus）開始傳出通訊至各種裝置。只要您的主機型防火牆具有「狀態」功能、允許傳回流量通過防火牆、Insight Server上的主機型防火牆就不應影響資料擷取。

資料倉儲連接埠

對於Insight DWH伺服器：

傳入**HTTPS 443**-假設您在TCP 443上執行Insight WebUI、您必須公開該AS以允許下列使用者：

- DWH管理入口網站的Insight管理使用者

傳入**HTTPS**（**TCP 9300**）*：這是Cognos報告介面。如果您要讓使用者與Cognos報告介面互動、則必須從遠端公開。

我們可以想像DWH可能不需要曝光的環境、可能是報告作者只是將RDP連線到DWH伺服器、然後在那裡製作和排程報告、同時將所有報告排程為透過SMTP傳送、或寫入遠端檔案系統。

傳入**MySQL**（**TCP 3306**）。只有當貴組織與DWH資料有任何MySQL型整合時、才需要公開此連接埠、您是否要從各種DWH資料夾擷取資料、以便擷取至其他應用程式、例如CMDB、計費系統等

分析緩慢的電腦效能

如果您接到網路使用者的來電、抱怨他們的電腦執行速度緩慢、您就需要分析主機效能並識別受影響的資源。

開始之前

在此範例中、呼叫者提供主機名稱。

步驟

1. 在瀏覽器中開啟Insight。
2. 在「搜尋資產」方塊中輸入主機名稱、然後在搜尋結果中按一下主機名稱。

   此時將打開資源的_asset頁面。

3. 在主機的資產頁面上、檢查頁面中央的效能圖表。除了通常預先選取的延遲和IOPS之外、您可能還需要顯示不同類型的資料。按一下其他類型資料的核取方塊、例如：處理量、記憶體、CPU或IP處理量、視裝置類型而定。
4. 若要在圖表上顯示某點的說明、請將滑鼠指標放在該點上。
5. 您也可以將頁面頂端的選取範圍變更為3小時至7天或所有可用資料。
6. 檢查*最高關聯資源*清單、查看是否有其他資源與基礎資源具有相同的活動模式。

   清單中的第一個資源永遠是基礎資源。

   a. 按一下關聯資源旁的連結百分比、查看關聯的活動模式是否適用於基礎資源和其他資源的IOPS或CPU。
   b. 按一下關聯資源的核取方塊、將其資料新增至效能圖表。
   c. 按一下關聯資源的連結名稱、以顯示其資產頁面。
7. 如本範例所示、若為VM、請在*最高相關資源*中找出儲存資源池、然後按一下儲存資源池名稱。

分析相關資源

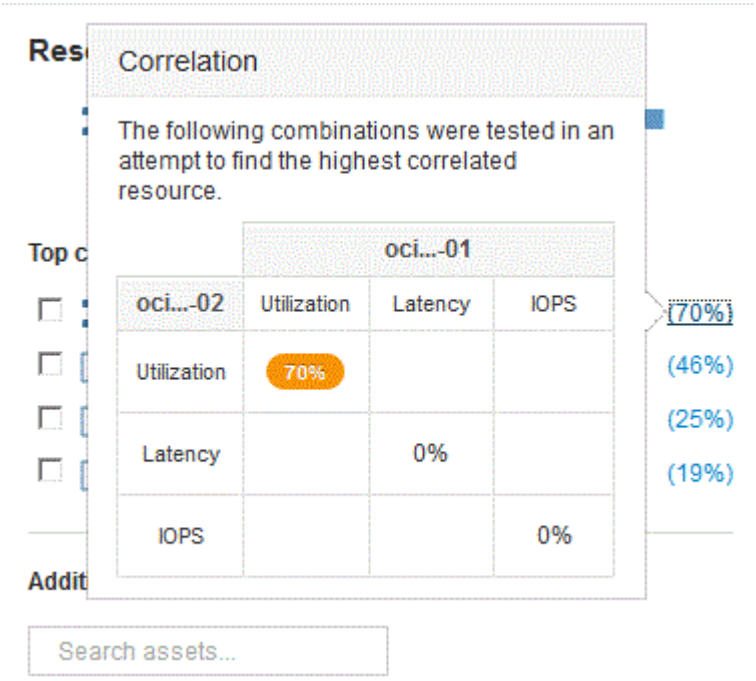
當您在研究效能問題時、開啟裝置的_asset頁面_時、您應該使用最重要的關聯資源清單來精簡效能圖表中顯示的資料。百分比較高的資源表示資源與基礎資源具有類似的活動。

關於這項工作

您正在調查效能問題、並開啟裝置的資產頁面。

步驟

1. 在*最高關聯資源*清單中、第一個資源是基礎資源。清單中的關聯資源會依第一個裝置的關聯活動百分比排序。按一下連結的關聯百分比以查看詳細資料。在此範例中、70%的關聯是在使用率中、因此基礎資源和此相關資源的使用率都同樣高。



2. 若要將關聯資源新增至效能圖表、請選取您要新增之資源*頂端關聯資源*清單中的核取方塊。根據預設、每個資源都會提供可用的總資料、但您可以從核取方塊的功能表中選取「只讀取」或「只寫入資料」。

   圖表中的每個資源都有不同的色彩、因此您可以比較每個資源的效能測量值。只會針對所選的測量指標繪製適當類型的資料。例如、CPU資料不包含讀取或寫入度量、因此只有「總資料」可用。

3. 按一下關聯資源的連結名稱、以顯示其資產頁面。
4. 如果您在分析中未看到您認為應該考慮的最高關聯資源中列出某個資源、您可以使用*搜尋資產*方塊來尋找該資源。

Fibre Channel環境監控

使用《Insight Fibre Channel》資產頁面、您可以監控環境中的Fabric效能與庫存、並留意可能造成問題的任何變更OnCommand 。

Fibre Channel資產頁面

Insight的資產頁面提供有關資源、其拓撲（裝置及其連線）、效能圖表及相關資源表格的摘要資訊。您可以使用Fabric、交換器和連接埠資產頁面來監控光纖通道環境。在排除光纖通道問題時、特別實用的功能是每個連接埠資產的效能圖表、其中會顯示所選主要貢獻者連接埠的流量。此外、您也可以在此圖表中顯示緩衝區對緩衝區的信用度量和連接埠錯誤、Insight會針對每個度量顯示個別的效能圖表。

連接埠度量的效能原則

Insight可讓您建立效能原則、以監控網路的各種臨界值、並在超過臨界值時發出警示。您可以根據可用的連接埠度量來建立連接埠的效能原則。發生違反臨界值的情況時、Insight會在相關的資產頁面中顯示紅色圓圈、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中、偵測並報告臨界值。

存留時間（**TTL**）和縮減取樣的資料

從OnCommand Insight 7.3開始、資料保留或存留時間（TTL）已從7天增加至90天。因為這意味著圖表和表格的資料處理量會增加許多、而且可能會有成千上萬個資料點、因此資料會在顯示之前先進行縮減取樣。

縮減取樣提供圖表中資料的統計近似、讓您能夠有效地概述資料、而不需要顯示每個資料點、同時維持所收集資料的正確檢視。

為何需要縮減取樣？

Insight 7.3可將資料的存留時間（TTL）增加至90天。這表示準備資料以在圖表中顯示所需的處理量增加。為了讓圖表快速且有效率地顯示、資料會以保留圖表整體圖形的方式進行縮減取樣、而不需要處理該圖表的每個資料點。

> 在降級取樣期間不會遺失任何實際資料。您可以依照下列步驟、選擇檢視圖表的實際資料、而非縮減取樣資料。

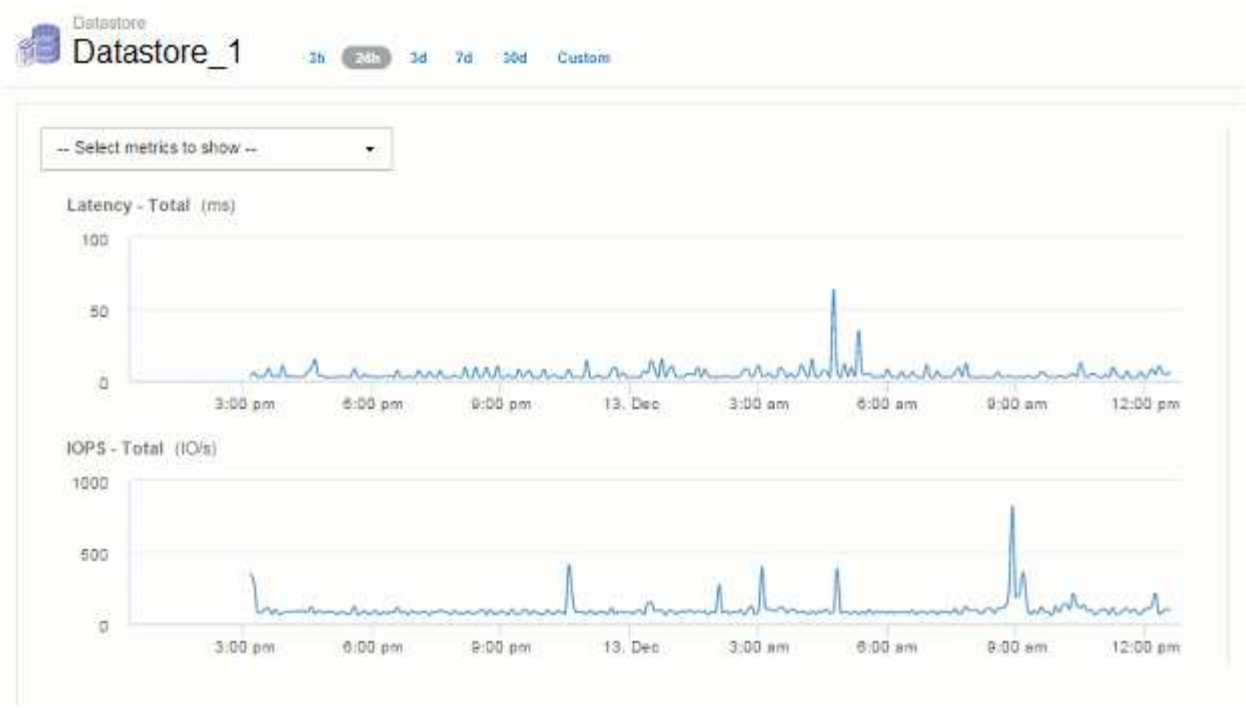
縮減取樣的運作方式

資料會在下列情況下降級：

- 如果您所選的時間範圍包含7天或更短的資料、則不會發生降級。圖表會顯示實際資料。
- 如果您所選的時間範圍包含超過7天的資料、但資料點少於1、000個、則不會進行降級取樣。圖表會顯示實際資料。
- 如果您所選的時間範圍包含超過7天的資料和超過1、000個資料點、則會將資料降級。圖表會顯示近似資料。

下列範例顯示正在進行降級取樣。第一個圖例顯示資料存放區資產頁面上24小時內的延遲和IOPS圖表、如資產頁面時間選取器上的* 24h*所示。您也可以選取*自訂*並將時間範圍設定為相同的24小時週期、以查看相同的資料。

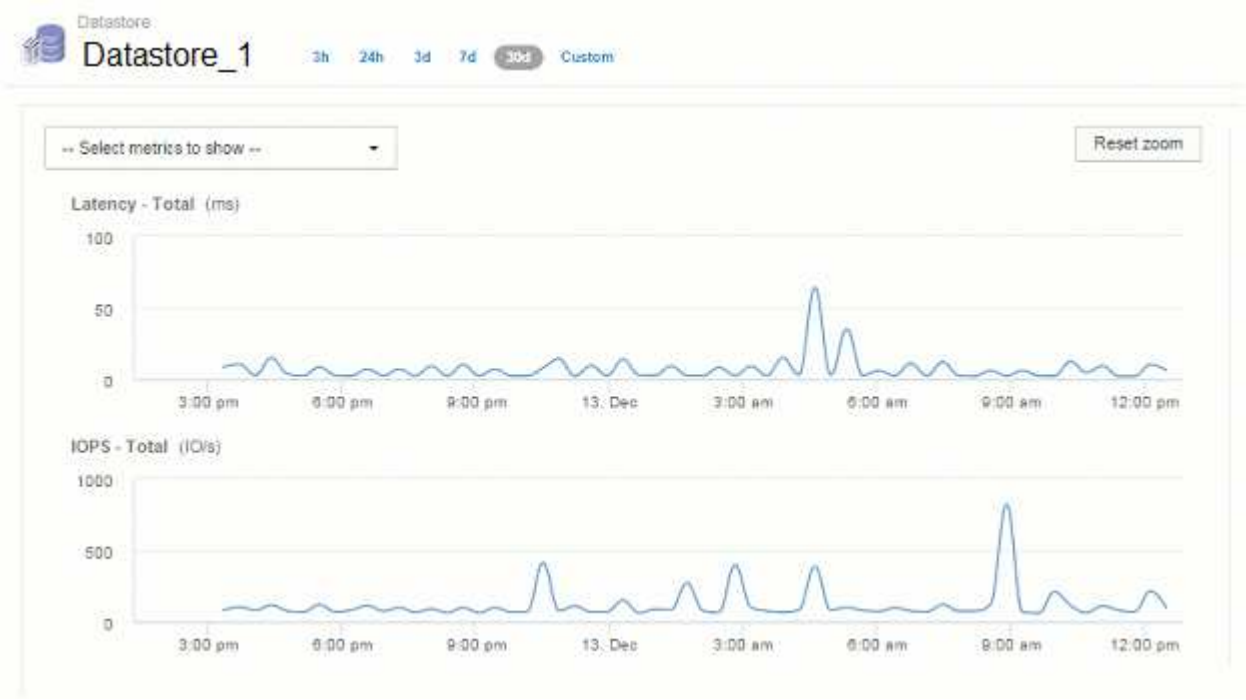
由於我們選擇的時間範圍少於7天、而且要記錄的資料點少於1、000個、因此顯示的資料是實際資料。不會發生降級取樣。



不過、如果您要檢視資料、請在資產頁面時間選取器上選擇* 30d*、 或是將自訂時間範圍設定為7天以上（或Insight在所選時間期間收集超過1、000個資料樣本）、則會先將資料降級、然後再顯示。當您放大縮小取樣的圖表時、畫面會繼續顯示近似的資料。

> 當您放大縮小取樣的圖表時、縮放是數位縮放。螢幕會繼續顯示近似資料。

您可以在下圖中看到這一點、其中時間範圍會先設定為30d、然後再放大圖表、以顯示與上述相同的24小時期間。



縮減取樣的圖表顯示的時間與上方「實際」圖表相同、因此這些圖表的一般形狀相同、可讓您快速找出效能資料中有趣的高峰或低谷。

由於資料的縮減取樣方式、比較縮減取樣與時、圖表線可能會稍微偏離實際資料、以便更妥善地對齊圖形。然而、差異極小、不會影響所顯示資料的整體準確度。

縮減取樣圖表上的違規行為

檢視下取樣圖表時、請注意、不會顯示違規情形。若要查看違規情形、您可以執行下列兩項操作之一：

- 選取資產頁面時間選取器中的「自訂」、然後輸入7天內的時間範圍、即可檢視該時間範圍的實際資料。將游標暫留在每個紅點上。工具提示會顯示發生的違規情形。
- 請記下時間範圍、並在違規儀表板中找到違規。

資源清冊歷史記錄的剪除

從7.3.2版開始、Insight會將庫存（基礎）變更記錄保留90天。先前版本的Insight會保留安裝時的所有庫存變更記錄。從舊版Insight升級之後、舊版的庫存記錄會保留至90天。

升級OnCommand Insight 至目前版本的更新版本之後、歷史記錄會被刪除至最近的90天。洞見會以每天一次的30天時間區塊、從最早的區塊開始、將歷史刪除、直到90天的歷史仍有其價值。因此、為了維持90天的庫存變更歷史記錄、我們每天都會刪除歷史記錄。

VM的NAS路徑

支援NAS路徑、可讓虛擬機器連接至儲存共享區OnCommand Insight 。這些路徑類似於主機到儲存共用的NAS路徑。當允許VM的IP位址存取共用區時、就會建立NAS路徑。

虛擬機器的NAS路徑會顯示在「內部磁碟區」登陸頁面上。此頁面包含來賓掛載儲存資源Widget、可識別VM可存取的內部Volume。

- 當虛擬機器能夠存取後端共用時、就會建立NAS路徑。不知道虛擬機器是否存取共用區。
- 關聯計算是以延遲和IOPs為基礎、不包括VM有NAS路徑可通往後端儲存設備的情況。
- 使用者可以依啟動器IP位址查詢共用區、但不支援依路徑查詢。

「內部Volume」的「運算資源」表現在也會顯示具有NAS路徑的VM。針對每個VM、CPU和記憶體、都會提供使用率和效能資料。

資料倉儲影響

升級OnCommand Insight 到版本號為37的7.3版之後、資料倉儲的變更內容如下：

- 會從Inventory資料倉儲中移除dwh_inventory.ns_logical表格、並以檢視取代。

  所有包含NFS路徑表的Insight 7.2.x報告都會保留下來。

- 會將dwh_inventory.ns_cr_logical表格新增至Inventory資料倉儲、其中包含下列項目：
  - 運算資源
  - 內部Volume
  - 儲存設備

- NAS共用

容量即時間序列

利用NetApp 7.3.1、容量資訊會報告並記錄為時間序列資料OnCommand Insight 。

過去、從資料來源取得的容量資訊只是「時間點」（PIT）資料、這表示無法在圖表中作為時間序列資料使用。現在、資產的容量值可透過下列方式做為時間序列資料：

- 以表格、小工具、專家檢視和時間序列資料顯示的任何位置製作圖表
- 使用現有的語義、套用至效能臨界值、但有違規情形
- 在適當的情況下、用於運算式與其他效能計數器

請注意、如果您從先前版本的Insight升級、查詢或自訂儀表板篩選器中使用的舊PIT容量值將會被時間序列容量資料取代。相較於先前Insight版本中的同等資料、這可能會導致容量資料的報告或篩選方式發生小幅變更。

OCI 資料收集器支援對照表

Data Collector Support Matrix 提供 OCI 支援的 Data Collectors 參考資料、包括廠商和機型資訊。

HP Enterprise 3PAR / Alletra 9000/ Primera StoreServ 儲存設備

此資料收集器支援的機型和版本：

模型	韌體版本
HPE_3PAR 20450 HPE_3PAR 7200 HPE_3PAR 7400 HPE_3PAR 7440c HPE_3PAR 7450c HPE_3PAR 8200 HPE_3PAR 8400 HPE_3PAR 8440 HPE_3PAR 8450 HPE_3PAR A670 HP_3P7200 P400c HP 7200_P400c	3.2.2 （ MU2 ） 3.2.2 （ MU4 ） 3.2.2 （ MU6 ） 3.3.1 （ MU2 ） 3.3.1 （ MU5 ） 4.4.1 版本類型：標準支援版本

此資料收集器支援的產品：

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
基礎					
312					

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
		目標Volume	實作	SSH	
		技術	實作	SSH	改變儲存效率的
	Volume	自動層級原則識別碼	實作	SSH	動態層級原則識別碼
		自動分層	實作	SSH	指出此儲存集區是否參與與其他集區的自動分層
		容量	實作	SSH	Snapshot使用容量（單位：MB）
		名稱	實作	SSH	
		總原始容量	實作	SSH	總原始容量（陣列上所有磁碟的總和）
		備援	實作	SSH	備援層級
		儲存資源池ID	實作	SSH	
		資源隨需配置	實作	SSH	
		類型	落差	SSH	
		UUID	實作	SSH	
		已用容量	實作	SSH	
		虛擬化	實作	SSH	這是儲存虛擬化設備嗎？
	Volume Map	LUN	實作	SSH	後端LUN的名稱
		傳輸協定控制器	實作	SSH	
		儲存連接埠	實作	SSH	
	Volume遮罩	啟動器	實作	SSH	
		傳輸協定控制器	實作	SSH	
		儲存連接埠	實作	SSH	
	Volume Ref	名稱	實作	SSH	
		儲存IP	實作	SSH	
	WWN別名	主機別名	實作	SSH	
		物件類型	實作	SSH	
		來源	實作	SSH	
		WWN	實作	SSH	

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
效能					

		Snapshot已用容量	實作	SMI-S	
		Snapshot使用容量	實作	SMI-S	報告為時間序列
產品	類別	功能屬性	狀態	使用的傳輸協定	其他資訊
	Volume	快取命中率讀取	實作	SMI-S	
		快取命中率總計	實作	SMI-S	
		快取命中率寫入	實作	SMI-S	
		原始容量	實作	SMI-S	
		總容量	實作	SMI-S	
		已用容量	實作	SMI-S	
		容量使用率	實作	SMI-S	
		寫入的容量比率	實作	SMI-S	
		IOPS讀取	實作	SMI-S	磁碟上的讀取IOP 數
		IOPS總計	實作	SMI-S	
		IOPS寫入	實作	SMI-S	
		金鑰	實作	SMI-S	
		延遲讀取	實作	SMI-S	
		總延遲	實作	SMI-S	
		延遲寫入	實作	SMI-S	
		部分封鎖比率	實作	SMI-S	
		伺服器ID	實作	SMI-S	
		處理量讀取	實作	SMI-S	
		總處理量	實作	SMI-S	平均磁碟總速率（橫跨所有磁碟的讀寫）、單位為MB/s
		處理量寫入	實作	SMI-S	
		寫入擱置中	實作	SMI-S	等待寫入總計

此資料收集器使用的管理 API ：

API	使用的傳輸協定	使用傳輸層傳輸層傳輸協定	使用的傳入連接埠	使用的傳出連接埠	支援驗證	僅需要「唯讀」認證	支援加密	防火牆易用（靜態連接埠）
3PAR SMI-S	SMI-S	HTTP / HTTPS	5988/5989		是的	是的	是的	是的
3PAR CLI	SSH	SSH	22		是的	錯	是的	是的

Amazon AWS EC2

此資料收集器支援的機型和版本：

API 版本：

- 2014-10-01

此資料收集器支援的產品：

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
基礎					
320					

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

		製造商	實作	HTTPS	
		名稱	實作	HTTPS	
產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
	資訊	API說明	實作	HTTPS	
		API名稱	實作	HTTPS	
		API版本	實作	HTTPS	
		資料來源名稱	實作	HTTPS	資訊
		日期	實作	HTTPS	
		建立者ID	實作	HTTPS	
		建立者金鑰	實作	HTTPS	

此資料收集器使用的管理 API ：

API	使用的傳輸協定	使用傳輸層傳輸層傳輸協定	使用的傳入連接埠	使用的傳出連接埠	支援驗證	僅需要「唯讀」認證	支援加密	防火牆易用（靜態連接埠）
EC2 API	HTTPS	HTTPS	443		是的	是的	是的	是的

Brocade光纖通道交換器

此資料收集器支援的機型和版本：

模型	韌體版本
184.0 Brocade 200E Brocade 300E Brocade Brocade 4024 內嵌式 Brocade 4100 Brocade 4900 Brocade 5000 Brocade 5100 Brocade 5480 內嵌式 Brocade 6505 Brocade 6510 Brocade 6520 Brocade 7800 Brocade 7840 Brocade DCX8510-4 Brocade DCX8510-8 Brocade G610 Brocade G620 Brocade G630 Brocade M5424 內嵌式 Brocade M6505 Brocade VA-40FC Brocade X6-4 Brocade X6-8 Brocade X8-8	v5.3.0a v6.1.0c v6.1.9.1.3 v9.1.9.7.2.1 v6.2d v6.2.2d v6.2.2d v6.3.2b v6.4.2d v6.4.8.2.1d

此資料收集器支援的產品：

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
基礎					

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

		類型	落差	SSH	
		vSAN已啟用	實作	SSH	
產品	類別	功能屬性	狀態	使用的傳輸協定	其他資訊
	WWN別名	主機別名	實作	SSH	
		物件類型	實作	SSH	
		來源	實作	SSH	
		WWN	實作	SSH	
	區域	區域名稱	實作	SSH	
	區域成員	類型	落差	SSH	
		WWN	實作	SSH	
	分區功能	作用中組態	實作	SSH	
		組態名稱	實作	SSH	
		WWN	實作	SSH	

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
效能					
326					

		總流量影格速率	實作	SNMP	
		交通路況影格速率	實作	SNMP	
產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
		平均影格大小	實作	SNMP	流量的平均影格大小
		傳輸框架	實作	SNMP	流量平均影格大小
		已接收流量	實作	SNMP	
		總流量	實作	SNMP	
		流量傳輸率	實作	SNMP	
		已接收流量使用率	實作	SNMP	
		總流量使用率	實作	SNMP	總流量使用率
		流量傳輸使用率	實作	SNMP	

此資料收集器使用的管理 API ：

API	使用的傳輸協定	使用傳輸層傳輸層傳輸協定	使用的傳入連接埠	使用的傳出連接埠	支援驗證	僅需要「唯讀」認證	支援加密	防火牆易用（靜態連接埠）
Brocade SNMP	SNMP	SNMPv1、SNMPv2、v3	161		是的	是的	是的	是的
Brocade SSH	SSH	SSH	22		錯	錯	是的	是的
資料來源精靈組態	手動輸入				是的	是的	是的	是的

Brocade網路顧問HTTP

此資料收集器支援的機型和版本：

API 版本：

- 14.4.5

此資料收集器支援的產品：

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
基礎	網路	名稱	實作	HTTP/S	
		WWN	實作	HTTP/S	
	資訊	API說明	實作	HTTP/S	
		API名稱	實作	HTTP/S	
		API版本	實作	HTTP/S	
		資料來源名稱	實作	HTTP/S	資訊
		日期	實作	HTTP/S	
		建立者ID	實作	HTTP/S	
		建立者金鑰	實作	HTTP/S	
	WWN別名	主機別名	實作	HTTP/S	
		物件類型	實作	HTTP/S	
		來源	實作	HTTP/S	
		WWN	實作	HTTP/S	
	區域	區域名稱	實作	HTTP/S	
	區域成員	類型	落差	HTTP/S	
		WWN	實作	HTTP/S	
	分區功能	作用中組態	實作	HTTP/S	
		組態名稱	實作	HTTP/S	
		WWN	實作	HTTP/S	

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
效能	連接埠	BB Credit Zero Total	實作	HTTP/S	BB Credit Zero Total
		BB Credit Zero 已傳輸	實作	HTTP/S	BB Credit Zero 已傳輸
		傳輸的 BB Credit Zero M	實作	HTTP/S	傳輸的 BB Credit Zero M
		連接埠錯誤類別 3 捨棄	實作	HTTP/S	
		連接埠錯誤 CRC	實作	HTTP/S	連接埠錯誤 CRC
		連接埠錯誤環境	實作	HTTP/S	連接埠錯誤環境
		連接埠錯誤短訊框	實作	HTTP/S	短框架導致連接埠錯誤
		連接埠錯誤連結失敗	實作	HTTP/S	連接埠錯誤連結失敗
		連接埠錯誤訊號遺失	實作	HTTP/S	連接埠錯誤訊號遺失
		連接埠錯誤同步遺失	實作	HTTP/S	連接埠錯誤同步遺失
		連接埠錯誤傳輸捨棄逾時	實作	HTTP/S	連接埠錯誤逾時捨棄
		連接埠錯誤總數	實作	HTTP/S	連接埠錯誤總計

此資料收集器使用的管理 API ：

API	使用的傳輸協定	使用傳輸層傳輸層傳輸協定	使用的傳入連接埠	使用的傳出連接埠	支援驗證	僅需要「唯讀」認證	支援加密	防火牆易用（靜態連接埠）
Brocade網路顧問REST API	HTTP / HTTPS	HTTP / HTTPS	80/443		是的	是的	是的	是的

Cisco MDS 與 Nexus Fabric 交換器

此資料收集器支援的機型和版本：

模型	韌體版本
8978-E16 DS-C9124-2-K9 DS-C9124-K9 DS-C9124-K9 DS-C9139148-K9 DS-C9148-K9 DS-C9148-32P-DS-DS-C9148-48P-K9	3.2(2c)4.1(3a)5.0(1a)5.0(3)N2(3.13e)5.0(3)N2(44.04i)5.0(3)N2(4.13j)5.0222a(44.21k)8.2(8)5.2(8)5.2(8)5.2(8c)5.2(8)7.2(7)6.2(7)

此資料收集器支援的產品：

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
基礎					

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

		物件類型	實作	SNMP	
		來源	實作	SNMP	
產品	類別	功能屬性	狀態	使用的傳輸協定	其他資訊
	區域	區域名稱	實作	SNMP	
		區域類型	實作	SNMP	
	區域成員	類型	落差	SNMP	
		WWN	實作	SNMP	
	分區功能	作用中組態	實作	SNMP	
		組態名稱	實作	SNMP	
		預設分區行為	實作	SNMP	
		合併控制	實作	SNMP	
		WWN	實作	SNMP	

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
效能					
334					

		傳輸框架	實作	SNMP	流量平均影格大小
產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
		總流量	實作	SNMP	
		流量傳輸率	實作	SNMP	
		已接收流量使用率	實作	SNMP	
		總流量使用率	實作	SNMP	總流量使用率
		流量傳輸使用率	實作	SNMP	

此資料收集器使用的管理 API ：

API	使用的傳輸協定	使用傳輸層傳輸層傳輸協定	使用的傳入連接埠	使用的傳出連接埠	支援驗證	僅需要「唯讀」認證	支援加密	防火牆易用（靜態連接埠）
Cisco SNMP	SNMP	SNMPv1（僅限庫存）、SNMP v2、v3	161		是的	是的	是的	是的

EMC Celerra（SSH）

此資料收集器支援的機型和版本：

模型	韌體版本
NSX VG8 VNX5600	5.5.38-1 7.1.76-4 7.1.79-8.1.9-184

此資料收集器支援的產品：

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
基礎					
336					

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

					容量（所有備援磁碟的總和）
		虛擬化	實作	SSH	這是儲存虛擬化設備嗎？
產品	類別	功能/屬性	狀態	使用的傳輸協定	註解
	儲存資源池	資料分配容量	落差	SSH	分配給資料的容量
		資料使用容量	實作	SSH	
		已啟用重複資料刪除	實作	SSH	是否在儲存資源池上啟用重複資料刪除功能
		包括在DWh容量中	實作	SSH	從 ACQ 控制 DWH 容量感興趣的儲存池
		名稱	實作	SSH	
		RAID群組	實作	SSH	指出此storagePool是否為RAID群組
		原始對可用比率	實作	SSH	從可用容量轉換為原始容量的比率
		Snapshot分配容量	落差	SSH	快照的已分配容量（以MB為單位）
		Snapshot已用容量	實作	SSH	
		儲存資源池ID	實作	SSH	
		支援精簡配置	實作	SSH	此內部磁碟區是否支援其上的磁碟區層精簡配置
		已分配容量總計	實作	SSH	
		總使用容量	實作	SSH	總容量（單位：MB）
		類型	落差	SSH	
		虛擬化	實作	SSH	這是儲存虛擬化設備嗎？

此資料收集器使用的管理 API ：

API	使用的傳輸協定	使用傳輸層傳輸層傳輸協定	使用的傳入連接埠	使用的傳出連接埠	支援驗證	僅需要「唯讀」認證	支援加密	防火牆易用（靜態連接埠）
Celerra CLI	SSH	SSH			是的	錯	是的	是的

EMC CLARiiON（導航CLI）

此資料收集器支援的機型和版本：

API 版本	模型	韌體版本
6.28 7.32 7.33	CX4-120 VNX5200 VNX5400 VNX5500 VNX5600 VNX5700 VNX5800 VNX7600 VNX8000	04.28.000.5.008 05.32.000.5.218 05.32.000.5.219 05.32.000.5.221 05.32.000.5.249 05.33.009.5.155 05.33.009.5.184 05.33.009.5.186 05.33.009.5.218 05.33.009.5.231 05.33.009.5.238 05.33.021.5.021.256 5.33.021.032.66

此資料收集器支援的產品：

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
基礎					
342					

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

		傳輸協定控制器	實作	CLI	
		儲存連接埠	實作	CLI	
產品	類別	類型/屬性	狀態	使用的傳輸協定	其他資訊
	Volume成員	容量	實作	CLI	Snapshot使用容量（單位：MB）
		名稱	實作	CLI	
		排名	實作	CLI	
		總原始容量	實作	CLI	總原始容量（陣列上所有磁碟的總和）
		備援	實作	CLI	備援層級
		儲存資源池ID	實作	CLI	
		已用容量	實作	CLI	
	WWN別名	主機別名	實作	CLI	
		IP	實作	CLI	
		物件類型	實作	CLI	
		來源	實作	CLI	
		WWN	實作	CLI	

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
效能					
348					

		量			
		金鑰	實作	CLI	
產品	類別	特徵屬性	狀態	使用的傳輸協定	其他資訊
	儲存資源池	已配置的容量	實作	CLI	
		原始容量	實作	CLI	
		總容量	實作	CLI	
		已用容量	實作	CLI	
		過度使用容量比率	實作	CLI	報告為時間序列
		容量使用率	實作	CLI	
		金鑰	實作	CLI	
		其他總容量	實作	CLI	
		其他已用容量	實作	CLI	
		伺服器ID	實作	CLI	
		Snapshot保留容量	實作	CLI	
		Snapshot已用容量	實作	CLI	
		Snapshot使用容量比率	實作	CLI	報告為時間序列
	Volume	原始容量	實作	CLI	
		總容量	實作	CLI	
		已用容量	實作	CLI	
		容量使用率	實作	CLI	
		金鑰	實作	CLI	
		伺服器ID	實作	CLI	

此資料收集器使用的管理 API ：

API	使用的傳輸協定	使用傳輸層傳輸層傳輸協定	使用的傳入連接埠	使用的傳出連接埠	支援驗證	僅需要「唯讀」認證	支援加密	防火牆易用（靜態連接埠）
新版CLI	CLI		6389、2162、2163、443（HTTPS）/80（HTTP）		是的	是的	是的	錯

EMC資料網域（SSH）

此資料收集器支援的機型和版本：

模型	韌體版本
DD2500 DD4200 DD4500 DD6300 DD670 DD6800 DD6900 DD9300 DD9400 DD990	5.4.6.0-503967 5.5.0.9-471508 5.5.2.1-486308 6.1.0.5-567091 6.2.30-663869 6.2.1.50-680189 7.10.1.1.15-1078832 7.10.1.1.20-1090468 7.2.0.70-686757.6.0.40-691389

此資料收集器支援的產品：

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
基礎					

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

					容量（所有備援磁碟的總和）
		虛擬化	實作	SSH	這是儲存虛擬化設備嗎？
產品	類別	功能/屬性	狀態	使用的傳輸協定	說明
	儲存資源池	資料分配容量	落差	SSH	分配給資料的容量
		資料使用容量	實作	SSH	
		已啟用重複資料刪除	實作	SSH	是否在儲存資源池上啟用重複資料刪除功能
		重複資料刪除技術的節約效益	實作	SSH	重複資料刪除技術的節約比率（以百分比表示）
		包括在DWh容量中	實作	SSH	從 ACQ 控制 DWH 容量感興趣的儲存池
		名稱	實作	SSH	
		其他已分配容量	落差	SSH	分配給其他（非資料而非快照）的容量
		其他已用容量（MB）	實作	SSH	資料與快照以外的任何容量
		實體磁碟容量（MB）	實作	SSH	用作儲存資源池的原始容量
		RAID群組	實作	SSH	指出此storagePool是否為RAID群組
		原始對可用比率	實作	SSH	從可用容量轉換為原始容量的比率
		儲存資源池ID	實作	SSH	
		支援精簡配置	實作	SSH	此內部磁碟區是否支援其上的磁碟區層精簡配置
		已分配容量總計	實作	SSH	
		總使用容量	實作	SSH	總容量（單位：MB）
		類型	落差	SSH	
		虛擬化	實作	SSH	這是儲存虛擬化設備嗎？

此資料收集器使用的管理 API ：

API	使用的傳輸協定	使用傳輸層傳輸層傳輸協定	使用的傳入連接埠	使用的傳出連接埠	支援驗證	僅需要「唯讀」認證	支援加密	防火牆易用（靜態連接埠）
Data Domain CLI	SSH	SSH	22		是的	是的	是的	是的

EMC ECS

此資料收集器支援的機型和版本：

模型	韌體版本
ECS	3.6.1.3 3.7.0.6 3.8.0.6 3.8.1.1

此資料收集器支援的產品：

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
基礎					

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

	儲存節點	名稱	實作	HTTPS	
		UUID	實作	HTTPS	
產品	類別	版本/屬性	狀態	使用的傳輸協定	軟體廠商
	儲存資源池	包括在DWh容量中	實作	HTTPS	從 ACQ 控制 DWH 容量感興趣的儲存池
		名稱	實作	HTTPS	
		實體磁碟容量（MB）	實作	HTTPS	用作儲存資源池的原始容量
		RAID群組	實作	HTTPS	指出此storagePool是否為RAID群組
		原始對可用比率	實作	HTTPS	從可用容量轉換為原始容量的比率
		儲存資源池ID	實作	HTTPS	
		支援精簡配置	實作	HTTPS	此內部磁碟區是否支援其上的磁碟區層精簡配置
		已分配容量總計	實作	HTTPS	
		總使用容量	實作	HTTPS	總容量（單位：MB）
		類型	落差	HTTPS	
		虛擬化	實作	HTTPS	這是儲存虛擬化設備嗎？

此資料收集器使用的管理 API ：

API	使用的傳輸協定	使用傳輸層傳輸層傳輸協定	使用的傳入連接埠	使用的傳出連接埠	支援驗證	僅需要「唯讀」認證	支援加密	防火牆易用（靜態連接埠）
EMC ECS REST API	HTTPS	HTTPS	443		是的	是的	是的	是的

Dell EMC Isilon / PowerScale （ CLI ）

此資料收集器支援的機型和版本：

模型	韌體版本
A200 A2000 A300 A3000 F800 H400 H500 H500-4U-Single-128GB-1x1GE-2X10GE SFP+ -30TB-1638GB SSD H700 NL400 NL410 追溯（最近通話時間最後一通）： X210 X400 Sudo python	9.2.1.12 9.4.0.14 9.4.0.17 9.5.0.7 v8.0.0.6 v8.0.0.7

此資料收集器支援的產品：

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
基礎					
362					

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

					免費文字
		UUID	實作	SSH	
產品	類別	物理/屬性	狀態	使用的傳輸協定	其他資訊
	儲存資源池	資料分配容量	落差	SSH	分配給資料的容量
		資料使用容量	實作	SSH	
		包括在DWh容量中	實作	SSH	從 ACQ 控制 DWH 容量感興趣的儲存池
		名稱	實作	SSH	
		實體磁碟容量（MB）	實作	SSH	用作儲存資源池的原始容量
		RAID群組	實作	SSH	指出此storagePool是否為RAID群組
		原始對可用比率	實作	SSH	從可用容量轉換為原始容量的比率
		Snapshot分配容量	落差	SSH	快照的已分配容量（以MB為單位）
		Snapshot已用容量	實作	SSH	
		儲存資源池ID	實作	SSH	
		支援精簡配置	實作	SSH	此內部磁碟區是否支援其上的磁碟區層精簡配置
		已分配容量總計	實作	SSH	
		總使用容量	實作	SSH	總容量（單位：MB）
		類型	落差	SSH	
		虛擬化	實作	SSH	這是儲存虛擬化設備嗎？

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
效能	儲存設備	金鑰	實作	SSH	
		伺服器ID	實作	SSH	
		原始容量	實作	SSH	
		備用原始容量	實作	SSH	備用磁碟的原始容量（所有備援磁碟的總和）
		原始容量失敗	實作	SSH	
		StoragePools容量	實作	SSH	
	儲存節點資料	IOPS讀取	實作	SSH	檔案系統上的讀取IOPs數目
		IOPS寫入	實作	SSH	檔案系統的IOPS寫入
		檔案處理量讀取	實作	SSH	
		檔案系統處理量	實作	SSH	檔案系統處理量寫入
		IOPS讀取	實作	SSH	磁碟上的讀取IOP 數
		IOPS總計	實作	SSH	
		IOPS寫入	實作	SSH	
		金鑰	實作	SSH	
		總延遲	實作	SSH	
		伺服器ID	實作	SSH	
		處理量讀取	實作	SSH	
		總處理量	實作	SSH	平均磁碟總速率（橫跨所有磁碟的讀寫）、單位為MB/s
		處理量寫入	實作	SSH	
		使用率總計	實作	SSH	

此資料收集器使用的管理 API ：

API	使用的傳輸協定	使用傳輸層傳輸層傳輸協定	使用的傳入連接埠	使用的傳出連接埠	支援驗證	僅需要「唯讀」認證	支援加密	防火牆易用（靜態連接埠）
Isilon SSH	SSH	SSH	22		是的	錯	是的	是的

EMC PowerStore REST

此資料收集器支援的機型和版本：

模型	韌體版本
PowerStore 1000T PowerStore 5000T PowerStore 5200T	2.1.1.3.2.1.03.5.0.2

此資料收集器支援的產品：

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
基礎					

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

		UUID	實作		
		已用容量	實作		
產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
	Volume Map	LUN	實作		後端LUN的名稱
		需要遮罩	實作		
		傳輸協定控制器	實作		
		儲存連接埠	實作		
		類型	落差		
	Volume遮罩	啟動器	實作		
		傳輸協定控制器	實作		
		類型	落差		
	WWN別名	主機別名	實作		
		物件類型	實作		
		來源	實作		
		WWN	實作		
效能	儲存設備	原始容量失敗	實作		
		原始容量	實作		
		備用原始容量	實作		備用磁碟的原始容量（所有備援磁碟的總和）
		StoragePools容量	實作		
		IOPS其他	實作		
		IOPS讀取	實作		磁碟上的讀取IOP 數
		IOPS總計	實作		
		IOPS寫入	實作		
		金鑰	實作		
		延遲讀取	實作		
		總延遲	實作		
		延遲寫入	實作		
		伺服器ID	實作		

此資料收集器使用的管理 API ：

API	使用的傳輸協定	使用傳輸層傳輸層傳輸協定	使用的傳入連接埠	使用的傳出連接埠	支援驗證	僅需要「唯讀」認證	支援加密	防火牆易用（靜態連接埠）
EMC PowerStore REST API	HTTPS	HTTPS	443		是的	是的	是的	是的

EMC RecoverPoint（HTTP）

此資料收集器支援的機型和版本：

模型	韌體版本
RecoverPoint	5.1.SP3.P1（g.69） 5.1.SP4.HF1 （h.86 5.4.SP4.P1 （h.89）

此資料收集器支援的產品：

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
基礎					
374					

					免費文字
		UUID	實作	HTTPS	
產品	類別	版本/屬性	狀態	使用的傳輸協定	軟體廠商
	儲存同步	模式	實作	HTTPS	
		模式環境	實作	HTTPS	
		來源儲存設備	實作	HTTPS	
		來源Volume	實作	HTTPS	
		州/省	實作	HTTPS	說明裝置狀態的免費文字
		國家環境	實作	HTTPS	
		目標儲存設備	實作	HTTPS	
		目標Volume	實作	HTTPS	
		技術	實作	HTTPS	改變儲存效率的技術

此資料收集器使用的管理 API ：

API	使用的傳輸協定	使用傳輸層傳輸層傳輸協定	使用的傳入連接埠	使用的傳出連接埠	支援驗證	僅需要「唯讀」認證	支援加密	防火牆易用（靜態連接埠）
RecoverPoint REST API	HTTPS	HTTPS	443		是的	是的	是的	是的

EMC Symmetrix CLI

此資料收集器支援的機型和版本：

API 版本	模型	韌體版本
V10.0.0.0 V10.0.0.3 V10.0.1.0 V10.0.1.3 V10.1.0.0.0 V10.1.0.0.3 V10.1.0.0.6 V9.1.0.15 V9.2.0.0 V9.2.3.0 V9.2.3.4 V9.2.3.6 V9.2.4.1 V9.2.4.2 V9.2.4.6	PMax8000 PowerMax_2000 PowerMax_8000 VMAX-1 VMAX250F VMAX40K VMAX450F VMAX950F	5876.286.194(16F40000) 建置 1155978.479.479(175A0000) 建置 3725978.711.711(175A0000) 建置 175978.714

此資料收集器支援的產品：

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
基礎					
376					

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	設備訊
		已用容量	實作		
		虛擬化	實作		這是儲存虛擬化
		寫入容量	實作		主機寫入此磁碟區的總容量（以MB為單位）
		加密	實作		
		QoS 限制 IOPS	實作		
		QoS限制Mbps	實作		
		儲存群組	實作		
	Volume Map	LUN	實作		後端LUN的名稱
		傳輸協定控制器	實作		
		儲存連接埠	實作		
		類型	落差		
	Volume遮罩	啟動器	實作		
		傳輸協定控制器	實作		
		儲存連接埠	實作		
		類型	落差		
	Volume成員	自動分層	實作		指出此儲存集區是否參與與其他集區的自動分層
		容量	實作		Snapshot使用容量（單位：MB）
		汽缸	實作		
		名稱	實作		
		排名	實作		
		總原始容量	實作		總原始容量（陣列上所有磁碟的總和）
		備援	實作		備援層級
		儲存資源池ID	實作		
		UUID	實作		
	WWN別名	主機別名	實作		
		物件類型	實作		
		來源	實作		
		WWN	實作		

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
效能	Volume	快取命中率讀取	實作		
		快取命中率總計	實作		
		快取命中率寫入	實作		
		原始容量	實作		
		總容量	實作		
		已用容量	實作		
		容量使用率	實作		
		IOPS讀取	實作		磁碟上的讀取IOP 數
		IOPS總計	實作		
		IOPS寫入	實作		
		金鑰	實作		
		延遲讀取	實作		
		總延遲	實作		
		延遲寫入	實作		
		伺服器ID	實作		
		處理量讀取	實作		
		總處理量	實作		平均磁碟總速率（橫跨所有磁碟的讀寫）、單位為MB/s
		處理量寫入	實作		
		寫入擱置中	實作		等待寫入總計

此資料收集器使用的管理 API ：

API	使用的傳輸協定	使用傳輸層傳輸層傳輸協定	使用的傳入連接埠	使用的傳出連接埠	支援驗證	僅需要「唯讀」認證	支援加密	防火牆易用（靜態連接埠）
SYMCLI	CLI		2707		是的	是的	是的	是的
Symmetrix SMI-S	SMI-S	HTTP / HTTPS	5988/5989		是的	錯	錯	是的

Dell Unisphere REST

此資料收集器支援的機型和版本：

API 版本	模型	韌體版本
V10.0.1.3 V10.1.0.0.1 V10.1.0.0.5 V10.1.0.6.V9.2.4.7 V9.2.4.9	PowerMax_2000 PowerMax_2500 PowerMax_8000 PowerMax_8500 VMAX250F VMAX950F	5978.714.714 5978.714.714 組建 6 5978.714.714 組建 61 5978.714.714 組建 85 組建 6079.225.0 組建 127 組建 6079.225.0 組建 216

此資料收集器支援的產品：

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
基礎					

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

		虛擬化	實作	HTTPS	這是儲存虛擬化設備嗎？
		有效使用容量百分比	實作	HTTPS	
產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
	Volume	自動層級原則識別碼	實作	HTTPS	動態層級原則識別碼
		自動分層	實作	HTTPS	指出此儲存集區是否參與與其他集區的自動分層
		容量	實作	HTTPS	Snapshot使用容量（單位：MB）
		磁碟類型	無法使用	HTTPS	
		名稱	實作	HTTPS	
		總原始容量	實作	HTTPS	總原始容量（陣列上所有磁碟的總和）
		備援	實作	HTTPS	備援層級
		儲存資源池ID	實作	HTTPS	
		資源隨需配置	實作	HTTPS	
		類型	落差	HTTPS	
		UUID	實作	HTTPS	
		已用容量	實作	HTTPS	
		虛擬化	實作	HTTPS	這是儲存虛擬化設備嗎？
		儲存群組	實作	HTTPS	
	Volume Map	LUN	實作	HTTPS	後端LUN的名稱
		傳輸協定控制器	實作	HTTPS	
		儲存連接埠	實作	HTTPS	
		類型	落差	HTTPS	
	Volume遮罩	啟動器	實作	HTTPS	
		傳輸協定控制器	實作	HTTPS	
		儲存連接埠	實作	HTTPS	
		類型	落差	HTTPS	
	WWN別名	主機別名	實作	HTTPS	
		物件類型	實作	HTTPS	
		來源	實作	HTTPS	
		WWN	實作	HTTPS	

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
效能					

					為MB/s
		處理量寫入	實作	HTTPS	
產品	類別	特徵/指標	狀態	使用的傳輸協定	其他資訊
	儲存設備	快取命中率讀取	實作	HTTPS	
		快取命中率總計	實作	HTTPS	
		快取命中率寫入	實作	HTTPS	
		原始容量失敗	實作	HTTPS	
		原始容量	實作	HTTPS	
		備用原始容量	實作	HTTPS	備用磁碟的原始容量（所有備援磁碟的總和）
		StoragePools容量	實作	HTTPS	
		IOPS其他	實作	HTTPS	
		IOPS讀取	實作	HTTPS	磁碟上的讀取IOP 數
		IOPS總計	實作	HTTPS	
		IOPS寫入	實作	HTTPS	
		金鑰	實作	HTTPS	
		延遲讀取	實作	HTTPS	
		總延遲	實作	HTTPS	
		延遲寫入	實作	HTTPS	
		伺服器ID	實作	HTTPS	
		處理量讀取	實作	HTTPS	
		總處理量	實作	HTTPS	平均磁碟總速率（橫跨所有磁碟的讀寫）、單位為MB/s
		處理量寫入	實作	HTTPS	
		寫入擱置中	實作	HTTPS	等待寫入總計

此資料收集器使用的管理 API ：

API	使用的傳輸協定	使用傳輸層傳輸層傳輸協定	使用的傳入連接埠	使用的傳出連接埠	支援驗證	僅需要「唯讀」認證	支援加密	防火牆易用（靜態連接埠）
Dell Unisphere API	HTTPS	HTTPS	443		是的	是的	是的	是的

EMC VNX（SSH）

此資料收集器支援的機型和版本：

模型	韌體版本
VNX5300 VNX5400 VNX5800 VNX7500	05.32.000.5.219 05.32.000.5.221 05.32.000.5.225 05.33.009.5.186

此資料收集器支援的產品：

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
基礎					
392					

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

		類型	落差	SSH	
		虛擬化	實作	SSH	這是儲存虛擬化
產品	類別	功能/屬性	狀態	使用的傳輸協定	設備訊
	Volume	自動層級原則識別碼	實作	SSH	動態層級原則識別碼
		自動分層	實作	SSH	指出此儲存集區是否參與與其他集區的自動分層
		容量	實作	SSH	Snapshot使用容量（單位：MB）
		磁碟群組	實作	SSH	磁碟群組類型
		磁碟類型	無法使用	SSH	
		交會路徑	實作	SSH	
		名稱	實作	SSH	
		總原始容量	實作	SSH	總原始容量（陣列上所有磁碟的總和）
		備援	實作	SSH	備援層級
		儲存資源池ID	實作	SSH	
		資源隨需配置	實作	SSH	
		類型	落差	SSH	
		UUID	實作	SSH	
		已用容量	實作	SSH	
	Volume Map	LUN	實作	SSH	後端LUN的名稱
		傳輸協定控制器	實作	SSH	
		儲存連接埠	實作	SSH	
		類型	落差	SSH	
	Volume遮罩	啟動器	實作	SSH	
		傳輸協定控制器	實作	SSH	
		儲存連接埠	實作	SSH	
		類型	落差	SSH	
	WWN別名	主機別名	實作	SSH	
		IP	實作	SSH	
		物件類型	實作	SSH	
		來源	實作	SSH	
		WWN	實作	SSH	

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
效能					
396					

		其他總容量	實作	SSH	
		其他已用容量	實作	SSH	
產品	類別	特徵屬性	狀態	使用的傳輸協定	其他資訊
	Volume	原始容量	實作	SSH	
		總容量	實作	SSH	
		已用容量	實作	SSH	
		容量使用率	實作	SSH	
		金鑰	實作	SSH	
		伺服器ID	實作	SSH	

此資料收集器使用的管理 API ：

API	使用的傳輸協定	使用傳輸層傳輸層傳輸協定	使用的傳入連接埠	使用的傳出連接埠	支援驗證	僅需要「唯讀」認證	支援加密	防火牆易用（靜態連接埠）
VNX SSH 和 CLI	SSH	SSH	22		是的	錯	是的	是的

EMC VNXe 與 Unity Unisphere （ CLI ）

此資料收集器支援的機型和版本：

模型	韌體版本
Unity 300 Unity 300F Unity 350F Unity 450F Unity 480F Unity 550F Unity 600 Unity 600F Unity 650F Unity 680 Unity 680F Unity 880 Unity 880F VNXe3200	3.1.17.102239064.2.3.96706354.5.0.5.001 5.0.2.0.5.009 5.0.6.0.005.008.0.7.0.005.008.0.5.0085.1.0.5.394.2.0.5.007.2.0.5.007.1.2.0.5.00751.3.0.5.0035.2.0.0135.2.2.0.5.004.5.0.5.005.3.0.5.1205.3.1.0.5.008.0.005.4.0.0.5.094

此資料收集器支援的產品：

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
基礎					
398					

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

		類型	落差	HTTPS	
		虛擬化	實作	HTTPS	這是儲存虛擬化設備
產品	類別	功能/屬性	狀態	使用的傳輸協定	訊
	儲存同步	模式	實作	HTTPS	
		模式環境	實作	HTTPS	
		來源儲存設備	實作	HTTPS	
		來源Volume	實作	HTTPS	
		州/省	實作	HTTPS	說明裝置狀態的免費文字
		國家環境	實作	HTTPS	
		目標儲存設備	實作	HTTPS	
		目標Volume	實作	HTTPS	
		技術	實作	HTTPS	改變儲存效率的技術
	Volume	容量	實作	HTTPS	Snapshot使用容量（單位：MB）
		交會路徑	實作	HTTPS	
		名稱	實作	HTTPS	
		總原始容量	實作	HTTPS	總原始容量（陣列上所有磁碟的總和）
		儲存資源池ID	實作	HTTPS	
		資源隨需配置	實作	HTTPS	
		UUID	實作	HTTPS	
		已用容量	實作	HTTPS	
	Volume Map	LUN	實作	HTTPS	後端LUN的名稱
		傳輸協定控制器	實作	HTTPS	
		儲存連接埠	實作	HTTPS	
		類型	落差	HTTPS	
	Volume遮罩	啟動器	實作	HTTPS	
		傳輸協定控制器	實作	HTTPS	
		儲存連接埠	實作	HTTPS	
		類型	落差	HTTPS	

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
效能	磁碟	IOPS讀取	實作	HTTPS	磁碟上的讀取IOP 數
		IOPS總計	實作	HTTPS	
		IOPS寫入	實作	HTTPS	
		金鑰	實作	HTTPS	
		伺服器ID	實作	HTTPS	
		處理量讀取	實作	HTTPS	
		總處理量	實作	HTTPS	平均磁碟總速率（橫跨所有磁碟的讀寫）、單位為MB/s
		處理量寫入	實作	HTTPS	

此資料收集器使用的管理 API ：

API	使用的傳輸協定	使用傳輸層傳輸層傳輸協定	使用的傳入連接埠	使用的傳出連接埠	支援驗證	僅需要「唯讀」認證	支援加密	防火牆易用（靜態連接埠）
VNXe 和 UnEthisphere CLI	HTTPS	HTTPS	443		是的	是的	是的	是的

EMC VPLEX

此資料收集器支援的機型和版本：

模型	韌體版本
VPLEX	6.1.0.00.00.236.1.0.01.00.136.1.0.02.00.04

此資料收集器支援的產品：

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
基礎					

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

		UUID	實作	HTTP/S	
		虛擬化	實作	HTTP/S	這是儲存虛擬化
產品	類別	功能/屬性	狀態	使用的傳輸協定	設備訊
	Volume Map	LUN	實作	HTTP/S	後端LUN的名稱
		傳輸協定控制器	實作	HTTP/S	
		儲存連接埠	實作	HTTP/S	
		類型	落差	HTTP/S	
	Volume遮罩	啟動器	實作	HTTP/S	
		傳輸協定控制器	實作	HTTP/S	
		儲存連接埠	實作	HTTP/S	
		類型	落差	HTTP/S	

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
效能	儲存節點資料	快取命中率總計	實作	SSH	
		IOPS讀取	實作	SSH	磁碟上的讀取IOP 數
		IOPS總計	實作	SSH	
		IOPS寫入	實作	SSH	
		金鑰	實作	SSH	
		延遲讀取	實作	SSH	
		總延遲	實作	SSH	
		延遲寫入	實作	SSH	
		伺服器ID	實作	SSH	
		處理量讀取	實作	SSH	
		總處理量	實作	SSH	平均磁碟總速率（橫跨所有磁碟的讀寫）、單位為MB/s
		處理量寫入	實作	SSH	
		使用率總計	實作	SSH	
	Volume	原始容量	實作	SSH	
		總容量	實作	SSH	
		IOPS總計	實作	SSH	
		金鑰	實作	SSH	
		延遲讀取	實作	SSH	
		總延遲	實作	SSH	
		延遲寫入	實作	SSH	
		伺服器ID	實作	SSH	
		處理量讀取	實作	SSH	
		總處理量	實作	SSH	平均磁碟總速率（橫跨所有磁碟的讀寫）、單位為MB/s
		處理量寫入	實作	SSH	

此資料收集器使用的管理 API ：

API	使用的傳輸協定	使用傳輸層傳輸層傳輸協定	使用的傳入連接埠	使用的傳出連接埠	支援驗證	僅需要「唯讀」認證	支援加密	防火牆易用（靜態連接埠）
EMC VPLEX CLI	SSH	SSH	22		是的	是的	是的	是的
EMC VPLEX API	HTTP / HTTPS	HTTP / HTTPS	80/443		是的	是的	是的	是的

EMC XtremIO（HTTP）

此資料收集器支援的機型和版本：

API 版本	模型	韌體版本
4.2.2 6.2.1 6.3.1 6.3.2 6.3.3 6.4.0	1 塊磚、 48TB 1X20TB 2 塊磚塊、 251TB 2X20TB 3 塊磚塊、 283TB 4 塊磚塊、 503TB 4X10TB 6X20TB 8X20TB	4.0.25-274.0.31-11 6.1.0-99_X2 6.2.1-36_X2 6.3.3-8_X2 6.4.0-36_hotfix_2_X2

此資料收集器支援的產品：

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
基礎					
410					

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

		類型	落差	HTTPS	
		虛擬化	實作	HTTPS	這是儲存虛擬化設備嗎？
產品	類別	功能/屬性	狀態	使用的傳輸協定	說明
	儲存同步	模式	實作	HTTPS	
		模式環境	實作	HTTPS	
		來源Volume	實作	HTTPS	
		州/省	實作	HTTPS	說明裝置狀態的免費文字
		國家環境	實作	HTTPS	
		目標Volume	實作	HTTPS	
		技術	實作	HTTPS	改變儲存效率的技術
	Volume	容量	實作	HTTPS	Snapshot使用容量（單位：MB）
		磁碟大小	實作	HTTPS	以英文分隔的磁碟大小清單（GB）
		磁碟速度	實作	HTTPS	以英文分隔的磁碟速度（rpm）清單
		磁碟類型	無法使用	HTTPS	
		名稱	實作	HTTPS	
		總原始容量	實作	HTTPS	總原始容量（陣列上所有磁碟的總和）
		備援	實作	HTTPS	備援層級
		儲存資源池ID	實作	HTTPS	
		資源隨需配置	實作	HTTPS	
		類型	落差	HTTPS	
		UUID	實作	HTTPS	
		已用容量	實作	HTTPS	
		虛擬化	實作	HTTPS	這是儲存虛擬化設備嗎？
	Volume Map	LUN	實作	HTTPS	後端LUN的名稱
		傳輸協定控制器	實作	HTTPS	
		類型	落差	HTTPS	
	Volume遮罩	啟動器	實作	HTTPS	
		傳輸協定控制器	實作	HTTPS	
		類型	落差	HTTPS	

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
效能	儲存設備	原始容量失敗	實作	HTTPS	
		原始容量	實作	HTTPS	
		備用原始容量	實作	HTTPS	備用磁碟的原始容量（所有備援磁碟的總和）
		StoragePools容量	實作	HTTPS	
		金鑰	實作	HTTPS	
		伺服器ID	實作	HTTPS	
	儲存節點資料	金鑰	實作	HTTPS	
		伺服器ID	實作	HTTPS	
	Volume	原始容量	實作	HTTPS	
		總容量	實作	HTTPS	
		已用容量	實作	HTTPS	
		容量使用率	實作	HTTPS	
		IOPS讀取	實作	HTTPS	磁碟上的讀取IOP 數
		IOPS總計	實作	HTTPS	
		IOPS寫入	實作	HTTPS	
		金鑰	實作	HTTPS	
		延遲讀取	實作	HTTPS	
		總延遲	實作	HTTPS	
		延遲寫入	實作	HTTPS	
		部分封鎖比率	實作	HTTPS	
		伺服器ID	實作	HTTPS	
		處理量讀取	實作	HTTPS	
		總處理量	實作	HTTPS	平均磁碟總速率（橫跨所有磁碟的讀寫）、單位為MB/s
		處理量寫入	實作	HTTPS	

此資料收集器使用的管理 API ：

API	使用的傳輸協定	使用傳輸層傳輸層傳輸協定	使用的傳入連接埠	使用的傳出連接埠	支援驗證	僅需要「唯讀」認證	支援加密	防火牆易用（靜態連接埠）
EMC XtremIO REST API	HTTPS	HTTPS	443		是的	是的	是的	是的

NetApp E系列

此資料收集器支援的機型和版本：

模型	韌體版本
2650 2660 2704 2806 5600 5700	8.10.15.0 8.20.11.60 8.20.16.0 8.20.5.60 8.40.0.3 8.40.60.2 8.63.0.2 8.72.0.0 8.72.1.0 8.72.2.0 8.73.0.0 8.74.2.0

此資料收集器支援的產品：

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
基礎					
416					

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

		類型	落差	RMI	
		虛擬化	實作	RMI	這是儲存虛擬化設備嗎？
產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
	Volume	容量	實作	RMI	Snapshot使用容量（單位：MB）
		磁碟類型	無法使用	RMI	
		名稱	實作	RMI	
		總原始容量	實作	RMI	總原始容量（陣列上所有磁碟的總和）
		備援	實作	RMI	備援層級
		儲存資源池ID	實作	RMI	
		資源隨需配置	實作	RMI	
		類型	落差	RMI	
		UUID	實作	RMI	
		已用容量	實作	RMI	
		虛擬化	實作	RMI	這是儲存虛擬化設備嗎？
		寫入容量	實作	RMI	主機寫入此磁碟區的總容量（以MB為單位）
	Volume Map	LUN	實作	RMI	後端LUN的名稱
	Volume遮罩	啟動器	實作	RMI	

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
效能					
420					

		量			
		金鑰	實作	RMI	
產品	類別	特徵屬性	狀態	使用的傳輸協定	其他資訊
	儲存資源池	已配置的容量	實作	RMI	
		原始容量	實作	RMI	
		總容量	實作	RMI	
		已用容量	實作	RMI	
		過度使用容量比率	實作	RMI	報告為時間序列
		容量使用率	實作	RMI	
		總資料容量	實作	RMI	
		資料使用容量	實作	RMI	
		金鑰	實作	RMI	
		其他總容量	實作	RMI	
		其他已用容量	實作	RMI	
		伺服器ID	實作	RMI	
	Volume	快取命中率讀取	實作	RMI	
		快取命中率總計	實作	RMI	
		快取命中率寫入	實作	RMI	
		原始容量	實作	RMI	
		總容量	實作	RMI	
		已用容量	實作	RMI	
		容量使用率	實作	RMI	
		IOPS讀取	實作	RMI	磁碟上的讀取IOP 數
		IOPS總計	實作	RMI	
		IOPS寫入	實作	RMI	
		金鑰	實作	RMI	
		延遲讀取	實作	RMI	
		總延遲	實作	RMI	
		延遲寫入	實作	RMI	
		伺服器ID	實作	RMI	
		處理量讀取	實作	RMI	
		總處理量	實作	RMI	平均磁碟總速率（橫跨所有磁碟的讀寫）、單位為MB/s
		處理量寫入	實作	RMI	

此資料收集器使用的管理 API ：

API	使用的傳輸協定	使用傳輸層傳輸層傳輸協定	使用的傳入連接埠	使用的傳出連接埠	支援驗證	僅需要「唯讀」認證	支援加密	防火牆易用（靜態連接埠）
部分API SANtricity	RMI	TCP			是的	是的	錯	錯

HDS HCPs（HTTPS）

此資料收集器支援的機型和版本：

模型	韌體版本
Hitachi內容平台	9.6.2.37 9.6.3.33

此資料收集器支援的產品：

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
基礎					

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

					設備嗎？
	儲存節點	名稱	實作	HTTPS	
產品	類別	功能屬性	狀態	使用的傳輸協定	其他資訊
	儲存資源池	包括在DWh容量中	實作	HTTPS	從 ACQ 控制 DWH 容量感興趣的儲存池
		名稱	實作	HTTPS	
		實體磁碟容量（MB）	實作	HTTPS	用作儲存資源池的原始容量
		RAID群組	實作	HTTPS	指出此storagePool是否為RAID群組
		原始對可用比率	實作	HTTPS	從可用容量轉換為原始容量的比率
		軟限制（MB）	實作	HTTPS	在磁碟區建立或調整作業大小期間所定義的邏輯磁碟區大小
		儲存資源池ID	實作	HTTPS	
		支援精簡配置	實作	HTTPS	此內部磁碟區是否支援其上的磁碟區層精簡配置
		已分配容量總計	實作	HTTPS	
		總使用容量	實作	HTTPS	總容量（單位：MB）
		類型	落差	HTTPS	
		虛擬化	實作	HTTPS	這是儲存虛擬化設備嗎？

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
效能	儲存設備	原始容量失敗	實作		
		原始容量	實作		
		備用原始容量	實作		備用磁碟的原始容量（所有備援磁碟的總和）
		StoragePools容量	實作		
		金鑰	實作		
		伺服器ID	實作		
	儲存節點資料	金鑰	實作		
		伺服器ID	實作		
		處理量讀取	實作		
		總處理量	實作		平均磁碟總速率（橫跨所有磁碟的讀寫）、單位為MB/s
		處理量寫入	實作		
		使用率總計	實作		

此資料收集器使用的管理 API ：

API	使用的傳輸協定	使用傳輸層傳輸層傳輸協定	使用的傳入連接埠	使用的傳出連接埠	支援驗證	僅需要「唯讀」認證	支援加密	防火牆易用（靜態連接埠）
HDS HCP REST API	HTTPS	HTTPS	9090		是的	是的	是的	是的

Hndvice管理程式

此資料收集器支援的機型和版本：

API 版本	模型	韌體版本
8.6.48.7.8.8.8.8.8.8.8.8.5	D850XS HM700 HM800M R800	0988/J-W DKC:73-03-69-00/00 DKC:80-06-92-00/00 DKC:83-05-48-00 DKC:83-05-50-40/00 SVP:73-03-68/00 SVP:80-06-87/00 SVP:83-05-52-40/00 SVP:80-06-40/00-05-40/00

此資料收集器支援的產品：

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
基礎					
428					

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

	Volume遮罩	啟動器	實作	HDS XML API	
		傳輸協定控制器	實作	HDS XML API	
產品	類別	儲存連接埠	實作	使用的傳輸協定	其他資訊
	Volume成員	名稱	實作	HDS XML API	
		儲存資源池ID	實作	HDS XML API	
		排名	實作	HDS XML API	
		汽缸	實作	HDS XML API	
		容量	實作	HDS XML API	Snapshot使用容量（單位：MB）
		總原始容量	實作	HDS XML API	總原始容量（陣列上所有磁碟的總和）
		已用容量	實作	HDS XML API	
	WWN別名	主機別名	實作	HDS XML API	
		物件類型	實作	HDS XML API	
		來源	實作	HDS XML API	
		WWN	實作	HDS XML API	
效能	磁碟	IOPS讀取	實作	匯出/CLI	磁碟上的讀取IOP 數
		IOPS總計	實作	匯出/CLI	
		IOPS寫入	實作	匯出/CLI	
		金鑰	實作	匯出/CLI	
		伺服器ID	實作	匯出/CLI	
		處理量讀取	實作	匯出/CLI	
		總處理量	實作	匯出/CLI	平均磁碟總速率（橫跨所有磁碟的讀寫）、單位為MB/s
		處理量寫入	實作	匯出/CLI	
		使用率總計	實作	匯出/CLI	

此資料收集器使用的管理 API ：

API	使用的傳輸協定	使用傳輸層傳輸層傳輸協定	使用的傳入連接埠	使用的傳出連接埠	支援驗證	僅需要「唯讀」認證	支援加密	防火牆易用（靜態連接埠）
匯出公用程式（USPV）/ SNM CLI（AMS）	匯出/CLI				錯	錯	錯	錯

API	使用的傳輸協定	使用傳輸層傳輸層傳輸協定	使用的傳入連接埠	使用的傳出連接埠	支援驗證	僅需要「唯讀」認證	支援加密	防火牆易用（靜態連接埠）
HiCommand Device Manager XML API	HDS XML API	HTTP / HTTPS	2001		是的	是的	是的	是的

HDS HNAS（CLI）

此資料收集器支援的機型和版本：

模型	韌體版本
G600 HNAS 4100	14.6.7520.04

此資料收集器支援的產品：

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
基礎					
436					

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

					免費文字
		UUID	實作	SSH	
產品	類別	屬性	狀態	使用的傳輸協定	軟體版本
	儲存資源池	資料使用容量	實作	SSH	
		已啟用重複資料刪除	實作	SSH	是否在儲存資源池上啟用重複資料刪除功能
		包括在DWh容量中	實作	SSH	從 ACQ 控制 DWH 容量感興趣的儲存池
		名稱	實作	SSH	
		RAID群組	實作	SSH	指出此storagePool是否為RAID群組
		原始對可用比率	實作	SSH	從可用容量轉換為原始容量的比率
		Snapshot已用容量	實作	SSH	
		儲存資源池ID	實作	SSH	
		支援精簡配置	實作	SSH	此內部磁碟區是否支援其上的磁碟區層精簡配置
		已分配容量總計	實作	SSH	
		總使用容量	實作	SSH	總容量（單位：MB）
		類型	落差	SSH	
		虛擬化	實作	SSH	這是儲存虛擬化設備嗎？

此資料收集器使用的管理 API ：

API	使用的傳輸協定	使用傳輸層傳輸層傳輸協定	使用的傳入連接埠	使用的傳出連接埠	支援驗證	僅需要「唯讀」認證	支援加密	防火牆易用（靜態連接埠）
HDS HNAS CLI	SSH	SSH	22		是的	是的	是的	是的

HPE Nimble / Alletra 6000儲存設備

此資料收集器支援的機型和版本：

API 版本	模型	韌體版本
v1	AFF 40 AFF 80 HF60	5.0.3.100-575430-opt 5.2.1.6600-841103 選項

此資料收集器支援的產品：

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
基礎					
442					

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

		類型	落差	HTTPS	
		虛擬化	實作	HTTPS	這是儲存虛擬化設備嗎？
產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
	Volume	容量	實作	HTTPS	Snapshot使用容量（單位：MB）
		名稱	實作	HTTPS	
		總原始容量	實作	HTTPS	總原始容量（陣列上所有磁碟的總和）
		備援	實作	HTTPS	備援層級
		儲存資源池ID	實作	HTTPS	
		資源隨需配置	實作	HTTPS	
		類型	落差	HTTPS	
		UUID	實作	HTTPS	
		已用容量	實作	HTTPS	
		虛擬化	實作	HTTPS	這是儲存虛擬化設備嗎？
		壓縮已啟用	實作	HTTPS	
		加密	實作	HTTPS	
	Volume Map	LUN	實作	HTTPS	後端LUN的名稱
		需要遮罩	實作	HTTPS	
		傳輸協定控制器	實作	HTTPS	
		類型	落差	HTTPS	
	Volume遮罩	啟動器	實作	HTTPS	
		傳輸協定控制器	實作	HTTPS	
		類型	落差	HTTPS	
	WWN別名	主機別名	實作	HTTPS	
		物件類型	實作	HTTPS	
		來源	實作	HTTPS	
		WWN	實作	HTTPS	

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
效能	儲存設備	原始容量失敗	實作	HTTPS	
		原始容量	實作	HTTPS	
		備用原始容量	實作	HTTPS	備用磁碟的原始容量（所有備援磁碟的總和）
		StoragePools容量	實作	HTTPS	
		IOPS其他	實作	HTTPS	
		IOPS讀取	實作	HTTPS	磁碟上的讀取IOP 數
		IOPS總計	實作	HTTPS	
		IOPS寫入	實作	HTTPS	
		金鑰	實作	HTTPS	
		延遲讀取	實作	HTTPS	
		總延遲	實作	HTTPS	
		延遲寫入	實作	HTTPS	
		伺服器ID	實作	HTTPS	
		處理量讀取	實作	HTTPS	
		總處理量	實作	HTTPS	平均磁碟總速率（橫跨所有磁碟的讀寫）、單位為MB/s
		處理量寫入	實作	HTTPS	

此資料收集器使用的管理 API ：

API	使用的傳輸協定	使用傳輸層傳輸層傳輸協定	使用的傳入連接埠	使用的傳出連接埠	支援驗證	僅需要「唯讀」認證	支援加密	防火牆易用（靜態連接埠）
HP Nimble REST API	HTTPS	HTTPS	5392		是的	錯	是的	是的

Huawei海洋儲存設備（REST / HTTPS）

此資料收集器支援的機型和版本：

模型	韌體版本
5500 V3 6800 V3	V300R006C50

此資料收集器支援的產品：

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
基礎					
448					

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

		已用容量	實作	HTTPS	
		虛擬化	實作	HTTPS	這是儲存虛擬化
產品	類別	功能/屬性	狀態	使用的傳輸協定	設備訊
	Volume Map	LUN	實作	HTTPS	後端LUN的名稱
		傳輸協定控制器	實作	HTTPS	
		類型	落差	HTTPS	
	Volume遮罩	啟動器	實作	HTTPS	
		傳輸協定控制器	實作	HTTPS	
		類型	落差	HTTPS	

此資料收集器使用的管理 API ：

API	使用的傳輸協定	使用傳輸層傳輸層傳輸協定	使用的傳入連接埠	使用的傳出連接埠	支援驗證	僅需要「唯讀」認證	支援加密	防火牆易用（靜態連接埠）
Huawei OceanStor REST API	HTTPS	HTTPS	8088		是的	是的	是的	是的
Huawei OceanStor Performance REST API	HTTPS	HTTPS	8088		是的	錯	是的	是的

IBM SVC（CLI）

此資料收集器支援的機型和版本：

模型	韌體版本
2076-112 20766-124 2076-12F 2076-212 2076-224 2076-224 F 2076-224G 20766-52420766-624 20766-724 2077-24F 20777-324 467-924 4662-6H2 9840-AE1 9843-AE2 9843-AE3 服務	1.5.2.5 1.6.1.0 1.6.1.5 7.8.1.11 7.8.1.13.7.8.1.5 7.8.1.7 7.8.1.8.1.3.5 8.1.3.6.8.2.1.11.8.2.1.8.3.1.2 8.3.1.5 8.4.0.10 8.4.0.11 8.5.0.11 8.5.0.12 8.5.0.9.8.5.3.16.6.0.4

此資料收集器支援的產品：

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
基礎					
452					

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

		傳輸協定控制器	實作	SSH	
		儲存連接埠	實作	SSH	
產品	類別	類型/屬性	狀態	使用的傳輸協定	其他資訊
	WWN別名	主機別名	實作	SSH	
		物件類型	實作	SSH	
		來源	實作	SSH	
		WWN	實作	SSH	

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
效能					
458					

		量			
		金鑰	實作	SSH	
產品	類別	特徵屬性	狀態	使用的傳輸協定	其他資訊
	儲存節點資料	快取命中率總計	實作	SSH	
		IOPS讀取	實作	SSH	磁碟上的讀取IOP 數
		IOPS總計	實作	SSH	
		IOPS寫入	實作	SSH	
		金鑰	實作	SSH	
		延遲讀取	實作	SSH	
		總延遲	實作	SSH	
		延遲寫入	實作	SSH	
		伺服器ID	實作	SSH	
		處理量讀取	實作	SSH	
		總處理量	實作	SSH	平均磁碟總速率（橫跨所有磁碟的讀寫）、單位為MB/s
		處理量寫入	實作	SSH	
		使用率總計	實作	SSH	
	儲存資源池	已配置的容量	實作	SSH	
		原始容量	實作	SSH	
		總容量	實作	SSH	
		已用容量	實作	SSH	
		過度使用容量比率	實作	SSH	報告為時間序列
		容量使用率	實作	SSH	
		金鑰	實作	SSH	
		伺服器ID	實作	SSH	
	Volume	原始容量	實作	SSH	
		總容量	實作	SSH	
		已用容量	實作	SSH	
		寫入容量	實作	SSH	
		容量使用率	實作	SSH	
		寫入的容量比率	實作	SSH	
		金鑰	實作	SSH	
		伺服器ID	實作	SSH	

此資料收集器使用的管理 API ：

API	使用的傳輸協定	使用傳輸層傳輸層傳輸協定	使用的傳入連接埠	使用的傳出連接埠	支援驗證	僅需要「唯讀」認證	支援加密	防火牆易用（靜態連接埠）
IBM SVC CLI	SSH	SSH	22		是的	錯	是的	是的

Infinidat Infinidat Infinbox（HTTP）

此資料收集器支援的機型和版本：

模型	韌體版本
F4304 F4304T F6260 F6306	7.1.14.0

此資料收集器支援的產品：

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
基礎					

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

		傳輸協定控制器	實作	HTTPS	
		儲存連接埠	實作	HTTPS	
產品	類別	類型/屬性	狀態	使用的傳輸協定	其他資訊
	Volume遮罩	啟動器	實作	HTTPS	
		傳輸協定控制器	實作	HTTPS	
		儲存連接埠	實作	HTTPS	
		類型	落差	HTTPS	
	WWN別名	主機別名	實作	HTTPS	
		物件類型	實作	HTTPS	
		來源	實作	HTTPS	
		WWN	實作	HTTPS	

此資料收集器使用的管理 API ：

API	使用的傳輸協定	使用傳輸層傳輸層傳輸協定	使用的傳入連接埠	使用的傳出連接埠	支援驗證	僅需要「唯讀」認證	支援加密	防火牆易用（靜態連接埠）
Infinidat REST API	HTTPS	HTTPS	443		是的	是的	是的	是的

Microsoft Hyper-V

此資料收集器支援的產品：

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
基礎					
466					

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

		已用容量	實作	WMI	已用容量報告（MB）
產品	類別	功能屬性	狀態	使用的傳輸協定	其他資訊
	虛擬機器	DNS名稱	實作	WMI	
		訪客狀態	實作	WMI	
		資料存放區oID	實作	WMI	
		主機oID	實作	WMI	
		IPS	實作	WMI	
		MOID	實作	WMI	
		記憶體	實作	WMI	
		名稱	實作	WMI	
		oID	實作	WMI	
		作業系統	實作	WMI	
		電源狀態	實作	WMI	
		狀態變更時間	實作	WMI	
		處理器	實作	WMI	
		已配置的容量	實作	WMI	
		已用容量	實作	WMI	
	虛擬機器磁碟	oID	實作	WMI	
		虛擬磁碟oID	實作	WMI	
		虛擬機器oID	實作	WMI	
	主機	主機CPU計數	實作	WMI	
		主機CPU速度	實作	WMI	
		主機網域	實作	WMI	
		主機安裝的記憶體	實作	WMI	
		主機模式	實作	WMI	
		NIC數	實作	WMI	
		NIC速度	實作	WMI	
		IPS	實作	WMI	
		製造商	實作	WMI	
		名稱	實作	WMI	
		oID	實作	WMI	
		平台類型	實作	WMI	
	資訊	資料來源名稱	實作	WMI	資訊
		日期	實作	WMI	
		建立者ID	實作	WMI	

此資料收集器使用的管理 API ：

API	使用的傳輸協定	使用傳輸層傳輸層傳輸協定	使用的傳入連接埠	使用的傳出連接埠	支援驗證	僅需要「唯讀」認證	支援加密	防火牆易用（靜態連接埠）
PowerShell	WS 管理	HTTP	5985		是的	錯	錯	是的
WMI	WMI	WMI	135		是的	錯	是的	是的

NetApp 7 模式

此資料收集器支援的機型和版本：

API 版本	模型	韌體版本
1.12 1.17 1.19 1.20 1.21	FAS2220 FAS2240-2 FAS2240-4 FAS2554 FAS3210 FAS32250 FAS6240 FAS8040 FAS8060 N6070	8.1.1 7-Mode 8.1.4P6 7-Mode 8.2.3P2 7-Mode 8.2.3P3 7-Mode 8.2.3P6 7-Mode 8.2.4P4 7-Mode 8.2.4P5 7-Mode 8.2.5P3 7-Mode 8.2.5P5 7-Mode 8.2P5 7-Mode 8.2P4 7-Mode Data ONTAP 7.3.3 Data ONTAP 7.3.4 版

此資料收集器支援的產品：

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
基礎					
470					

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

					Pool（NetApp專屬）
		虛擬化	實作		這是儲存虛擬化
產品	類別	功能/屬性	狀態	使用的傳輸協定	設備訊
	Volume	容量	實作		Snapshot使用容量（單位：MB）
		磁碟群組	實作		磁碟群組類型
		磁碟大小	實作		以英文分隔的磁碟大小清單（GB）
		磁碟速度	實作		以英文分隔的磁碟速度（rpm）清單
		磁碟類型	無法使用		
		交會路徑	實作		
		上次已知存取時間	實作		最後一次知道對Volume的存取
		名稱	實作		
		保護類型	實作		
		qtree ID	實作		qtree的唯一ID
		總原始容量	實作		總原始容量（陣列上所有磁碟的總和）
		儲存資源池ID	實作		
		資源隨需配置	實作		
		類型	落差		
		已用容量	實作		
	Volume Map	LUN	實作		後端LUN的名稱
		傳輸協定控制器	實作		
		類型	落差		
	Volume遮罩	啟動器	實作		
		傳輸協定控制器	實作		
		儲存連接埠	實作		
		類型	落差		

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
效能	儲存節點資料	快取命中率總計	實作		
		已更換磁碟讀取總數	實作		
		IOPS讀取	實作		磁碟上的讀取IOP 數
		IOPS總計	實作		
		IOPS寫入	實作		
		金鑰	實作		
		延遲讀取	實作		
		總延遲	實作		
		延遲寫入	實作		
		伺服器ID	實作		
		處理量讀取	實作		
		總處理量	實作		平均磁碟總速率（橫跨所有磁碟的讀寫）、單位為MB/s
		處理量寫入	實作		
		使用率總計	實作		
	儲存資源池	已配置的容量	實作		
		原始容量	實作		
		總容量	實作		
		已用容量	實作		
		過度使用容量比率	實作		報告為時間序列
		容量使用率	實作		
		總資料容量	實作		
		資料使用容量	實作		
		金鑰	實作		
		伺服器ID	實作		
		Snapshot保留容量	實作		
		Snapshot已用容量	實作		
		Snapshot使用容量比率	實作		報告為時間序列

此資料收集器使用的管理 API ：

API	使用的傳輸協定	使用傳輸層傳輸層傳輸協定	使用的傳入連接埠	使用的傳出連接埠	支援驗證	僅需要「唯讀」認證	支援加密	防火牆易用（靜態連接埠）
NetApp 7 模式 ZAPI	ZAPI	ZAPI			是的	是的	是的	是的

NetApp叢集Data ONTAP 式NetApp 8.1.1以上

此資料收集器支援的機型和版本：

模型	韌體版本
AFF AFF FAS500f A150 FAS2240-A200 FAS2520 FAS8040 FAS8040 FAS8040 AFF AFF AFF FAS8200 FAS8300 FAS8700 FAS9000 FAS9500 FAS30252552 FAS802050 AFF FAS2620 FAS2650 FAS2720 FAS2750 ： A250 AFF 、 A300 AFF 、 A400 AFF 、 A700s 、 AFF 、 A800 AFF 、 A900 AFF 、 C190 AFF 、 C250 FAS2240-2 FAS2520 FAS8040 AFF8080 CDVM200 AFF 、 FAS802552	8.2.3P5 8.2.4P3 8.3.1P2 8.3.2.3.2.2P12 8.3.2P5 8.3.2P8 9.1.09.1.0P15 9.1.0P19 9.1.0P2 9.1.09.1.0P20 9.10.1P11 9.10.1P12 9.P12

此資料收集器支援的產品：

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
基礎					

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

		傳輸協定控制器	實作	HTTPS	
		儲存連接埠	實作	HTTPS	
產品	類別	類型/屬性	落差	使用的傳輸協定	其他資訊
	Volume遮罩	啟動器	實作	HTTPS	
		傳輸協定控制器	實作	HTTPS	
		儲存連接埠	實作	HTTPS	
		類型	落差	HTTPS	

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
效能					
494					

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

		使用的物件存放區空間	實作	HTTPS	
產品	類別	物件屬性	狀態	使用的傳輸協定	其他資訊
		Snapshot保留容量	實作	HTTPS	
		Snapshot已用容量	實作	HTTPS	
		Snapshot使用容量比率	實作	HTTPS	報告為時間序列
		處理量讀取	實作	HTTPS	
		總處理量	實作	HTTPS	平均磁碟總速率（橫跨所有磁碟的讀寫）、單位為MB/s
		處理量寫入	實作	HTTPS	
		讀取使用率	實作	HTTPS	
		使用率總計	實作	HTTPS	
		使用率寫入	實作	HTTPS	
	Volume	金鑰	實作	HTTPS	
		伺服器ID	實作	HTTPS	
		處理量讀取	實作	HTTPS	
		處理量寫入	實作	HTTPS	
		總處理量	實作	HTTPS	平均磁碟總速率（橫跨所有磁碟的讀寫）、單位為MB/s
		延遲讀取	實作	HTTPS	
		延遲寫入	實作	HTTPS	
		總延遲	實作	HTTPS	
		IOPS讀取	實作	HTTPS	磁碟上的讀取IOP 數
		IOPS寫入	實作	HTTPS	
		IOPS總計	實作	HTTPS	
		部分封鎖比率	實作	HTTPS	

此資料收集器使用的管理 API ：

API	使用的傳輸協定	使用傳輸層傳輸層傳輸協定	使用的傳入連接埠	使用的傳出連接埠	支援驗證	僅需要「唯讀」認證	支援加密	防火牆易用（靜態連接埠）
NetApp ONTAP API	HTTP / HTTPS	HTTP / HTTPS	80/443		是的	是的	是的	是的

NetApp SolidFire RJ8.1以上

此資料收集器支援的機型和版本：

模型	韌體版本
H410S-1 SF19210 SF2405 SF38410 SF4805 FC0025 FCCN001 H410S-0H610S-1 SF19210 SF2405 SF38410 SF4805	11.1.0.72 11.3.1.5 12.3.0.958 12.3.1.103 12.3.2.3 12.5.0.897 12.7.0.380 9.3.0.40

此資料收集器支援的產品：

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
基礎					

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

		總使用容量	實作	HTTPS	總容量（單位：MB）
產品	類別	類型/屬性	落差	使用的傳輸協定	其他資訊
		虛擬化	實作	HTTPS	這是儲存虛擬化設備嗎？
		加密	實作	HTTPS	
	Volume	容量	實作	HTTPS	Snapshot使用容量（單位：MB）
		交會路徑	實作	HTTPS	
		名稱	實作	HTTPS	
		總原始容量	實作	HTTPS	總原始容量（陣列上所有磁碟的總和）
		備援	實作	HTTPS	備援層級
		儲存資源池ID	實作	HTTPS	
		資源隨需配置	實作	HTTPS	
		類型	落差	HTTPS	
		UUID	實作	HTTPS	
		已用容量	實作	HTTPS	
		虛擬化	實作	HTTPS	這是儲存虛擬化設備嗎？
		帳戶識別碼	實作	HTTPS	
		帳戶名稱	實作	HTTPS	
		壓縮已啟用	實作	HTTPS	
		加密	實作	HTTPS	
		QoS爆發IOPS	實作	HTTPS	
		QoS 限制 IOPS	實作	HTTPS	
		QoS最低IOPS	實作	HTTPS	
		QoS -原則	實作	HTTPS	
	Volume Map	LUN	實作	HTTPS	後端LUN的名稱
		需要遮罩	實作	HTTPS	
		傳輸協定控制器	實作	HTTPS	
		儲存連接埠	實作	HTTPS	
		類型	落差	HTTPS	
	Volume遮罩	啟動器	實作	HTTPS	
		傳輸協定控制器	實作	HTTPS	
		儲存連接埠	實作	HTTPS	
		類型	落差	HTTPS	

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
效能					
504					

		其他總容量	實作	HTTPS	
		其他已用容量	實作	HTTPS	
產品	類別	物件屬性	狀態	使用的傳輸協定	其他資訊
	Volume	原始容量	實作	HTTPS	
		總容量	實作	HTTPS	
		已用容量	實作	HTTPS	
		容量使用率	實作	HTTPS	
		總壓縮節約量	實作	HTTPS	
		IOPS讀取	實作	HTTPS	磁碟上的讀取IOP 數
		IOPS總計	實作	HTTPS	
		IOPS寫入	實作	HTTPS	
		金鑰	實作	HTTPS	
		延遲讀取	實作	HTTPS	
		總延遲	實作	HTTPS	
		延遲寫入	實作	HTTPS	
		部分封鎖比率	實作	HTTPS	
		伺服器ID	實作	HTTPS	
		處理量讀取	實作	HTTPS	
		總處理量	實作	HTTPS	平均磁碟總速率（橫跨所有磁碟的讀寫）、單位為MB/s
		處理量寫入	實作	HTTPS	
		使用率總計	實作	HTTPS	

此資料收集器使用的管理 API ：

API	使用的傳輸協定	使用傳輸層傳輸層傳輸協定	使用的傳入連接埠	使用的傳出連接埠	支援驗證	僅需要「唯讀」認證	支援加密	防火牆易用（靜態連接埠）
SolidFire REST API	HTTPS	HTTPS	443		是的	是的	是的	是的

NetApp StorageGRID （HTTPS）

此資料收集器支援的機型和版本：

模型	韌體版本
Webscale	11.6.0.11 11.6.0.7 11.7.0.4 11.7.0.8 11.8.0.5 3.3.4 3.5 4.0

此資料收集器支援的產品：

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
基礎					

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

		節點容量使用率 使用中繼資料（以 MB 為單位）	實作	HTTPS	
產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
	儲存資源池	包括在DWh容量中	實作	HTTPS	從 ACQ 控制 DWH 容量感興趣的儲存池
		名稱	實作	HTTPS	
		實體磁碟容量（MB）	實作	HTTPS	用作儲存資源池的原始容量
		RAID群組	實作	HTTPS	指出此storagePool是否為RAID群組
		原始對可用比率	實作	HTTPS	從可用容量轉換為原始容量的比率
		儲存資源池ID	實作	HTTPS	
		支援精簡配置	實作	HTTPS	此內部磁碟區是否支援其上的磁碟區層精簡配置
		已分配容量總計	實作	HTTPS	
		總使用容量	實作	HTTPS	總容量（單位：MB）
		類型	落差	HTTPS	
		虛擬化	實作	HTTPS	這是儲存虛擬化設備嗎？

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
效能					

					（橫跨所有磁碟的讀寫）、單位為MB/s
產品	類別	處理量輸入	狀態	使用的傳輸協定	其他資訊
	儲存資源池	已配置的容量	實作		
		原始容量	實作		
		總容量	實作		
		已用容量	實作		
		過度使用容量比率	實作		報告為時間序列
		容量使用率	實作		
		金鑰	實作		
		伺服器ID	實作		

此資料收集器使用的管理 API ：

API	使用的傳輸協定	使用傳輸層傳輸層傳輸協定	使用的傳入連接埠	使用的傳出連接埠	支援驗證	僅需要「唯讀」認證	支援加密	防火牆易用（靜態連接埠）
靜態API StorageGRID	HTTPS	HTTPS	443		是的	錯	是的	是的

Nutanix儲存設備（REST）

此資料收集器支援的機型和版本：

模型	韌體版本
HX3310 NX-8150-G5 HX3310 HX3321 HX5510 NX-8155-G6 NX-8155-G7 XC640-10 核心 XC740xd-12 XC740xd-12 核心	5.20.2.1.5.20.4.6.5.46.5.5.6.5.6.5.7.6.6.7.1.76.8.1.

此資料收集器支援的產品：

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
基礎					

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

		類型	落差	HTTPS	
		虛擬化	實作	HTTPS	這是儲存虛擬化裝備訊
產品	類別	功能/屬性	狀態	使用的傳輸協定	
	Volume	容量	實作	HTTPS	Snapshot使用容量（單位：MB）
		交會路徑	實作	HTTPS	
		名稱	實作	HTTPS	
		qtree ID	實作	HTTPS	qtree的唯一ID
		總原始容量	實作	HTTPS	總原始容量（陣列上所有磁碟的總和）
		備援	實作	HTTPS	備援層級
		儲存資源池ID	實作	HTTPS	
		資源隨需配置	實作	HTTPS	
		UUID	實作	HTTPS	
	Volume Map	LUN	實作	HTTPS	後端LUN的名稱
		儲存連接埠	實作	HTTPS	
		傳輸協定控制器	實作	HTTPS	
		類型	落差	HTTPS	
	Volume遮罩	儲存連接埠	實作	HTTPS	
		啟動器	實作	HTTPS	
		傳輸協定控制器	實作	HTTPS	
		類型	落差	HTTPS	

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
效能	儲存設備	原始容量失敗	實作	HTTPS	
		原始容量	實作	HTTPS	
		備用原始容量	實作	HTTPS	備用磁碟的原始容量（所有備援磁碟的總和）
		StoragePools容量	實作	HTTPS	
		IOPS其他	實作	HTTPS	
		IOPS讀取	實作	HTTPS	磁碟上的讀取IOP 數
		IOPS總計	實作	HTTPS	
		IOPS寫入	實作	HTTPS	
		金鑰	實作	HTTPS	
		延遲讀取	實作	HTTPS	
		總延遲	實作	HTTPS	
		延遲寫入	實作	HTTPS	
		伺服器ID	實作	HTTPS	
		處理量讀取	實作	HTTPS	
		總處理量	實作	HTTPS	平均磁碟總速率（橫跨所有磁碟的讀寫）、單位為MB/s
		處理量寫入	實作	HTTPS	

此資料收集器使用的管理 API ：

API	使用的傳輸協定	使用傳輸層傳輸層傳輸協定	使用的傳入連接埠	使用的傳出連接埠	支援驗證	僅需要「唯讀」認證	支援加密	防火牆易用（靜態連接埠）
Nutanix REST API	HTTPS	HTTPS	443		是的	是的	是的	是的

Oracle ZFS（HTTPS）

此資料收集器支援的機型和版本：

模型	韌體版本
Sun ZFS Storage 7330 Sun ZFS Storage 7420 Sun ZFS Storage 7430	1-1.1 2013.06.05.7.28

此資料收集器支援的產品：

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
基礎					

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
		已分配容量總計	實作	HTTP/S	
		總使用容量	實作	HTTP/S	總容量（單位：MB）
		類型	落差	HTTP/S	
		虛擬化	實作	HTTP/S	這是儲存虛擬化設備嗎？
	Volume	自動分層	實作	HTTP/S	指出此儲存集區是否參與與其他集區的自動分層
		容量	實作	HTTP/S	Snapshot使用容量（單位：MB）
		磁碟大小	實作	HTTP/S	以英文分隔的磁碟大小清單（GB）
		磁碟速度	實作	HTTP/S	以英文分隔的磁碟速度（rpm）清單
		磁碟類型	無法使用	HTTP/S	
		交會路徑	實作	HTTP/S	
		名稱	實作	HTTP/S	
		總原始容量	實作	HTTP/S	總原始容量（陣列上所有磁碟的總和）
		備援	實作	HTTP/S	備援層級
		儲存資源池ID	實作	HTTP/S	
		資源隨需配置	實作	HTTP/S	
		類型	落差	HTTP/S	
		UUID	實作	HTTP/S	
		已用容量	實作	HTTP/S	
		虛擬化	實作	HTTP/S	這是儲存虛擬化設備嗎？
	Volume Map	LUN	實作	HTTP/S	後端LUN的名稱
		需要遮罩	實作	HTTP/S	
		傳輸協定控制器	實作	HTTP/S	
		儲存連接埠	實作	HTTP/S	
		類型	落差	HTTP/S	
	Volume遮罩	啟動器	實作	HTTP/S	
		傳輸協定控制器	實作	HTTP/S	
		儲存連接埠	實作	HTTP/S	
		類型	落差	HTTP/S	

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
效能	儲存節點資料	快取命中率總計	實作		
		IOPS總計	實作		
		金鑰	實作		
		伺服器ID	實作		
		使用率總計	實作		

此資料收集器使用的管理 API ：

API	使用的傳輸協定	使用傳輸層傳輸層傳輸協定	使用的傳入連接埠	使用的傳出連接埠	支援驗證	僅需要「唯讀」認證	支援加密	防火牆易用（靜態連接埠）
Oracle ZFS REST API	HTTP / HTTPS	HTTP / HTTPS	215		是的	是的	是的	是的

Pure Storage FlashArray（HTTP）

此資料收集器支援的機型和版本：

模型	韌體版本
DFSC1 FA-X20R3 FA-X50R2 FA-X70R3 FA-X70R4 FA-X90R2 FA-X90R3 FA-X90R4	6.1.21 6.3.16.3.106.3.96.5.16.5.26.5.4.

此資料收集器支援的產品：

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
基礎					
528					

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

		類型	落差	HTTP/S	
		虛擬化	實作	HTTP/S	這是儲存虛擬化設備嗎？
產品	類別	功能/屬性	狀態	使用的傳輸協定	備註
	Volume	容量	實作	HTTP/S	Snapshot使用容量（單位：MB）
		磁碟大小	實作	HTTP/S	以英文分隔的磁碟大小清單（GB）
		磁碟速度	實作	HTTP/S	以英文分隔的磁碟速度（rpm）清單
		磁碟類型	無法使用	HTTP/S	
		名稱	實作	HTTP/S	
		總原始容量	實作	HTTP/S	總原始容量（陣列上所有磁碟的總和）
		備援	實作	HTTP/S	備援層級
		儲存資源池ID	實作	HTTP/S	
		資源隨需配置	實作	HTTP/S	
		類型	落差	HTTP/S	
		已用容量	實作	HTTP/S	
		虛擬化	實作	HTTP/S	這是儲存虛擬化設備嗎？
	Volume Map	LUN	實作	HTTP/S	後端LUN的名稱
		傳輸協定控制器	實作	HTTP/S	
		儲存連接埠	實作	HTTP/S	
		類型	落差	HTTP/S	
	Volume遮罩	啟動器	實作	HTTP/S	
		傳輸協定控制器	實作	HTTP/S	
		儲存連接埠	實作	HTTP/S	
		類型	落差	HTTP/S	
	WWN別名	主機別名	實作	HTTP/S	
		物件類型	實作	HTTP/S	
		來源	實作	HTTP/S	
		WWN	實作	HTTP/S	

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
效能	儲存設備	原始容量失敗	實作		
		原始容量	實作		
		備用原始容量	實作		備用磁碟的原始容量（所有備援磁碟的總和）
		StoragePools容量	實作		
		IOPS其他	實作		
		IOPS讀取	實作		磁碟上的讀取IOP 數
		IOPS總計	實作		
		IOPS寫入	實作		
		金鑰	實作		
		延遲讀取	實作		
		總延遲	實作		
		延遲寫入	實作		
		伺服器ID	實作		
		處理量讀取	實作		
		總處理量	實作		平均磁碟總速率（橫跨所有磁碟的讀寫）、單位為MB/s
		處理量寫入	實作		

此資料收集器使用的管理 API ：

API	使用的傳輸協定	使用傳輸層傳輸層傳輸協定	使用的傳入連接埠	使用的傳出連接埠	支援驗證	僅需要「唯讀」認證	支援加密	防火牆易用（靜態連接埠）
Pure Storage REST API	HTTP / HTTPS	HTTP / HTTPS	80/443		是的	是的	是的	是的

VMware vSphere（Web服務）

此資料收集器支援的機型和版本：

API 版本：

- VMware vCenter Server 5.5.0 內部版本 -1750787
- VMware vCenter Server 5.5.0 組建 - 3252642

- VMware vCenter Server 5.5.0 組建編號： 4180647
- VMware vCenter Server 5.5.0 建置 -9911218
- VMware vCenter Server 6.0.0 組建 - 13638472
- VMware vCenter Server 6.0.0 內部版本 -14510545
- VMware vCenter Server 6.0.0 內部版本 -4541947
- VMware vCenter Server 6.0.0 內部版本 - 5318200
- VMware vCenter Server 6.0.0 內部版本 -9313458
- VMware vCenter Server 6.5.0 內部版本 -10964411
- VMware vCenter Server 6.5.0 內部版本 -17994927
- VMware vCenter Server 6.5.0 組建編號： 18499837
- VMware vCenter Server 6.5.0 建置 -18711281
- VMware vCenter Server 6.5.0 內部版本 -19757181
- VMware vCenter Server 6.5.0 組建 - 22499743
- VMware vCenter Server 6.5.0 內部版本 -7515524
- VMware vCenter Server 6.5.0 組建版 - 9451637
- VMware vCenter Server 6.7.0 內部版本 -16046713
- VMware vCenter Server 6.7.0 內部版本 -18485185
- VMware vCenter Server 6.7.0 內部版本 -19299595
- VMware vCenter Server 6.7.0 內部版本 -19832280
- VMware vCenter Server 6.7.0 組建版本 -20504362
- VMware vCenter Server 6.7.0 內部版本 -22509732
- VMware vCenter Server 6.7.0 內部版本 -22509751
- VMware vCenter Server 7.0.1 內部版本 -17491160
- VMware vCenter Server 7.0.3 內部版本 -19234570
- VMware vCenter Server 7.0.3 內部版本 -19717403
- VMware vCenter Server 7.0.3 build -20051473
- VMware vCenter Server 7.0.3 build -20150588
- VMware vCenter Server 7.0.3 build -20395099
- VMware vCenter Server 7.0.3 組建 -20845200
- VMware vCenter Server 7.0.3 build -20990077
- VMware vCenter Server 7.0.3 build 21290409
- VMware vCenter Server 7.0.3 build -2147706
- VMware vCenter Server 7.0.3 build -21784236
- VMware vCenter Server 7.0.3 build -22357613
- VMware vCenter Server 7.0.3 build -22837322

- VMware vCenter Server 7.0.3 組建 - 23788036
- VMware vCenter Server 7.0.3 組建 - 24026615
- VMware vCenter Server 8.0.1 組建 - 22368047
- VMware vCenter Server 8.0.1 build 22742005
- VMware vCenter Server 8.0.1 組建 - 23525738
- VMware vCenter Server 8.0.1 內部版本 - 2405165
- VMware vCenter Server 8.0.2 組建 - 22385739
- VMware vCenter Server 8.0.2 組建編號 22617221
- VMware vCenter Server 8.0.2 內部版本 23319993
- VMware vCenter Server 8.0.2 組建 - 23504390
- VMware vCenter Server 8.0.2 組建編號 23929136
- VMware vCenter Server 8.0.3 build 24022515
- VMware vCenter Server 8.0.3 build 24091160

此資料收集器支援的產品：

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊
基礎					
536					

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

產品	類別	功能/屬性	狀態	使用的傳輸協定	其他資訊

		名稱	實作	Web服務	
		oID	實作	Web服務	
產品	類別	功能屬性	狀態	使用的傳輸協定	其他資訊
	iSCSI節點	主機別名	實作	Web服務	
		節點名稱	實作	Web服務	
		oID	實作	Web服務	
		類型	落差	Web服務	
	資訊	API說明	實作	Web服務	
		API名稱	實作	Web服務	
		API版本	實作	Web服務	
		用戶端API名稱	實作	Web服務	
		用戶端API版本	實作	Web服務	
		資料來源名稱	實作	Web服務	資訊
		日期	實作	Web服務	
		建立者ID	實作	Web服務	

此資料收集器使用的管理 API ：

API	使用的傳輸協定	使用傳輸層傳輸層傳輸協定	使用的傳入連接埠	使用的傳出連接埠	支援驗證	僅需要「唯讀」認證	支援加密	防火牆易用（靜態連接埠）
VMware REST API	Web服務	HTTP / HTTPS	80/443		是的	是的	是的	是的

版權資訊

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

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

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

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

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

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

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

商標資訊

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