设置Insight

OnCommand Insight

NetApp
April 01, 2024

目录

设置Insight

要设置Insight、您必须激活Insight许可证、设置数据源、定义用户和通知、启用备份并执行任何所需的高级配置步骤。

安装OnCommand Insight 系统后、您必须执行以下设置任务：

- 安装Insight许可证。
- 在Insight中设置数据源。
- 设置用户帐户。
- 配置电子邮件。
- 根据需要定义SNMP、电子邮件或系统日志通知。
- 为Insight数据库启用每周自动备份。
- 执行所需的任何高级配置步骤、包括定义标注和阈值。

访问Web UI

安装OnCommand Insight 后、您必须安装许可证、然后设置Insight以监控您的环境。为此、您可以使用Web浏览器访问Insight Web UI。

步骤

1. 执行以下操作之一：
   - 在Insight服务器上打开Insight：

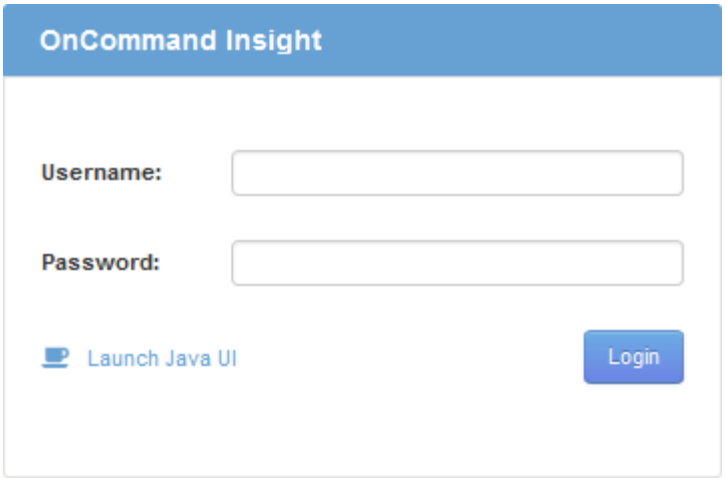
     ```
     https://fqdn
     ```

   - 从任何其他位置打开Insight：

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

     端口号是443、或者是在安装Insight服务器时配置的其他端口。如果未在URL中指定端口号、则端口号默认为443。

此时将显示OnCommand Insight 对话框：



2. 输入您的用户名和密码、然后单击*登录*。

   如果已安装许可证、则会显示数据源设置页面。

> 处于非活动状态30分钟的Insight浏览器会话将超时、您将自动从系统中注销。为了提高安全性、建议在注销Insight后关闭浏览器。

安装Insight许可证

从NetApp收到包含Insight许可证密钥的许可证文件后、您可以使用设置功能同时安装所有许可证。

关于此任务

Insight许可证密钥存储在中 `.txt` 或 `.lcn` 文件

步骤

1. 在文本编辑器中打开许可证文件并复制文本。
2. 在浏览器中打开Insight。
3. 在Insight工具栏上、单击*管理*。
4. 单击*设置*。
5. 单击*许可证*选项卡。
6. 单击 * 更新许可证 * 。
7. 将许可证密钥文本复制到*许可证*文本框中。
8. 选择*更新(最常见)*操作。
9. 单击 * 保存 * 。
10. 如果您使用的是Insight消费许可模式、则必须选中*发送使用情况信息*部分中的*启用向NetApp*发送使用情况信息复选框。必须为您的环境正确配置和启用代理。

完成后

安装许可证后、您可以执行以下配置任务：

- 配置数据源。
- 创建OnCommand Insight 用户帐户。

OnCommand Insight 许可证

OnCommand Insight 使用许可证运行、这些许可证可在Insight服务器上启用特定功能。

- * 发现 *

  Discover是支持清单的基本Insight许可证。要使用OnCommand Insight 、您必须具有发现许可证、并且发现许可证必须至少与一个Assure、Perform或Plan许可证配对。

- 保证

  Assure许可证支持Assurance功能、包括全局和SAN路径策略以及违规管理。使用Assure许可证还可以查看和管理漏洞。

- 执行

  Perform许可证支持对资产页面、信息板小工具、查询等进行性能监控、并管理性能策略和违规。

- 计划

  Plan许可证支持规划功能、包括资源使用和分配。

- 主机利用率软件包

  主机利用率许可证支持主机和虚拟机上的文件系统利用率。

- 报告创作

  报告创作许可证支持其他作者进行报告。此许可证需要Plan许可证。

OnCommand Insight 模块按年期或永久期限获得许可：

- 按TB的监控容量来监控发现、保证、计划和执行模块
- 按Host Utilization Pack的主机数
- 按报告创作所需的其他Cognos专业作者单位数

许可证密钥是为每个客户生成的一组唯一字符串。您可以从OnCommand Insight 代表处获取许可证密钥。

已安装的许可证可控制软件中提供的以下选项：

- * 发现 *

  获取和管理清单(基础)

监控更改并管理清单策略

- 保证

  查看和管理SAN路径策略和违规

  查看和管理漏洞

  查看和管理任务和迁移

- 计划

  查看和管理请求

  查看和管理待定任务

  查看和管理预留违规

  查看和管理端口平衡违规

- 执行

  监控性能数据、包括信息板小工具、资产页面和查询中的数据

  查看和管理性能策略和违规

下表详细介绍了管理员用户和非管理员用户在使用和不使用Perform许可证的情况下可以使用的功能。

功能(管理员)	具有Perform许可证	没有Perform许可证
应用程序	是的。	无性能数据或图表
虚拟机	是的。	无性能数据或图表
虚拟机管理程序	是的。	无性能数据或图表
主机	是的。	无性能数据或图表
数据存储库	是的。	无性能数据或图表
VMDK	是的。	无性能数据或图表
内部卷	是的。	无性能数据或图表
Volume	是的。	无性能数据或图表
存储池	是的。	无性能数据或图表

Disk	是的。	无性能数据或图表
存储	是的。	无性能数据或图表
存储节点	是的。	无性能数据或图表
网络结构	是的。	无性能数据或图表
交换机端口	是的。	无性能数据或图表；“Port Errors`" 显示"`N/A”
存储端口	是的。	是的。
NPV端口	是的。	无性能数据或图表
交换机	是的。	无性能数据或图表
NPV交换机	是的。	无性能数据或图表
qtree	是的。	无性能数据或图表
配额	是的。	无性能数据或图表
路径	是的。	无性能数据或图表
分区	是的。	无性能数据或图表
区域成员	是的。	无性能数据或图表
通用设备	是的。	无性能数据或图表
磁带	是的。	无性能数据或图表
屏蔽	是的。	无性能数据或图表
iSCSI会话	是的。	无性能数据或图表
ICSI网络门户	是的。	无性能数据或图表
搜索	是的。	是的。
管理员	是的。	是的。

信息板	是的。	是的。
小工具	是的。	部分可用(仅提供资产、查询和管理小工具)
违规信息板	是的。	隐藏
资产信息板	是的。	部分可用(存储IOPS和虚拟机IOPS小工具将隐藏)
管理性能策略	是的。	隐藏
管理标注	是的。	是的。
管理标注规则	是的。	是的。
管理应用程序	是的。	是的。
查询	是的。	是的。
管理业务实体	是的。	是的。

功能	用户—具有Perform许可证	来宾—具有Perform许可证	用户—不具有Perform许可证	来宾—无Perform许可证
资产信息板	是的。	是的。	部分可用(存储IOPS和虚拟机IOPS小工具将隐藏)	部分可用(存储IOPS和虚拟机IOPS小工具将隐藏)
自定义信息板	仅查看(无创建、编辑或保存选项)	仅查看(无创建、编辑或保存选项)	仅查看(无创建、编辑或保存选项)	仅查看(无创建、编辑或保存选项)
管理性能策略	是的。	隐藏	隐藏	隐藏
管理标注	是的。	隐藏	是的。	隐藏
管理应用程序	是的。	隐藏	是的。	隐藏
管理业务实体	是的。	隐藏	是的。	隐藏
查询	是的。	仅查看和编辑(无保存选项)	是的。	仅查看和编辑(无保存选项)

设置和管理用户帐户

用户帐户、用户身份验证和用户授权可以通过以下两种方式定义和管理：在Microsoft Active Directory (版本2或3) LDAP (轻型目录访问协议)服务器或内部OnCommand Insight 用户数据库。为每个人设置不同的用户帐户可以控制访问权限、个人首选项和责任。请使用具有管理员权限的帐户执行此操作。

开始之前

您必须已完成以下任务：

- 安装OnCommand Insight 许可证。
- 为每个用户分配唯一的用户名。
- 确定要使用的密码。
- 分配正确的用户角色。

> 安全最佳实践要求管理员配置主机操作系统、以防止非管理员/标准用户交互登录。

步骤

1. 在浏览器中打开Insight。
2. 在Insight工具栏上、单击*管理*。
3. 单击*设置*。
4. 选择"*用户"*选项卡。
5. 要创建新用户、请单击*操作*按钮并选择*添加用户*。

   输入*名称*、密码、*电子邮件*地址、然后选择一个用户*角色*作为管理员、用户或来宾。

6. 要更改用户信息、请从列表中选择用户、然后单击用户问题描述 右侧的*编辑用户帐户*符号。
7. 要从OnCommand Insight 系统中删除用户、请从列表中选择该用户、然后单击用户问题描述 右侧的*删除用户帐户*。

结果

如果已启用LDAP、则在用户登录到OnCommand Insight 时、服务器会首先尝试通过LDAP进行身份验证。如果OnCommand Insight 在LDAP服务器上找不到该用户、则会在本地Insight数据库中搜索。

Insight用户角色

系统会为每个用户帐户分配三个可能的权限级别之一。

- 通过子系统、您可以登录到Insight并查看各种页面。
- 用户允许所有来宾级别的特权、并允许访问Insight操作、例如定义策略和标识通用设备。用户帐户类型不允许您执行数据源操作、也不允许添加或编辑除您自己帐户之外的任何用户帐户。

- 管理员允许您执行任何操作、包括添加新用户和管理数据源。

*最佳实践：*通过为用户或来宾创建大多数帐户来限制具有管理员权限的用户数量。

为LDAP配置Insight

OnCommand Insight 必须使用在公司LDAP域中配置的轻型目录访问协议(LDAP)设置进行配置。

在配置Insight以与LDAP或安全LDAP (LDAPS)结合使用之前、请记下企业环境中的Active Directory配置。Insight设置必须与您组织的LDAP域配置中的设置匹配。在配置Insight以用于LDAP之前、请查看以下概念、并与LDAP域管理员联系、了解要在您的环境中使用的正确属性。

对于所有安全Active Directory (例如LDAPS)用户、您必须使用证书中定义的AD服务器名称。不能使用IP地址进行安全AD登录。

> OnCommand Insight 通过Microsoft Active Directory服务器或Azure AD支持LDAP和LDAPS。其他LDAP实施可能有效、但尚未通过Insight认证。这些指南中的过程假定您使用的是Microsoft Active Directory版本2或3 LDAP (轻型目录访问协议)。

用户主体名称属性：

Insight使用LDAP User Principal Name属性(userPrincipalName)作为username属性。用户主体名称保证在Active Directory (AD)林中具有全局唯一性、但在许多大型组织中、用户主体名称可能不会立即为其所识别或识别。您的组织可能会在主用户名中使用User Principal Name属性的替代项。

以下是User Principal Name属性字段的一些备用值：

- * sAMAccountName*

  此用户属性是旧版Windows 2000 NT之前的用户名、大多数用户都习惯使用此用户登录到其个人Windows计算机。这并不能保证在整个AD林中具有全局唯一性。

  > 对于User Principal Name属性、sAMAccountName区分大小写。

- 邮件

  在使用MS Exchange的AD环境中、此属性是最终用户的主电子邮件地址。与userPrincipalName属性不同、此属性在整个AD林中应具有全局唯一性(最终用户也很熟悉)。大多数非MS Exchange环境中都不存在邮件属性。

- 转介

  LDAP转介是指域控制器向客户端应用程序指示其没有所请求对象的副本(或者更准确地说、 它不会保留目录树中该对象所在的部分(如果该对象确实存在)、并为客户端提供更可能持有该对象的位置。而客户端又会使用转介作为对域控制器进行DNS搜索的基础。理想情况下、转介始终引用确实持有该对象的域控制器。但是、转介到的域控制器可能会生成另一个转介、但通常不需要很长时间才能发现对象不存在并通知客户端。

sAMAccountName通常优先于用户主体名称。sAMAccountName在域中是唯一的(虽然在域林中可能不是唯一的)、但它是用户通常用于登录的字符串域(例如、*NetApp\username*)。Distinguished Name是林中的唯一名称、但通常不为用户所知。

在同一域的Windows系统部分上、您可以始终打开命令提示符并键入set以查找正确的域名(USERDOMAIN=)。然后、OCI登录名将为 `USERDOMAIN\sAMAccountName`。

域名*：mydomain.x.y.z.com *、请使用 `DC=x,DC=y,DC=z,DC=com` 在Insight的域字段中。

- 端口 *：

LDAP的默认端口为389、LDAPS的默认端口为636

LDAPS的典型URL： `ldaps://<ldap_server_host_name>:636`

日志位于：`\\<install directory>\SANscreen\wildfly\standalone\log\ldap.log`

默认情况下、Insight需要以下字段中记录的值。如果这些更改在Active Directory环境中发生、请务必在Insight LDAP配置中进行更改。

Role属性
成员
Mail属性
邮件
Distinguished Name属性
distinguishedName
转介
请遵循

组：

要对OnCommand Insight 和DWH服务器中具有不同访问角色的用户进行身份验证、您必须在Active Directory中创建组、并在OnCommand Insight 和DWH服务器中输入这些组名称。以下组名称仅为示例；您在Insight中为LDAP配置的名称必须与为Active Directory环境设置的名称匹配。

Insight Group	示例
Insight服务器管理员组	insight.server.admins

Insight管理员组	insight.m管理员
Insight用户组	insight.users
Insight来宾组	insight.guests
报告管理员组	insight.report.管理员
报告专业作者组	insight.report.proauthors
报告作者组	insight.report.business.authors
报告使用者组	insight.report.business.consumers
报告收件人组	insight.report.recipients

使用**LDAP**配置用户定义

要从LDAP服务器配置OnCommand Insight (OCI)以进行用户身份验证和授权、必须在LDAP服务器中将您定义为OnCommand Insight 服务器管理员。

开始之前

您必须知道在LDAP域中为Insight配置的用户和组属性。

对于所有安全Active Directory (例如LDAPS)用户、您必须使用证书中定义的AD服务器名称。不能使用IP地址进行安全AD登录。

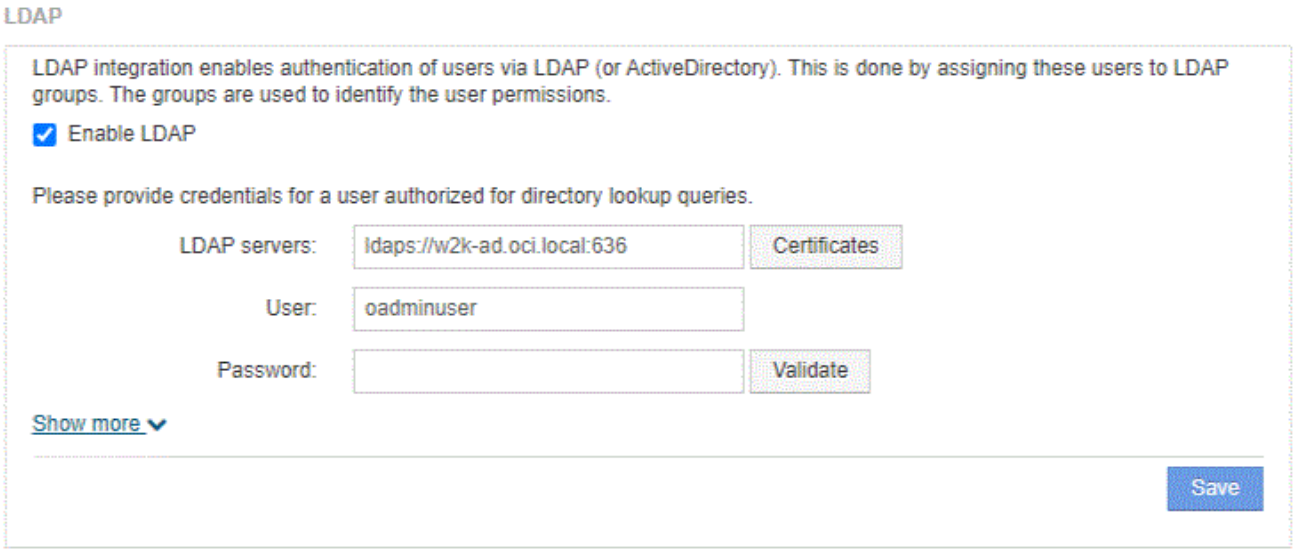
关于此任务

OnCommand Insight 通过Microsoft Active Directory服务器支持LDAP和LDAPS。其他LDAP实施可能有效、但尚未通过Insight认证。此操作步骤 假定您使用的是Microsoft Active Directory版本2或3 LDAP (轻型目录访问协议)。

LDAP用户与本地定义的用户一起显示在*管理*>菜单：设置[用户]列表中。

步骤

1. 在Insight工具栏上、单击*管理*。
2. 单击*设置*。
3. 单击*用户*选项卡。
4. 滚动到LDAP部分、如下所示。



5. 单击*启用LDAP*以允许LDAP用户进行身份验证和授权。
6. 填写以下字段：

   - `LDAP servers`：Insight接受以逗号分隔的LDAP URL列表。Insight会尝试连接到提供的URL、而不验证LDAP协议。

     > 要导入LDAP证书、请单击*证书*、然后自动导入或手动查找证书文件。

     用于标识LDAP服务器的IP地址或DNS名称通常采用以下格式输入：

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

     或者、如果使用默认端口：

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

     + 在此字段中输入多个LDAP服务器时、请确保在每个条目中使用正确的端口号。

   - `User name`：输入在LDAP服务器上有权进行目录查找查询的用户的凭据。
   - `Password`：输入上述用户的密码。要在LDAP服务器上确认此密码、请单击*验证*。
7. 如果要更精确地定义此LDAP用户、请单击*显示更多*并填写列出属性的字段。

   这些设置必须与LDAP域中配置的属性匹配。如果您不确定要为这些字段输入的值、请咨询Active Directory管理员。

   - 管理员组

     具有Insight管理员权限的用户的LDAP组。默认值为 `insight.admins`。

   - 用户组

具有Insight用户权限的用户的LDAP组。默认值为 `insight.users`。

- 来宾组

  具有Insight来宾权限的用户的LDAP组。默认值为 `insight.guests`。

- 服务器管理员组

  具有Insight Server管理员权限的用户的LDAP组。默认值为 `insight.server.admins`。

- 超时

  超时前等待LDAP服务器响应的时间长度、以毫秒为单位。默认值为2、000、这在所有情况下都是足够的、不应修改。

- 域

  OnCommand Insight 应开始查找LDAP用户的LDAP节点。通常、这是组织的顶级域。例如：

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

- 用户主体名称属性

  用于标识LDAP服务器中每个用户的属性。默认值为 `userPrincipalName`、全局唯一。OnCommand Insight 会尝试将此属性的内容与上述提供的用户名进行匹配。

- 角色属性

  用于确定用户是否适合指定组的LDAP属性。默认值为 `memberOf`。

- 邮件属性

  用于标识用户电子邮件地址的LDAP属性。默认值为 `mail`。如果您要订阅OnCommand Insight 提供的报告、此功能非常有用。Insight会在每个用户首次登录时获取用户的电子邮件地址、之后不会查找该地址。

  > 如果LDAP服务器上的用户电子邮件地址发生变化、请务必在Insight中对其进行更新。

- 可分辨名称属性

  用于标识用户可分辨名称的LDAP属性。默认值为 `distinguishedName`。

8. 单击 * 保存 * 。

更改用户密码

具有管理员权限的用户可以更改本地服务器上定义的任何OnCommand Insight 用户帐户的密码。

开始之前

必须已完成以下项目：

- 向登录到要修改的用户帐户的任何人发送通知。
- 更改后要使用的新密码。

关于此任务

使用此方法时、您无法更改通过LDAP验证的用户的密码。

步骤

1. 使用管理员权限登录。
2. 在Insight工具栏上、单击*管理*。
3. 单击*设置*。
4. 单击*用户*选项卡。
5. 找到显示要修改的用户帐户的行。
6. 单击用户信息右侧的*编辑用户帐户*。
7. 输入新的*密码*、然后在验证字段中再次输入。
8. 单击 * 保存 * 。

编辑用户定义

具有管理员权限的用户可以编辑用户帐户、以更改OnCommand Insight 或DWH的电子邮件地址或角色以及报告功能。

开始之前

确定需要更改的用户帐户类型(OnCommand Insight 、DWH或组合)。

关于此任务

对于LDAP用户、您只能使用此方法修改电子邮件地址。

步骤

1. 使用管理员权限登录。
2. 在Insight工具栏上、单击*管理*。
3. 单击*设置*。
4. 单击*用户*选项卡。
5. 找到显示要修改的用户帐户的行。
6. 单击用户信息右侧的*编辑用户帐户*图标。
7. 进行必要的更改。

8. 单击 * 保存 * 。

删除用户帐户

任何具有管理员权限的用户都可以删除不再使用的用户帐户(对于本地用户定义)、或者强制OnCommand Insight 在用户下次登录时重新发现用户信息(对于LDAP用户)。

步骤

1. 使用管理员权限登录到OnCommand Insight。
2. 在Insight工具栏上、单击*管理*。
3. 单击*设置*。
4. 单击*用户*选项卡。
5. 找到显示要删除的用户帐户的行。
6. 单击用户信息右侧的*删除用户帐户*"* x*"图标。
7. 单击 * 保存 * 。

设置登录警告消息

管理员可以通过OnCommand Insight 设置用户登录时显示的自定义文本消息。

步骤

1. 要在OnCommand Insight 服务器中设置消息、请执行以下操作：
   a. 导航到菜单：Admin[故障排除>高级故障排除>高级设置]。
   b. 在文本区域中输入登录消息。
   c. 单击*客户端显示登录警告消息*复选框。
   d. 单击 * 保存 * 。

      所有用户登录时都会显示此消息。
2. 要在数据仓库(DWH)和报告(Cognos)中设置消息、请执行以下操作：
   a. 导航到*系统信息*、然后单击*登录警告*选项卡。
   b. 在文本区域中输入登录消息。
   c. 单击 * 保存 * 。

      当DWH和Cognos报告所有用户登录时、将显示此消息。

Insight安全性

OnCommand Insight 7.3.1版引入了一些安全功能、可使Insight环境以增强的安全性运行。

这些功能包括对加密、密码哈希以及更改内部用户密码和用于对密码进行加密和解密的密钥对的功能进行了改进。您可以在Insight环境中的所有服务器上管理这些功能。

Insight的默认安装包括一种安全配置、其中、环境中的所有站点共享相同的密钥和相同的默认密码。为了保护敏感数据、NetApp建议您在安装或升级后更改默认密钥和采集用户密码。

数据源加密密码存储在Insight Server数据库中。服务器具有一个公共密钥、当用户在WebUI数据源配置页面中输入密码时、它会对密码进行加密。服务器没有对存储在服务器数据库中的数据源密码进行解密所需的专用密钥。只有采集单元(LAU、RAU)具有解密数据源密码所需的数据源专用密钥。

重新设置服务器密钥

使用默认密钥会在您的环境中引入安全漏洞。默认情况下、数据源密码会以加密方式存储在Insight数据库中。它们使用所有Insight安装通用的密钥进行加密。在默认配置中、发送到NetApp的Insight数据库包含理论上可由NetApp解密的密码。

更改采集用户密码

使用默认的"采集"用户密码会在您的环境中引入安全漏洞。所有采集单元均使用"`Acquisition`"用户与服务器进行通信。理论上、使用默认密码的RAU可以使用默认密码连接到任何Insight服务器。

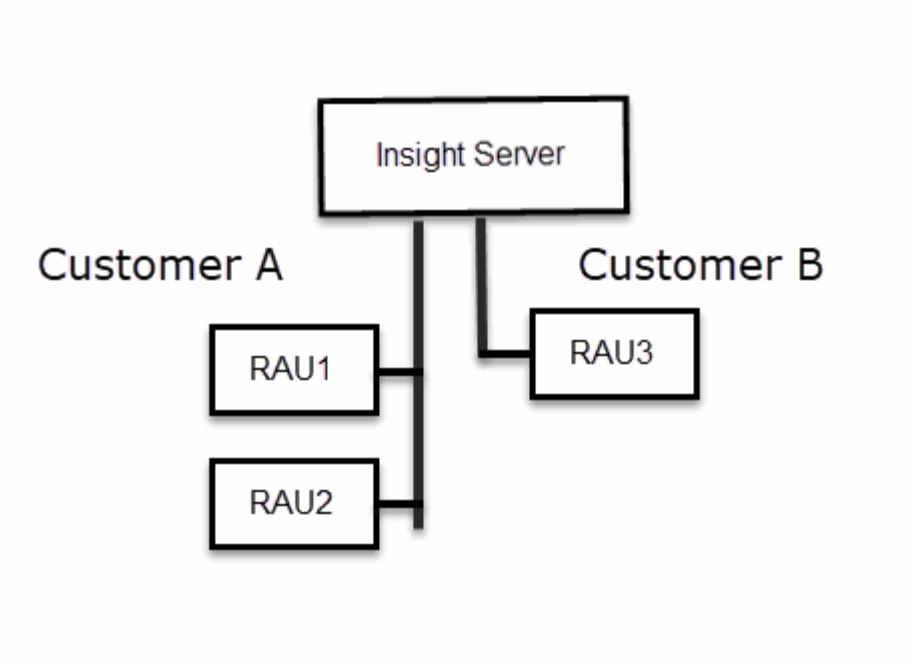
升级和安装注意事项

如果Insight系统包含非默认安全配置(您已重新设置密钥或更改密码)、则必须备份安全配置。安装新软件或在某些情况下升级软件会将系统还原为默认安全配置。当您的系统还原到默认配置时、您必须还原非默认配置、系统才能正常运行。

在复杂的服务提供商环境中管理密钥

一个服务提供商可以托管多个收集数据的OnCommand Insight 客户。这些密钥可防止多个客户在Insight服务器上未经授权访问客户数据。每个客户的数据都受其特定密钥对的保护。

可以按下图所示配置此Insight实施。



您需要为此配置中的每个客户创建单独的密钥。客户A要求两个RAU使用相同的密钥。客户B需要一组密钥。

更改客户A的加密密钥时应执行的步骤：

1. 远程登录到托管RAU1的服务器。
2. 启动安全管理工具。
3. 选择更改加密密钥以替换默认密钥。
4. 选择备份以创建安全配置的备份zip文件。
5. 远程登录到托管RAU2的服务器。
6. 将安全配置的备份zip文件复制到RAU2。
7. 启动安全管理工具。
8. 将安全备份从RAU1还原到当前服务器。

更改客户B的加密密钥时应执行的步骤：

1. 远程登录到托管RAU3的服务器。
2. 启动安全管理工具。
3. 选择更改加密密钥以替换默认密钥。
4. 选择备份以创建安全配置的备份zip文件。

管理Insight服务器上的安全性

。 `securityadmin` 使用工具可以管理Insight服务器上的安全选项。安全管理包括更改密码、生成新密钥、保存和还原您创建的安全配置或将配置还原为默认设置。

关于此任务

您可以使用 `securityadmin` 用于管理安全性的工具：

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

步骤

1. 远程登录到Insight服务器。
2. 在交互模式下启动安全管理工具：
   - Windows - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i`
   - Linux - `/bin/oci-securityadmin.sh -i`

     系统请求登录凭据。
3. 输入具有"`Admin`"凭据的帐户的用户名和密码。
4. 选择 * 服务器 * 。

   可以使用以下服务器配置选项：

   - * 备份 *

     为包含所有密码和密钥的存储创建一个备份zip文件、并将该文件放置在用户指定的位置或以下默认位置：

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

     还原已创建的存储的zip备份。还原后、所有密码和密钥将还原为创建备份时的现有值。

     > 还原可用于同步多个服务器上的密码和密钥、例如：-更改一台服务器上的服务器加密密钥-创建存储的备份-将存储备份还原到第二台服务器
   - 更改加密密钥

     更改用于对代理用户密码、SMTP用户密码、LDAP用户密码等进行加密或解密的服务器加密密钥。

     > 更改加密密钥时、您应备份新的安全配置、以便在升级或安装后还原它。
   - 更新密码

     更改Insight使用的内部帐户的密码。此时将显示以下选项：

     - 内部
     - 采集

- Cognos_admin
- dwh_internal
- 主机
- 清单
- root

> 更改密码后、某些帐户需要同步。例如、如果您更改服务器上"采集"用户的密码、则需要更改LAU、RAU和DWH上"采集"用户的密码以使其匹配。此外、更改密码时、您应备份新的安全配置、以便在升级或安装后还原它。

- 重置为默认值

  将密钥和密码重置为默认值。默认值是在安装期间提供的值。

- * 退出 *

  退出 `securityadmin` 工具。

  a. 选择要更改的选项、然后按照提示进行操作。

管理本地采集单元上的安全性

。 `securityadmin` 使用工具可以管理本地采集用户(LAU)上的安全选项。安全管理包括管理密钥和密码、保存和还原您创建的安全配置或将配置还原为默认设置。

开始之前

您必须拥有 `admin` 执行安全配置任务的权限。

关于此任务

您可以使用 `securityadmin` 用于管理安全性的工具：

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

步骤

1. 远程登录到Insight服务器。
2. 在交互模式下启动安全管理工具：
   - Windows - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i`
   - Linux - `/bin/oci-securityadmin.sh -i`

     系统请求登录凭据。

3. 输入具有"`Admin`"凭据的帐户的用户名和密码。

4. 选择*本地采集单元*以重新配置本地采集单元安全配置。

   此时将显示以下选项：

   - * 备份 *

     为包含所有密码和密钥的存储创建一个备份zip文件、并将该文件放置在用户指定的位置或以下默认位置：

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

   - * 还原 *

     还原已创建的存储的zip备份。还原后、所有密码和密钥将还原为创建备份时的现有值。

     > 还原可用于同步多个服务器上的密码和密钥、例如：-更改LAU上的加密密钥-创建存储备份-将存储备份还原到每个RAU

   - 更改加密密钥

     更改用于对设备密码进行加密或解密的AU加密密钥。

     > 更改加密密钥时、您应备份新的安全配置、以便在升级或安装后还原它。

   - 更新密码

     更改"采集"用户帐户的密码。

     > 更改密码后、某些帐户需要同步。例如、如果您更改服务器上"采集"用户的密码、则需要更改LAU、RAU和DWH上"采集"用户的密码以使其匹配。此外、更改密码时、您应备份新的安全配置、以便在升级或安装后还原它。

   - 重置为默认值

     将采集用户密码和采集用户加密密钥重置为默认值、默认值是在安装期间提供的值。

   - * 退出 *

     退出 `securityadmin` 工具。

5. 选择要配置的选项、然后按照提示进行操作。

管理RAU上的安全性

。 `securityadmin` 使用工具可以管理RAU上的安全选项。您可能需要备份或还原存储配置、更改加密密钥或更新采集单元的密码。

关于此任务

您可以使用 `securityadmin` 用于管理安全性的工具：

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

更新LAU安全配置的一种情形是、在服务器上更改了"采集"用户密码后、RAU会更新该用户的密码。所有RAU和LAU都使用与服务器"采集"用户相同的密码与服务器进行通信。

"采集"用户仅存在于Insight服务器上。RAU或LAU在连接到服务器时以该用户身份登录。

使用以下步骤管理RAU上的安全选项：

步骤

1. 远程登录到运行RAU的服务器
2. 在交互模式下启动安全管理工具：
   - Windows - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i`
   - Linux - `/bin/oci-securityadmin.sh -i`

     系统请求登录凭据。
3. 输入具有"`Admin`"凭据的帐户的用户名和密码。

   系统将显示RAU的菜单。

   - * 备份 *

     为包含所有密码和密钥的存储创建一个备份zip文件、并将该文件放置在用户指定的位置或以下默认位置：

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

     还原已创建的存储的zip备份。还原后、所有密码和密钥将还原为创建备份时的现有值。

     > 还原可用于同步多个服务器上的密码和密钥、例如：-更改一个服务器上的加密密钥-创建存储备份-将存储备份还原到第二个服务器
   - 更改加密密钥

     更改用于对设备密码进行加密或解密的RAU加密密钥。

     > 更改加密密钥时、您应备份新的安全配置、以便在升级或安装后还原它。
   - 更新密码

更改"采集"用户帐户的密码。

> 更改密码后、某些帐户需要同步。例如、如果您更改服务器上"采集"用户的密码、则需要更改LAU、RAU和DWH上"采集"用户的密码以使其匹配。此外、更改密码时、您应备份新的安全配置、以便在升级或安装后还原它。

- 重置为默认值

  将加密密钥和密码重置为默认值。默认值是在安装期间提供的值。

- * 退出 *

  退出 `securityadmin` 工具。

管理数据仓库上的安全性

。 `securityadmin` 您可以使用工具管理数据仓库服务器上的安全选项。安全管理包括更新DWH服务器上内部用户的内部密码、创建安全配置的备份或将配置还原为默认设置。

关于此任务

您可以使用 `securityadmin` 用于管理安全性的工具：

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

步骤

1. 远程登录到数据仓库服务器。
2. 在交互模式下启动安全管理工具：
   - Windows - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i`
   - Linux - `/bin/oci-securityadmin.sh -i`

     系统请求登录凭据。
3. 输入具有"`Admin`"凭据的帐户的用户名和密码。

   系统将显示数据仓库的安全管理员菜单：

   - * 备份 *

     为包含所有密码和密钥的存储创建一个备份zip文件、并将该文件放置在用户指定的位置或默认位置：

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

还原已创建的存储的zip备份。还原后、所有密码和密钥将还原为创建备份时的现有值。

> 还原可用于同步多个服务器上的密码和密钥、例如：-更改一个服务器上的加密密钥-创建存储备份-将存储备份还原到第二个服务器
>
> +

- 更改加密密钥

  更改用于对连接器密码和SMPT密码等密码进行加密或解密的DWH加密密钥。

- 更新密码

  更改特定用户帐户的密码。

  - 内部
  - 采集
  - Cognos_admin
  - dwh
  - dwh_internal
  - dwhuser
  - 主机
  - 清单
  - root

> 更改dwhuser、hosts、inventory或root密码时、您可以选择使用SHA-256密码哈希。此选项要求访问这些帐户的所有客户端都使用SSL连接。

+

- 重置为默认值

  将加密密钥和密码重置为默认值。默认值是在安装期间提供的值。

- * 退出 *

  退出 `securityadmin` 工具。

更改**OnCommand Insight** 内部用户密码

安全策略可能要求您更改OnCommand Insight 环境中的密码。一台服务器上的某些密码存在于环境中的另一台服务器上、要求您更改这两台服务器上的密码。例如、在Insight服务器上更改"`inventory`"用户密码时、必须与为该Insight服务器配置的Data Warehouse server Connector上的"`inventory`"用户密码匹配。

开始之前

> 在更改密码之前、您应了解用户帐户的依赖关系。如果未更新所有所需服务器上的密码、则Insight组件之间的通信将失败。

关于此任务

下表列出了Insight服务器的内部用户密码、并列出了具有需要与新密码匹配的相关密码的Insight组件。

Insight服务器密码	所需更改
内部	
采集	LAU、RAU
dwh_internal	数据仓库
主机	
清单	数据仓库
root	

下表列出了数据仓库的内部用户密码、并列出了具有需要与新密码匹配的相关密码的Insight组件。

数据仓库密码	所需更改
Cognos_admin	
dwh	
dwh_internal (使用服务器连接器配置UI进行更改)	Insight服务器
dwhuser	
主机	
清单(使用Server Connector配置UI进行更改)	Insight服务器
root	

在**DWH**服务器连接配置用户界面中更改密码

下表列出了LAU的用户密码、并列出了具有需要与新密码匹配的相关密码的Insight组件。

LAU密码	所需更改

采集	Insight服务器、RAU

使用服务器连接配置**UI**更改**"**清单**"**和**"dwh_interne"**密码

如果您需要更改"`inventory`"或`dwh_internal`"密码以匹配Insight服务器上的密码、请使用数据仓库UI。

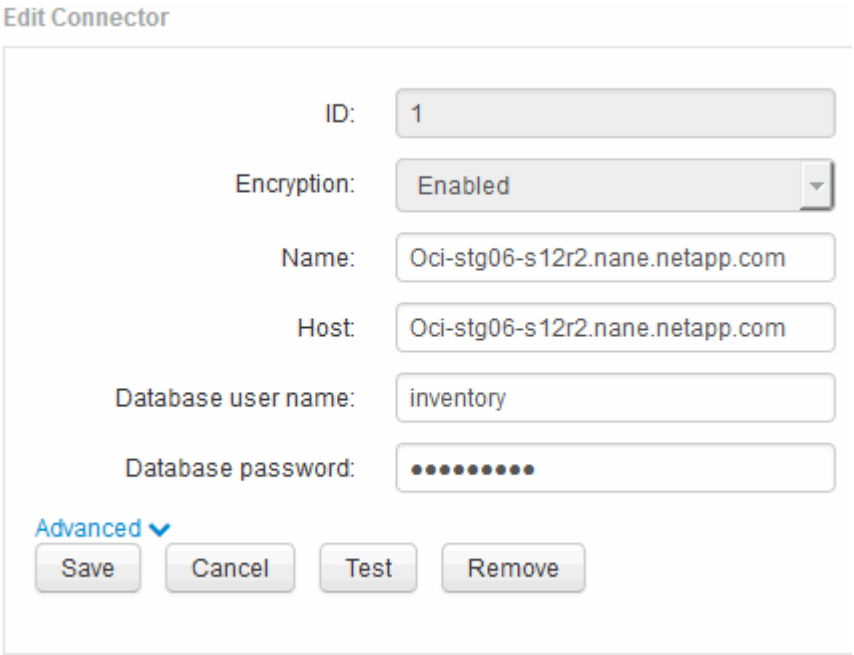
开始之前

要执行此任务、您必须以管理员身份登录。

步骤

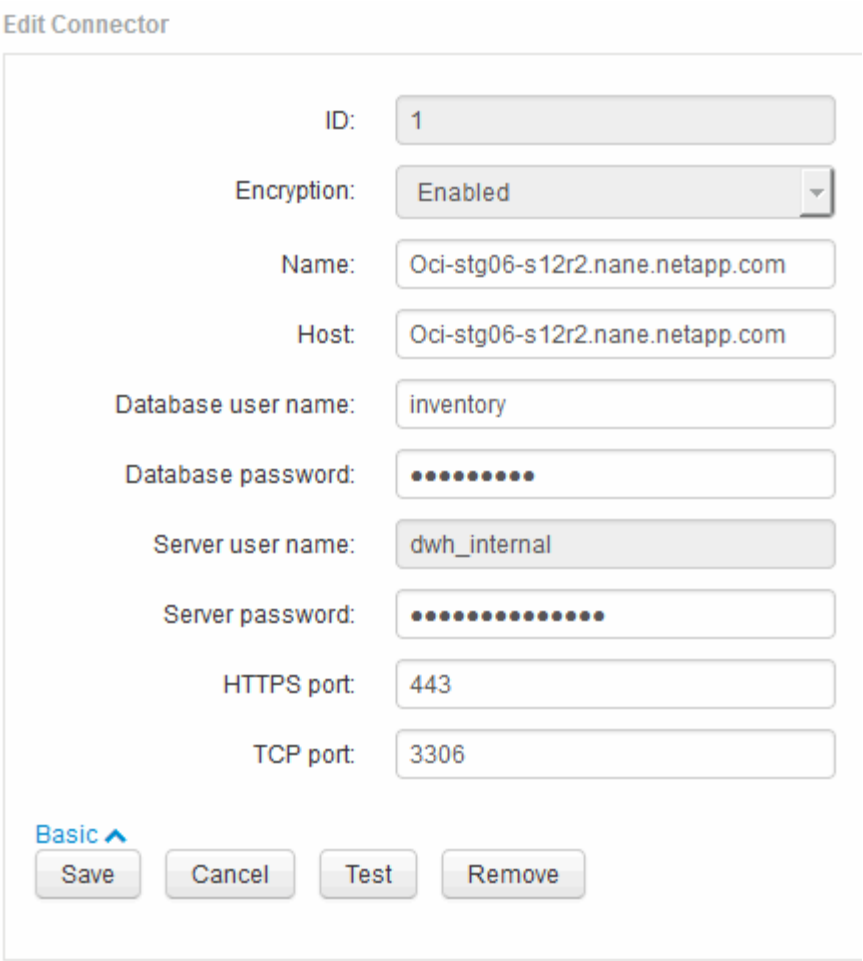
1. 登录到数据仓库门户、网址为 https://hostname/dwh、其中hostname是安装了OnCommand Insight 数据仓库的系统的名称。
2. 从左侧导航窗格中、单击*连接器*。

   此时将显示*编辑连接器*屏幕。



3. 为*数据库密码*字段输入新的"`inventory`"密码。
4. 单击 * 保存 * 。
5. 要更改`dwh_internal`密码、请单击*高级。*

   此时将显示编辑连接器高级屏幕。



6. 在*服务器密码*字段中输入新密码：
7. 单击保存。

使用**ODBC**管理工具更改**dwh**密码

在Insight服务器上更改dwh用户的密码时、还必须在数据仓库服务器上更改此密码。您可以使用ODBC数据源管理员工具更改数据仓库上的密码。

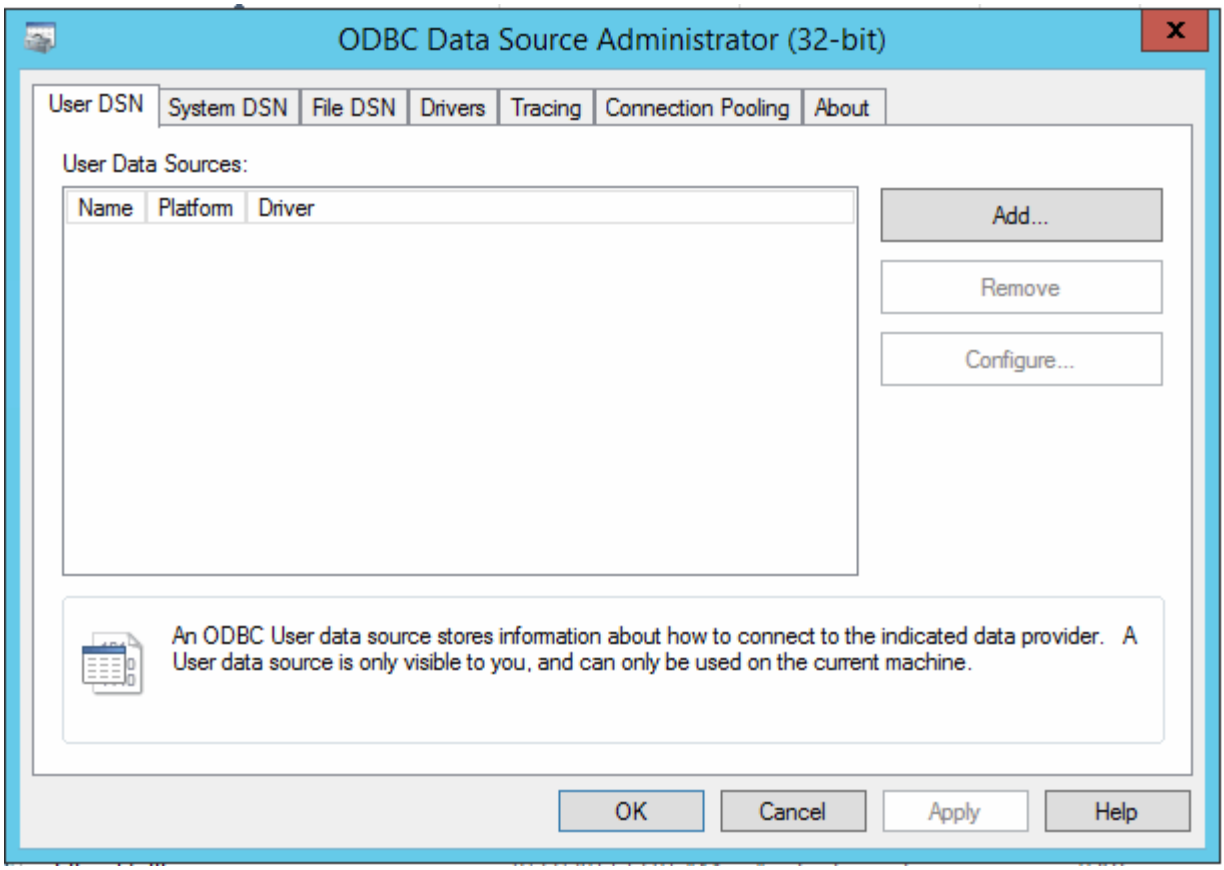
开始之前

您必须使用具有管理员权限的帐户远程登录到数据仓库服务器。

步骤

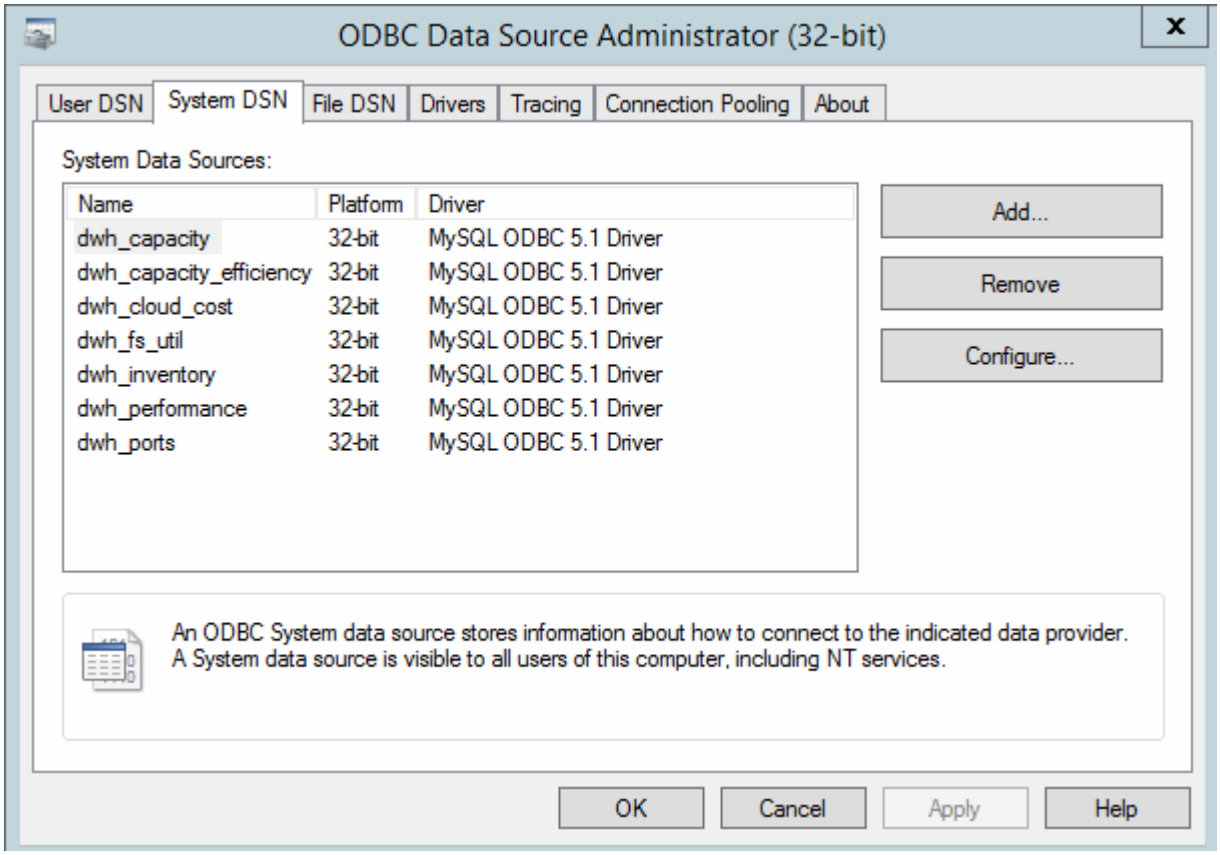
1. 远程登录到托管该数据仓库的服务器。
2. 访问ODBC管理工具、网址为 `C:\Windows\SysWOW64\odbcad32.exe`

   系统将显示"ODBC数据源管理员"屏幕。



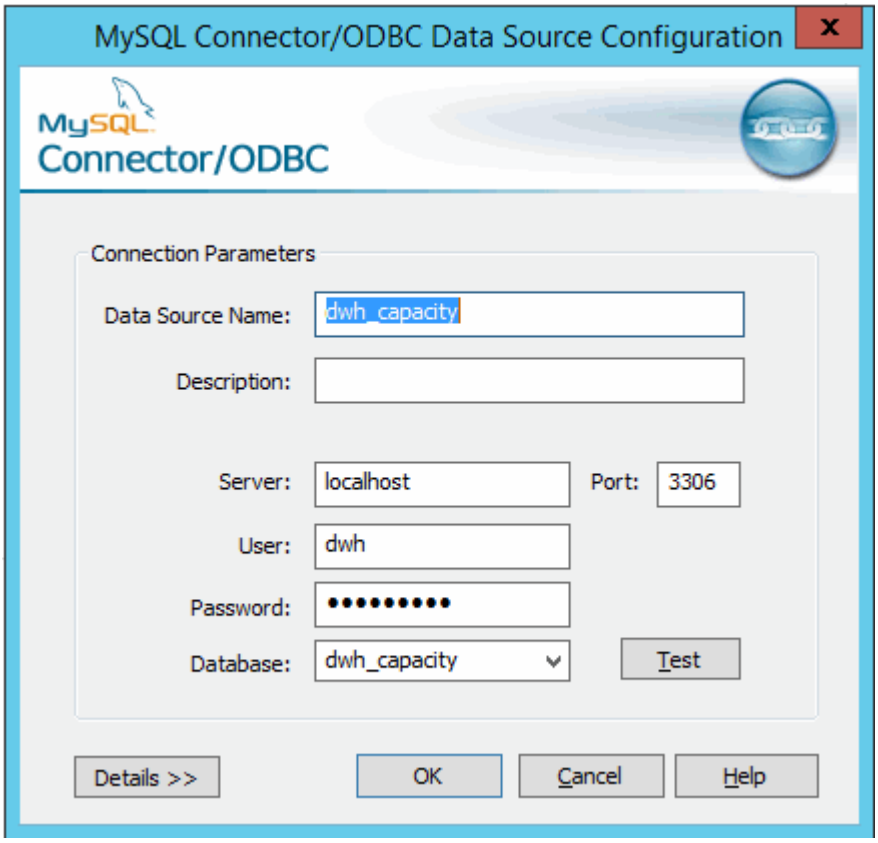
3. 单击*系统DSN*

此时将显示系统数据源。



4. 从列表中选择一个OnCommand Insight 数据源。
5. 单击*配置*

   此时将显示Data Source Configuration屏幕。



6. 在*密码*字段中输入新密码。

支持智能卡和证书登录

OnCommand Insight 支持使用智能卡(CAC)和证书对登录到Insight服务器的用户进行身份验证。要启用这些功能、必须对系统进行配置。

将系统配置为支持CAC和证书后、导航到新的OnCommand Insight 会话会导致浏览器显示一个本机对话框、为用户提供一个可供选择的个人证书列表。这些证书将根据OnCommand Insight 服务器信任的CA颁发的一组个人证书进行筛选。大多数情况下、只有一个选择。默认情况下、如果只有一个选项、Internet Explorer将跳过此对话框。

> 对于CAC用户、智能卡包含多个证书、其中只有一个证书可以与受信任的CA匹配。的CAC证书 `identification` 应使用。

有关最新的CAC和证书说明、请参见以下知识库文章(需要支持登录)：

- "如何为OnCommand Insight 配置通用访问卡(CAC)身份验证"
- "如何为OnCommand Insight 数据仓库配置通用访问卡(CAC)身份验证"
- "如何创建证书颁发机构(CA)签名证书并将其导入到OnComand Insight和OnCommand Insight 数据仓库7.3.x中"
- "如何在Windows主机上安装的OnCommand Insight 7.3.X中创建自签名证书"
- "如何将Cognos证书颁发机构(CA)签名证书导入到OnCommand 数据中心7.3.3及更高版本中"

为主机配置智能卡和证书登录

您必须修改OnCommand Insight 主机配置、以支持智能卡(CAC)和证书登录。

开始之前

- 必须在系统上启用LDAP。
- LDAP `User principal account name` 属性必须与包含用户ID的LDAP字段匹配。

有关最新的CAC和证书说明、请参见以下知识库文章(需要支持登录)：

- "如何为OnCommand Insight 配置通用访问卡(CAC)身份验证"
- "如何为OnCommand Insight 数据仓库配置通用访问卡(CAC)身份验证"
- "如何创建证书颁发机构(CA)签名证书并将其导入到OnComand Insight和OnCommand Insight 数据仓库7.3.x中"
- "如何在Windows主机上安装的OnCommand Insight 7.3.X中创建自签名证书"
- "如何将Cognos证书颁发机构(CA)签名证书导入到OnCommand 数据中心7.3.3及更高版本中"

步骤

1. 使用 `regedit` 用于修改注册表值的实用程序 `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun2.0\SANscreen Server\Parameters\Java`：
   a. 更改JVM_Option `DclientAuth=false` to `DclientAuth=true`.
2. 备份密钥库文件： `C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
3. 打开指定的命令提示符 `Run as administrator`
4. 删除自生成的证书： `C:\Program Files\SANscreen\java64\bin\keytool.exe -delete -alias "ssl certificate" -keystore C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
5. 生成新证书： `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. 生成证书签名请求(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. 在步骤6中返回CSR后、导入证书、然后以Base-64格式导出证书并将其放入 `"C:\temp"` named `servername.cer`。
8. 从密钥库提取证书：`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. 从p12文件提取私钥： `openssl pkcs12 -in "C:\temp\file.p12" -out "C:\temp\servername.private.pem"`
10. 将步骤7中导出的Base-64证书与私钥合并： `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. 将合并的证书导入到密钥库中： `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. 导入根证书： `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. 将根证书导入到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. 导入中间证书： `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"`

    对所有中间证书重复此步骤。

15. 在LDAP中指定与此示例匹配的域。
16. 重新启动服务器。

配置客户端以支持智能卡和证书登录

客户端计算机需要使用中间件并修改浏览器、才能使用智能卡并登录证书。已在使用智能卡的客户不需要对其客户端计算机进行其他修改。

开始之前

> 有关最新的CAC和证书说明、请参见以下知识库文章(需要支持登录)：
>
> - "如何为OnCommand Insight 配置通用访问卡(CAC)身份验证"
> - "如何为OnCommand Insight 数据仓库配置通用访问卡(CAC)身份验证"
> - "如何创建证书颁发机构(CA)签名证书并将其导入到OnComand Insight和OnCommand Insight 数据仓库7.3.x中"
> - "如何在Windows主机上安装的OnCommand Insight 7.3.X中创建自签名证书"
> - "如何将Cognos证书颁发机构(CA)签名证书导入到OnCommand 数据中心7.3.3及更高版本中"

关于此任务

以下是常见的客户端配置要求：

- 安装智能卡中间件、例如ActivClient (请参见
- 修改IE浏览器(请参见
- 修改Firefox浏览器(请参见

在Linux服务器上启用CAC

要在Linux OnCommand Insight 服务器上启用CAC、需要进行一些修改。

步骤

1. 导航到 `/opt/netapp/oci/conf/`
2. 编辑 `wildfly.properties` 并更改的值 `CLIENT_AUTH_ENABLED` 设置为"True"
3. 导入下存在的"`根证书`" `/opt/netapp/oci/wildfly/standalone/configuration/server.keystore`
4. 重新启动服务器

为智能卡和证书登录配置数据仓库

您必须修改OnCommand Insight 数据仓库配置以支持智能卡(CAC)和证书登录。

开始之前

- 必须在系统上启用LDAP。
- LDAP `User principal account name` 属性必须与包含用户的政府ID编号的LDAP字段匹配。

  政府颁发的CAC上存储的公用名(Common Name、CN)通常采用以下格式： `first.last.ID`。对于某些LDAP字段、例如 `sAMAccountName`、此格式太长。对于这些字段、OnCommand Insight 仅从CN中提取ID编号。

有关最新的CAC和证书说明、请参见以下知识库文章(需要支持登录)：

- "如何为OnCommand Insight 配置通用访问卡(CAC)身份验证"
- "如何为OnCommand Insight 数据仓库配置通用访问卡(CAC)身份验证"
- "如何创建证书颁发机构(CA)签名证书并将其导入到OnComand Insight和OnCommand Insight 数据仓库7.3.x中"
- "如何在Windows主机上安装的OnCommand Insight 7.3.X中创建自签名证书"
- "如何将Cognos证书颁发机构(CA)签名证书导入到OnCommand 数据中心7.3.3及更高版本中"

步骤

1. 使用regedit修改中的注册表值 `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun2.0\SANscreen Server\Parameters\Java`

   a. 更改JVM_Option `-DclientAuth=false` to `-DclientAuth=true`。

   对于Linux、修改 `clientAuth` 参数 `/opt/netapp/oci/scripts/wildfly.server`

2. 将证书颁发机构(CA)添加到数据仓库存储库：

   a. 在命令窗口中、转至 `..\SANscreen\wildfly\standalone\configuration`。

   b. 使用 `keytool` 用于列出受信任CA的实用程序： `C:\Program Files\SANscreen\java64\bin\keytool.exe -list -keystore server.trustore -storepass changeit`

      每行中的第一个词表示CA别名。

   c. 如有必要、请提供CA证书文件、通常为 `.pem` 文件要将客户的CA加入到数据仓库受信任的CA中、请转至 `..\SANscreen\wildfly\standalone\configuration` 并使用 `keytool` 导入命令： `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore server.trustore -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

      my_alias通常是一个可轻松在中标识CA的别名`keytool -list` 操作。

3. 在OnCommand Insight 服务器上、 `wildfly/standalone/configuration/standalone-full.xml` 需要通过在中将verify-client更新为"已请求"来修改文件 `/subsystem=undertow/server=default-server/https-listener=default-https`以启用CAC。登录到Insight服务器并运行相应的命令：

os	脚本
Windows	<install dir> \SANscreen\wildfly\bin\enableCACforRemoteEJB.bat
Linux	/opt/netapp/oci/wildfly/bin/enableCACforRemoteEJB.sh

执行此脚本后、请等待此wildfly服务器的重新加载完成、然后再继续执行下一步。

4. 重新启动OnCommand Insight 服务器。

为智能卡和证书登录配置Cognos (OnCommand Insight 7.3.5至7.3.9)

您必须修改OnCommand Insight 数据仓库配置、以支持Cognos服务器的智能卡(CAC)和证书登录。

开始之前

此操作步骤 适用于运行OnCommand Insight 7.3.5至7.3.3的系统。

> 有关最新的CAC和证书说明、请参见以下知识库文章(需要支持登录)：
>
> - "如何为OnCommand Insight 配置通用访问卡(CAC)身份验证"
> - "如何为OnCommand Insight 数据仓库配置通用访问卡(CAC)身份验证"
> - "如何创建证书颁发机构(CA)签名证书并将其导入到OnComand Insight和OnCommand Insight 数据仓库7.3.x中"
> - "如何在Windows主机上安装的OnCommand Insight 7.3.X中创建自签名证书"
> - "如何将Cognos证书颁发机构(CA)签名证书导入到OnCommand 数据中心7.3.3及更高版本中"

步骤

1. 将证书颁发机构(CA)添加到Cognos truestore。
   a. 在命令窗口中、转至 `..\SANscreen\cognos\analytics\configuration\certs\`
   b. 使用 `keytool` 用于列出受信任CA的实用程序： `..\..\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass NoPassWordSet`

      每行中的第一个词表示CA别名。

   c. 如果不存在合适的文件、请提供CA证书文件、通常为 `.pem` 文件
   d. 要将客户的CA与OnCommand Insight 可信CA结合使用、请转至 `..\SANscreen\cognos\analytics\configuration\certs\`。
   e. 使用 `keytool` 用于导入的实用程序 `.pem` 文件： `..\..\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

      `my_alias` 通常是一个可在中轻松标识CA的别名`keytool -list` 操作。

   f. 当系统提示您输入密码时、输入 `NoPassWordSet`。
   g. 问题解答 `yes` 当系统提示您信任此证书时。
2. 要启用CAC模式、请执行 `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`
3. 要禁用CAC模式、请执行 `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`

为智能卡和证书登录配置Cognos (OnCommand Insight 7.3.10及更高版本)

您必须修改OnCommand Insight 数据仓库配置、以支持Cognos服务器的智能卡(CAC)和证书登录。

开始之前

此操作步骤 适用于运行OnCommand Insight 7.3.10及更高版本的系统。

> 有关最新的CAC和证书说明、请参见以下知识库文章(需要支持登录)：
>
> - "如何为OnCommand Insight 配置通用访问卡(CAC)身份验证"
> - "如何为OnCommand Insight 数据仓库配置通用访问卡(CAC)身份验证"
> - "如何创建证书颁发机构(CA)签名证书并将其导入到OnComand Insight和OnCommand Insight 数据仓库7.3.x中"
> - "如何在Windows主机上安装的OnCommand Insight 7.3.X中创建自签名证书"
> - "如何将Cognos证书颁发机构(CA)签名证书导入到OnCommand 数据中心7.3.3及更高版本中"

步骤

1. 将证书颁发机构(CA)添加到Cognos truestore。
   a. 在命令窗口中、转至 `..\SANscreen\cognos\analytics\configuration\certs\`
   b. 使用 `keytool` 用于列出受信任CA的实用程序： `..\..\ibm-jre\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass NoPassWordSet`

      每行中的第一个词表示CA别名。

   c. 如果不存在合适的文件、请提供CA证书文件、通常为 `.pem` 文件
   d. 要将客户的CA与OnCommand Insight 可信CA结合使用、请转至 `..\SANscreen\cognos\analytics\configuration\certs\`。
   e. 使用 `keytool` 用于导入的实用程序 `.pem` 文件： `..\..\ibm-jre\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

      `my_alias` 通常是一个可在中轻松标识CA的别名`keytool -list` 操作。

   f. 当系统提示您输入密码时、输入 `NoPassWordSet`。
   g. 问题解答 `yes` 当系统提示您信任此证书时。
2. 要启用CAC模式、请执行以下操作：
   a. 使用以下步骤配置CAC注销页面：
      - 登录到Cognos门户(用户必须属于系统管理员组、例如Cognos_admin)
      - (仅适用于7.3.10和7.3.11)单击"管理"→"配置"→"系统"→"安全性"
      - (仅适用于7.3.10和7.3.11)针对注销重定向URL <→应用输入cacLogout.html

    - 关闭浏览器。
  b. 执行 `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`
  c. 启动IBM Cognos服务。等待Cognos服务启动。
3. 要禁用CAC模式、请执行以下操作：
  a. 执行 `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`
  b. 启动IBM Cognos服务。等待Cognos服务启动。
  c. (仅适用于7.3.10和7.3.11)使用以下步骤取消配置CAC注销页面：
    - 登录到Cognos门户(用户必须属于系统管理员组、例如Cognos_admin)
    - 单击"管理"→"配置"→"系统"→"安全性"
    - 在注销重定向URL <→应用中输入cacLogout.html
    - 关闭浏览器。

导入Cognos和DWH的CA签名SSL证书(Insight 7.3.5至7.3.9)

您可以添加SSL证书、以便为数据仓库和Cognos环境启用增强型身份验证和加密。

开始之前

此操作步骤 适用于运行OnCommnand Insight 7.3.5至7.3.9的系统。

> 有关最新的CAC和证书说明、请参见以下知识库文章(需要支持登录)：
>
> - "如何为OnCommand Insight 配置通用访问卡(CAC)身份验证"
> - "如何为OnCommand Insight 数据仓库配置通用访问卡(CAC)身份验证"
> - "如何创建证书颁发机构(CA)签名证书并将其导入到OnComand Insight和OnCommand Insight 数据仓库7.3.x中"
> - "如何在Windows主机上安装的OnCommand Insight 7.3.X中创建自签名证书"
> - "如何将Cognos证书颁发机构(CA)签名证书导入到OnCommand 数据中心7.3.3及更高版本中"

关于此任务

要执行此操作步骤 、您必须具有管理员权限。

步骤

1. 创建的备份 `..\SANScreen\cognos\analytics\configuration\cogstartup.xml`。
2. 在下创建"`certs`"和"`csk`"文件夹的备份 `..\ SANScreen\cognos\analytics\configuration`。
3. 从Cognos生成证书加密请求。在管理CMD窗口中、运行：
  a. CD `"\Program Files\sanscreen\cognos\analytics\bin"`
  b. `ThirdPartyCertificateTool.bat -java:local -c -e -p NoPassWordSet -a RSA -d "CN=FQDN,O=orgname,C=US" -r c:\temp\encryptRequest.csr`

4. 打开 `c:\temp\encryptRequest.csr` 归档并复制生成的内容。
5. 将encryptRequest.csr发送到证书颁发机构(CA)以获取SSL证书。

   请务必添加其他属性、例如"`San：dns=fqdn "(例如、hostname.netapp.com)`")以添加SubjectAltName。如果证书中缺少SubjectAltName、则Google Chrome 58及更高版本会进行投诉。

6. 使用PKCS7格式包含根证书以下载链证书

   此操作将下载FQDN.p7b文件

7. 从CA获取.p7b格式的证书。请使用一个名称将其标记为Cognos Web服务器的证书。
8. ThirdPartyCertificateTool.bat无法导入整个链、因此导出所有证书需要执行多个步骤。按如下所示单独导出链、从而拆分链：
   a. 在"`Crypto Shell扩展名`"中打开.p7b证书。
   b. 在左窗格中浏览到"`Certificates`"。
   c. 右键单击根CA >所有任务>导出。
   d. 选择Base64输出。
   e. 输入一个文件名、将其标识为根证书。
   f. 重复步骤8a到8c、将所有证书单独导出到.cer文件中。
   g. 将文件命名为intermediateX.cer和Cognos.cer。
9. 如果只有一个CA证书、请忽略此步骤、否则、请将root.cer和intermediateX.cer合并到一个文件中。
   a. 使用Notepad打开intermediate.cer并复制内容。
   b. 使用Notepad打开root.cer并保存9a中的内容。
   c. 将文件保存为CA.cer。
10. 使用管理CMD提示符将证书导入到Cognos密钥库中：
    a. cd “Program Files\SANscreen\cognos\Analytics \bin”
    b. ThirdPartyCertificateTool.bat -java：local -i -T -r c：\temp\cA.cer

       此操作会将CA.cer设置为根证书颁发机构。

    c. ThirdPartyCertificateTool.bat -java：local -i -e -r c：\temp\cognos.cer -t c：\temp\ca.cer

       此操作会将Cognos.cer设置为由CA.cer签名的加密证书。

11. 打开IBM Cognos配置。
    a. 选择本地配置→安全性→加密→ Cognos
    b. 更改"`使用第三方CA？`" 设置为True。
    c. 保存配置。
    d. 重新启动Cognos
12. 使用管理CMD提示符将最新的Cognos证书导出到Cognos.crt：
    a. "D：\Program Files\SANscreen\java\bin\keytool.exe"-exportcert -file "`c：\temp\Cognos.crt`-keystore D

：\Program Files\SANscreen\cognos\Analytics \configuration\certs\CamKeystore"-storetype PKCS12 -storepass NoPassWordalias -encryption

13. 使用管理CMD提示符窗口将"`c：\temp\cognos.crt`"导入到dwh trustore中、以在Cognos和DWH之间建立SSL通信。
    a. "D：\Program Files\SANscreen\java\bin\keytool.exe"-importcert -file “c：\temp\Cognos.crt”-keystore "D：\Program Files\SANscreen\wildfly\standalone\configuration\server.trustore"-storepchangeit -alias cognoscert
14. 重新启动SANscreen 服务。
15. 执行DWH备份以确保DWH与Cognos通信。

导入Cognos和DWH的CA签名SSL证书(Insight 7.3.10及更高版本)

您可以添加SSL证书、以便为数据仓库和Cognos环境启用增强型身份验证和加密。

开始之前

此操作步骤 适用于运行OnCommand Insight 7.3.10及更高版本的系统。

> 有关最新的CAC和证书说明、请参见以下知识库文章(需要支持登录)：
>
> - "如何为OnCommand Insight 配置通用访问卡(CAC)身份验证"
> - "如何为OnCommand Insight 数据仓库配置通用访问卡(CAC)身份验证"
> - "如何创建证书颁发机构(CA)签名证书并将其导入到OnComand Insight和OnCommand Insight 数据仓库7.3.x中"
> - "如何在Windows主机上安装的OnCommand Insight 7.3.X中创建自签名证书"
> - "如何将Cognos证书颁发机构(CA)签名证书导入到OnCommand 数据中心7.3.3及更高版本中"

关于此任务

要执行此操作步骤 、您必须具有管理员权限。

步骤

1. 使用IBM Cognos配置工具停止Cognos。关闭Cognos。
2. 创建的备份 `..\SANScreen\cognos\analytics\configuration` 和 `..\SANScreen\cognos\analytics\temp\cam\freshness` 文件夹。
3. 从Cognos生成证书加密请求。在管理CMD窗口中、运行：
    a. CD “`\Program Files\sanscreen\cognos\analytics\bin`”
    b. `ThirdPartyCertificateTool.bat -java:local -c -e -p NoPassWordSet -a RSA -r c:\temp\encryptRequest.csr -d “CN=server.domain.com,O=NETAPP,C=US” -H “server.domain.com” -I “ipaddress”`。注意：此处的-H和-i将添加subjectAltNames、例如DNS和ipaddress。
4. 打开 `c:\temp\encryptRequest.csr` 归档并复制生成的内容。

5. 输入encryptRequest.csr内容并使用CA签名门户生成证书。
6. 使用PKCS7格式包含根证书以下载链证书

   此操作将下载FQDN.p7b文件

7. 从CA获取.p7b格式的证书。请使用一个名称将其标记为Cognos Web服务器的证书。
8. ThirdPartyCertificateTool.bat无法导入整个链、因此导出所有证书需要执行多个步骤。按如下所示单独导出链、从而拆分链：
   a. 在"`Crypto Shell扩展名`"中打开.p7b证书。
   b. 在左窗格中浏览到"`Certificates`"。
   c. 右键单击根CA >所有任务>导出。
   d. 选择Base64输出。
   e. 输入一个文件名、将其标识为根证书。
   f. 重复步骤8a到8e、将所有证书单独导出到.cer文件中。
   g. 将文件命名为intermediateX.cer和Cognos.cer。
9. 如果只有一个CA证书、请忽略此步骤、否则、请将root.cer和intermediateX.cer合并到一个文件中。
   a. 使用Notepad打开root.cer并复制内容。
   b. 使用Notepad打开intermediate.cer、然后附加9a中的内容(中间优先、根下一个)。
   c. 将文件另存为chain.cer。
10. 使用管理CMD提示符将证书导入到Cognos密钥库中：
    a. cd “Program Files\SANscreen\cognos\Analytics \bin”
    b. ThirdPartyCertificateTool.bat -java：local -i -T -r c：\temp\root.cer
    c. ThirdPartyCertificateTool.bat -java：local -i -T -r c：\temp\intermediate.cer
    d. ThirdPartyCertificateTool.bat -java：local -i -e -r c：\temp\cognos.cer -t c：\temp\chain.cer
11. 打开IBM Cognos配置。
    a. 选择本地配置→安全性→加密→ Cognos
    b. 更改"`使用第三方CA？`" 设置为True。
    c. 保存配置。
    d. 重新启动Cognos
12. 使用管理CMD提示符将最新的Cognos证书导出到Cognos.crt：
    a. CD "`C：\Program Files\SANscreen"
    b. java.bin\keytool.exe -exportcert -file c：\temp\cognos.crt -keystore Cognos\Analytics \configuration\certs\CamKeystore -storetype PKCS12 -storepass NoPassWordSet -alias encryption
13. 备份DWH服务器数据存储库`..\SANscreen\wildfly\standalone\configuration\server.trustore`
14. 使用管理CMD提示符窗口将"`c：\temp\cognos.crt`"导入到DWH存储中、以便在Cognos和DWH之间建立SSL通信。

a. CD "`C：\Program Files\SANscreen"

b. java.bin\keytool.exe -importcert -file c：\temp\cognos.crt -keystore wildfly\standalone\configuration\server.trusstore -storepass changeit -alias cognos3rdca

15. 重新启动SANscreen 服务。

16. 执行DWH备份以确保DWH与Cognos通信。

17. 即使仅更改了`sSL证书`且默认Cognos证书保持不变、也应执行以下步骤。否则、Cognos可能会抱怨新的SANscreen 证书或无法创建DWH备份。

    a. `cd "%SANSCREEN_HOME%cognos\analytics\bin\"`

    b. `"%SANSCREEN_HOME%java64\bin\keytool.exe" -exportcert -file "c:\temp\sanscreen.cer" -keystore "%SANSCREEN_HOME%wildfly\standalone\configuration\server.keystore" -storepass changeit -alias "ssl certificate"`

    c. `ThirdPartyCertificateTool.bat -java:local -i -T -r "c:\temp\sanscreen.cer"`

    通常、这些步骤会在中所述的Cognos证书导入过程中执行 "如何将Cognos证书颁发机构(CA)签名证书导入到OnCommand 数据中心7.3.3及更高版本中"

为智能卡和证书登录配置数据仓库

您必须修改OnCommand Insight 数据仓库配置以支持智能卡(CAC)和证书登录。

开始之前

- 必须在系统上启用LDAP。
- LDAP `User principal account name` 属性必须与包含用户的政府ID编号的LDAP字段匹配。

  政府颁发的CAC上存储的公用名(Common Name、CN)通常采用以下格式： `first.last.ID`。对于某些LDAP字段、例如 `sAMAccountName`、此格式太长。对于这些字段、OnCommand Insight 仅从CN中提取ID编号。

> 有关最新的CAC和证书说明、请参见以下知识库文章(需要支持登录)：
>
> - "如何为OnCommand Insight 配置通用访问卡(CAC)身份验证"
> - "如何为OnCommand Insight 数据仓库配置通用访问卡(CAC)身份验证"
> - "如何创建证书颁发机构(CA)签名证书并将其导入到OnComand Insight和OnCommand Insight 数据仓库7.3.x中"
> - "如何在Windows主机上安装的OnCommand Insight 7.3.X中创建自签名证书"
> - "如何将Cognos证书颁发机构(CA)签名证书导入到OnCommand 数据中心7.3.3及更高版本中"

步骤

1. 使用regedit修改中的注册表值 `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun2.0\SANscreen Server\Parameters\Java`

a. 更改JVM_Option `-DclientAuth=false` to `-DclientAuth=true`。

对于Linux、修改 `clientAuth` 参数 `/opt/netapp/oci/scripts/wildfly.server`

2. 将证书颁发机构(CA)添加到数据仓库存储库：

   a. 在命令窗口中、转至 `..\SANscreen\wildfly\standalone\configuration`。

   b. 使用 `keytool` 用于列出受信任CA的实用程序： `C:\Program Files\SANscreen\java64\bin\keytool.exe -list -keystore server.trustore -storepass changeit`

      每行中的第一个词表示CA别名。

   c. 如有必要、请提供CA证书文件、通常为 `.pem` 文件要将客户的CA加入到数据仓库受信任的CA中、请转至 `..\SANscreen\wildfly\standalone\configuration` 并使用 `keytool` 导入命令： `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore server.trustore -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

      my_alias通常是一个可轻松在中标识CA的别名`keytool -list` 操作。

3. 在OnCommand Insight 服务器上、 `wildfly/standalone/configuration/standalone-full.xml` 需要通过在中将verify-client更新为"已请求"来修改文件 `/subsystem=undertow/server=default-server/https-listener=default-https`以启用CAC。登录到Insight服务器并运行相应的命令：

os	脚本
Windows	<install dir>\SANscreen\wildfly\bin\enableCACforRemoteEJB.bat
Linux	/opt/netapp/oci/wildfly/bin/enableCACforRemoteEJB.sh

   执行此脚本后、请等待此wildfly服务器的重新加载完成、然后再继续执行下一步。

4. 重新启动OnCommand Insight 服务器。

为智能卡和证书登录配置Cognos (OnCommand Insight 7.3.5至7.3.9)

您必须修改OnCommand Insight 数据仓库配置、以支持Cognos服务器的智能卡(CAC)和证书登录。

开始之前

此操作步骤 适用于运行OnCommand Insight 7.3.5至7.3.3的系统。

有关最新的CAC和证书说明、请参见以下知识库文章(需要支持登录)：

- "如何为OnCommand Insight 配置通用访问卡(CAC)身份验证"
- "如何为OnCommand Insight 数据仓库配置通用访问卡(CAC)身份验证"
- "如何创建证书颁发机构(CA)签名证书并将其导入到OnComand Insight和OnCommand Insight 数据仓库7.3.x中"
- "如何在Windows主机上安装的OnCommand Insight 7.3.X中创建自签名证书"
- "如何将Cognos证书颁发机构(CA)签名证书导入到OnCommand 数据中心7.3.3及更高版本中"

步骤

1. 将证书颁发机构(CA)添加到Cognos truestore。
   a. 在命令窗口中、转至 `..\SANscreen\cognos\analytics\configuration\certs\`
   b. 使用 `keytool` 用于列出受信任CA的实用程序： `..\..\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass NoPassWordSet`

      每行中的第一个词表示CA别名。

   c. 如果不存在合适的文件、请提供CA证书文件、通常为 `.pem` 文件
   d. 要将客户的CA与OnCommand Insight 可信CA结合使用、请转至 `..\SANscreen\cognos\analytics\configuration\certs\`。
   e. 使用 `keytool` 用于导入的实用程序 `.pem` 文件： `..\..\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

      `my_alias` 通常是一个可在中轻松标识CA的别名`keytool -list` 操作。

   f. 当系统提示您输入密码时、输入 `NoPassWordSet`。
   g. 问题解答 `yes` 当系统提示您信任此证书时。
2. 要启用CAC模式、请执行 `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`
3. 要禁用CAC模式、请执行 `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`

为智能卡和证书登录配置Cognos (OnCommand Insight 7.3.10及更高版本)

您必须修改OnCommand Insight 数据仓库配置、以支持Cognos服务器的智能卡(CAC)和证书登录。

开始之前

此操作步骤 适用于运行OnCommand Insight 7.3.10及更高版本的系统。

有关最新的CAC和证书说明、请参见以下知识库文章(需要支持登录)：

- "如何为OnCommand Insight 配置通用访问卡(CAC)身份验证"
- "如何为OnCommand Insight 数据仓库配置通用访问卡(CAC)身份验证"
- "如何创建证书颁发机构(CA)签名证书并将其导入到OnComand Insight和OnCommand Insight 数据仓库7.3.x中"
- "如何在Windows主机上安装的OnCommand Insight 7.3.X中创建自签名证书"
- "如何将Cognos证书颁发机构(CA)签名证书导入到OnCommand 数据中心7.3.3及更高版本中"

步骤

1. 将证书颁发机构(CA)添加到Cognos truestore。
   a. 在命令窗口中、转至 `..\SANscreen\cognos\analytics\configuration\certs\`
   b. 使用 `keytool` 用于列出受信任CA的实用程序： `..\..\ibm-jre\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass NoPassWordSet`

      每行中的第一个词表示CA别名。

   c. 如果不存在合适的文件、请提供CA证书文件、通常为 `.pem` 文件
   d. 要将客户的CA与OnCommand Insight 可信CA结合使用、请转至 `..\SANscreen\cognos\analytics\configuration\certs\`。
   e. 使用 `keytool` 用于导入的实用程序 `.pem` 文件： `..\..\ibm-jre\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

      `my_alias` 通常是一个可在中轻松标识CA的别名`keytool -list` 操作。

   f. 当系统提示您输入密码时、输入 `NoPassWordSet`。
   g. 问题解答 `yes` 当系统提示您信任此证书时。
2. 要启用CAC模式、请执行以下操作：
   a. 使用以下步骤配置CAC注销页面：
      - 登录到Cognos门户(用户必须属于系统管理员组、例如Cognos_admin)
      - (仅适用于7.3.10和7.3.11)单击"管理"→"配置"→"系统"→"安全性"
      - (仅适用于7.3.10和7.3.11)针对注销重定向URL <→应用输入cacLogout.html
      - 关闭浏览器。
   b. 执行 `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`
   c. 启动IBM Cognos服务。等待Cognos服务启动。
3. 要禁用CAC模式、请执行以下操作：
   a. 执行 `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`
   b. 启动IBM Cognos服务。等待Cognos服务启动。

c. (仅适用于7.3.10和7.3.11)使用以下步骤取消配置CAC注销页面：
   - 登录到Cognos门户(用户必须属于系统管理员组、例如Cognos_admin)
   - 单击"管理"→"配置"→"系统"→"安全性"
   - 在注销重定向URL <→应用中输入cacLogout.html
   - 关闭浏览器。

导入Cognos和DWH的CA签名SSL证书(Insight 7.3.5至7.3.9)

您可以添加SSL证书、以便为数据仓库和Cognos环境启用增强型身份验证和加密。

开始之前

此操作步骤 适用于运行OnCommnand Insight 7.3.5至7.3.9的系统。

> 有关最新的CAC和证书说明、请参见以下知识库文章(需要支持登录)：
>
> - "如何为OnCommand Insight 配置通用访问卡(CAC)身份验证"
> - "如何为OnCommand Insight 数据仓库配置通用访问卡(CAC)身份验证"
> - "如何创建证书颁发机构(CA)签名证书并将其导入到OnComand Insight和OnCommand Insight 数据仓库7.3.x中"
> - "如何在Windows主机上安装的OnCommand Insight 7.3.X中创建自签名证书"
> - "如何将Cognos证书颁发机构(CA)签名证书导入到OnCommand 数据中心7.3.3及更高版本中"

关于此任务

要执行此操作步骤 、您必须具有管理员权限。

步骤

1. 创建的备份 `..\SANScreen\cognos\analytics\configuration\cogstartup.xml`。
2. 在下创建"`certs`"和"`csk`"文件夹的备份 `..\ SANScreen\cognos\analytics\configuration`。
3. 从Cognos生成证书加密请求。在管理CMD窗口中、运行：
   a. CD “`\Program Files\sanscreen\cognos\analytics\bin`”
   b. `ThirdPartyCertificateTool.bat -java:local -c -e -p NoPassWordSet -a RSA -d “CN=FQDN,O=orgname,C=US” -r c:\temp\encryptRequest.csr`
4. 打开 `c:\temp\encryptRequest.csr` 归档并复制生成的内容。
5. 将encryptRequest.csr发送到证书颁发机构(CA)以获取SSL证书。

   请务必添加其他属性、例如"`San：dns=fqdn "(例如、hostname.netapp.com)`")以添加SubjectAltName。如果证书中缺少SubjectAltName、则Google Chrome 58及更高版本会进行投诉。

6. 使用PKCS7格式包含根证书以下载链证书

此操作将下载FQDN.p7b文件

7. 从CA获取.p7b格式的证书。请使用一个名称将其标记为Cognos Web服务器的证书。
8. ThirdPartyCertificateTool.bat无法导入整个链、因此导出所有证书需要执行多个步骤。按如下所示单独导出链、从而拆分链：
   a. 在"`Crypto Shell扩展名`"中打开.p7b证书。
   b. 在左窗格中浏览到"`Certificates`"。
   c. 右键单击根CA >所有任务>导出。
   d. 选择Base64输出。
   e. 输入一个文件名、将其标识为根证书。
   f. 重复步骤8a到8c、将所有证书单独导出到.cer文件中。
   g. 将文件命名为intermediateX.cer和Cognos.cer。
9. 如果只有一个CA证书、请忽略此步骤、否则、请将root.cer和intermediateX.cer合并到一个文件中。
   a. 使用Notepad打开intermediate.cer并复制内容。
   b. 使用Notepad打开root.cer并保存9a中的内容。
   c. 将文件保存为CA.cer。
10. 使用管理CMD提示符将证书导入到Cognos密钥库中：
    a. cd “Program Files\SANscreen\cognos\Analytics \bin”
    b. ThirdPartyCertificateTool.bat -java：local -i -T -r c：\temp\cA.cer

       此操作会将CA.cer设置为根证书颁发机构。

    c. ThirdPartyCertificateTool.bat -java：local -i -e -r c：\temp\cognos.cer -t c：\temp\ca.cer

       此操作会将Cognos.cer设置为由CA.cer签名的加密证书。

11. 打开IBM Cognos配置。
    a. 选择本地配置→安全性→加密→ Cognos
    b. 更改"`使用第三方CA？`" 设置为True。
    c. 保存配置。
    d. 重新启动Cognos
12. 使用管理CMD提示符将最新的Cognos证书导出到Cognos.crt：
    a. "D：\Program Files\SANscreen\java\bin\keytool.exe"-exportcert -file "`c：\temp\Cognos.crt`-keystore D：\Program Files\SANscreen\cognos\Analytics \configuration\certs\CamKeystore"-storetype PKCS12 -storepass NoPassWordalias -encryption
13. 使用管理CMD提示符窗口将"`c：\temp\cognos.crt`"导入到dwh trustore中、以在Cognos和DWH之间建立SSL通信。
    a. "D：\Program Files\SANscreen\java\bin\keytool.exe"-importcert -file “c：\temp\Cognos.crt”-keystore "D：\Program Files\SANscreen\wildfly\standalone\configuration\server.trustore"-storepchangeit -alias cognoscert

14. 重新启动SANscreen 服务。
15. 执行DWH备份以确保DWH与Cognos通信。

导入Cognos和DWH的CA签名SSL证书(Insight 7.3.10及更高版本)

您可以添加SSL证书、以便为数据仓库和Cognos环境启用增强型身份验证和加密。

开始之前

此操作步骤 适用于运行OnCommand Insight 7.3.10及更高版本的系统。

> 有关最新的CAC和证书说明、请参见以下知识库文章(需要支持登录)：
>
> - "如何为OnCommand Insight 配置通用访问卡(CAC)身份验证"
> - "如何为OnCommand Insight 数据仓库配置通用访问卡(CAC)身份验证"
> - "如何创建证书颁发机构(CA)签名证书并将其导入到OnComand Insight和OnCommand Insight 数据仓库7.3.x中"
> - "如何在Windows主机上安装的OnCommand Insight 7.3.X中创建自签名证书"
> - "如何将Cognos证书颁发机构(CA)签名证书导入到OnCommand 数据中心7.3.3及更高版本中"

关于此任务

要执行此操作步骤 、您必须具有管理员权限。

步骤

1. 使用IBM Cognos配置工具停止Cognos。关闭Cognos。
2. 创建的备份 `..\SANScreen\cognos\analytics\configuration` 和 `..\SANScreen\cognos\analytics\temp\cam\freshness` 文件夹。
3. 从Cognos生成证书加密请求。在管理CMD窗口中、运行：
   a. CD “`\Program Files\sanscreen\cognos\analytics\bin`”
   b. `ThirdPartyCertificateTool.bat -java:local -c -e -p NoPassWordSet -a RSA -r c:\temp\encryptRequest.csr -d “CN=server.domain.com,O=NETAPP,C=US” -H “server.domain.com” -I “ipaddress”`。注意：此处的-H和-i将添加subjectAltNames、例如DNS和ipaddress。
4. 打开 `c:\temp\encryptRequest.csr` 归档并复制生成的内容。
5. 输入encryptRequest.csr内容并使用CA签名门户生成证书。
6. 使用PKCS7格式包含根证书以下载链证书

   此操作将下载FQDN.p7b文件

7. 从CA获取.p7b格式的证书。请使用一个名称将其标记为Cognos Web服务器的证书。

8. ThirdPartyCertificateTool.bat无法导入整个链、因此导出所有证书需要执行多个步骤。按如下所示单独导出链、从而拆分链：
   a. 在"`Crypto Shell扩展名`"中打开.p7b证书。
   b. 在左窗格中浏览到"`Certificates`"。
   c. 右键单击根CA >所有任务>导出。
   d. 选择Base64输出。
   e. 输入一个文件名、将其标识为根证书。
   f. 重复步骤8a到8e、将所有证书单独导出到.cer文件中。
   g. 将文件命名为intermediateX.cer和Cognos.cer。
9. 如果只有一个CA证书、请忽略此步骤、否则、请将root.cer和intermediateX.cer合并到一个文件中。
   a. 使用Notepad打开root.cer并复制内容。
   b. 使用Notepad打开intermediate.cer、然后附加9a中的内容(中间优先、根下一个)。
   c. 将文件另存为chain.cer。
10. 使用管理CMD提示符将证书导入到Cognos密钥库中：
    a. cd “Program Files\SANscreen\cognos\Analytics \bin”
    b. ThirdPartyCertificateTool.bat -java：local -i -T -r c：\temp\root.cer
    c. ThirdPartyCertificateTool.bat -java：local -i -T -r c：\temp\intermediate.cer
    d. ThirdPartyCertificateTool.bat -java：local -i -e -r c：\temp\cognos.cer -t c：\temp\chain.cer
11. 打开IBM Cognos配置。
    a. 选择本地配置→安全性→加密→ Cognos
    b. 更改"`使用第三方CA？`" 设置为True。
    c. 保存配置。
    d. 重新启动Cognos
12. 使用管理CMD提示符将最新的Cognos证书导出到Cognos.crt：
    a. CD "`C：\Program Files\SANscreen"
    b. java.bin\keytool.exe -exportcert -file c：\temp\cognos.crt -keystore Cognos\Analytics \configuration\certs\CamKeystore -storetype PKCS12 -storepass NoPassWordSet -alias encryption
13. 备份DWH服务器数据存储库`..\SANscreen\wildfly\standalone\configuration\server.trustore`
14. 使用管理CMD提示符窗口将"`c：\temp\cognos.crt`"导入到DWH存储中、以便在Cognos和DWH之间建立SSL通信。
    a. CD "`C：\Program Files\SANscreen"
    b. java.bin\keytool.exe -importcert -file c：\temp\cognos.crt -keystore wildfly\standalone\configuration\server.trusstore -storepass changeit -alias cognos3rdca
15. 重新启动SANscreen 服务。
16. 执行DWH备份以确保DWH与Cognos通信。

17. 即使仅更改了`sSL证书`且默认Cognos证书保持不变、也应执行以下步骤。否则、Cognos可能会抱怨新的SANscreen 证书或无法创建DWH备份。

    a. `cd “%SANSCREEN_HOME%cognos\analytics\bin\”`

    b. `“%SANSCREEN_HOME%java64\bin\keytool.exe” -exportcert -file “c:\temp\sanscreen.cer” -keystore “%SANSCREEN_HOME%wildfly\standalone\configuration\server.keystore” -storepass changeit -alias “ssl certificate”`

    c. `ThirdPartyCertificateTool.bat -java:local -i -T -r “c:\temp\sanscreen.cer”`

    通常、这些步骤会在中所述的Cognos证书导入过程中执行 "如何将Cognos证书颁发机构(CA)签名证书导入到OnCommand 数据中心7.3.3及更高版本中"

导入SSL证书

您可以添加SSL证书以启用增强的身份验证和加密、从而增强OnCommand Insight 环境的安全性。

开始之前

您必须确保系统满足所需的最低位级别(1024位)。

关于此任务

> 在尝试执行此操作步骤 之前、您应备份现有的 `server.keystore` 文件、并为备份命名 `server.keystore.old`。损坏 `server.keystore` 文件可能会导致Insight服务器在重新启动后无法运行。如果创建备份、则可以在出现问题时还原到旧文件。

步骤

1. 创建原始密钥库文件的副本： `cp c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore.old`
2. 列出密钥库的内容： `C:\Program Files\SANscreen\java64\bin\keytool.exe -list -v -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore"`

    a. 当系统提示您输入密码时、输入 `changeit`。

    系统将显示密钥库的内容。密钥库中应至少有一个证书、 `"ssl certificate"`。

3. 删除 `"ssl certificate"`： `keytool -delete -alias "ssl certificate" -keystore c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
4. 生成新密钥： `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. 当系统提示您输入名字和姓氏时、请输入要使用的完全限定域名(FQDN)。

b. 提供有关您的组织和组织结构的以下信息：

- 国家/地区：您所在国家/地区的双字母ISO缩写(例如、US)
- 州或省：您的组织总部所在州或省的名称(例如、马萨诸塞州)
- Locality：您的组织总部所在城市的名称(例如、沃尔瑟姆)
- 组织名称：拥有域名的组织的名称(例如、NetApp)
- 组织单位名称：要使用证书的部门或组的名称(例如、支持)
- 域名/公用名：用于服务器DNS查找的FQDN (例如www.example.com)系统将使用类似于以下内容的信息进行响应： `Is CN=www.example.com, OU=support, O=NetApp, L=Waltham, ST=MA, C=US correct?`

c. 输入 ... `Yes` 公用名(Common Name、CN)等于FQDN时。

d. 当系统提示您输入密钥密码时、输入密码或按Enter键以使用现有密钥库密码。

5. 生成证书请求文件： `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` file是新生成的证书请求文件。

6. 提交 `c:\localhost.csr` 将文件提交给证书颁发机构(CA)进行审批。

   证书请求文件获得批准后、您希望证书在中返回给您 `.der` 格式。此文件可能会以返回、也可能不会以返回 `.der` 文件默认文件格式为 `.cer` 适用于Microsoft CA服务。

   大多数组织的CA都使用一系列信任模式、包括通常处于脱机状态的根CA。它仅为少数子CA (称为中间CA)的证书签名。

   您必须获取整个信任链的公共密钥(证书)—为OnCommand Insight 服务器签署证书的CA的证书、以及该签名CA与组织根CA之间的所有证书。

   在某些组织中、当您提交签名请求时、可能会收到以下消息之一：

   - 一个PKCS12文件、其中包含您的签名证书以及信任链中的所有公共证书
   - 答 `.zip` 包含各个文件(包括您的签名证书)以及信任链中的所有公共证书的文件
   - 仅限您的签名证书

     您必须获取公共证书。

7. 导入已批准的server.keystore证书： `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. 出现提示时、输入密钥库密码。

      此时将显示以下消息： `Certificate reply was installed in keystore`

8. 导入已批准的server.trustore证书： `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. 出现提示时、输入truestore密码。

   此时将显示以下消息： `Certificate reply was installed in trustore`

9. 编辑 `SANscreen\wildfly\standalone\configuration\standalone-full.xml` 文件：

   替换以下别名字符串： `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. 重新启动SANscreen 服务器服务。

    运行Insight后、您可以单击挂锁图标以查看系统上安装的证书。

    如果您看到包含与"颁发者"信息匹配的"颁发给"信息的证书、则仍会安装自签名证书。Insight安装程序生成的自签名证书的有效期为100年。

    NetApp无法保证此操作步骤 将删除数字证书警告。NetApp无法控制最终用户工作站的配置方式。请考虑以下情形：

    - Microsoft Internet Explorer和Google Chrome均在Windows上使用Microsoft本机证书功能。

      这意味着、如果Active Directory管理员将组织的CA证书推送到最终用户的证书存储库中、则当OnCommand Insight 自签名证书被替换为内部CA基础架构签名的证书时、这些浏览器的用户将看到证书警告消失。

    - Java和Mozilla Firefox具有各自的证书存储。

      如果系统管理员不自动将CA证书传入这些应用程序的受信任证书存储、则使用Firefox浏览器可能会由于证书不受信任而继续生成证书警告、即使已替换自签名证书也是如此。将您的组织的证书链安装到数据存储库中是另一项要求。

为Insight数据库设置每周备份

您可能希望为Insight数据库设置每周自动备份、以保护您的数据。这些自动备份会覆盖指定备份目录中的文件。

关于此任务

最佳实践：设置OCI数据库的每周备份时、如果服务器发生故障、您需要将备份存储在Insight使用的其他服务器上。请勿将任何手动备份存储在每周备份目录中、因为每个每周备份都会覆盖目录中的文件。

备份文件将包含以下内容：

- 清单数据

- 最多7天的性能数据

步骤

1. 在Insight工具栏上、单击*管理*>*设置*。
2. 单击*备份和归档*选项卡。
3. 在每周备份部分中、选择*启用每周备份*。
4. 输入*备份位置*的路径。此选项可以位于本地Insight服务器上的上、也可以位于可从Insight服务器访问的远程服务器上。

> 备份位置设置包含在备份本身中、因此、如果您在另一个系统上还原备份、请注意备份文件夹位置在新系统上可能无效。还原备份后、请仔细检查备份位置设置。

5. 选择*清理*选项以保留最后两个或最后五个备份。
6. 单击 * 保存 * 。

结果

您也可以转到*管理*>*故障排除*来创建按需备份。

备份中包含的内容

每周备份和按需备份可用于故障排除或迁移。

每周备份或按需备份包括以下内容：

- 清单数据
- 性能数据(如果选择包含在备份中)
- 数据源和数据源设置
- 集成软件包
- 远程采集单元
- ASUP/代理设置
- 备份位置设置
- 归档位置设置
- 通知设置
- 用户
- 性能策略
- 业务实体和应用程序
- 设备解析规则和设置
- 信息板和小工具
- 自定义资产页面信息板和小工具

- 查询
- 标注和标注规则

每周备份不包括：

- 安全工具设置/存储信息(通过单独的命令行界面过程进行备份)
- 日志(可按需保存到.zip文件中)
- 性能数据(如果未选择包含在备份中)
- licenses

> 如果选择在备份中包含性能数据、则会备份最近七天的数据。如果启用了此功能、则其余数据将保存在归档中。

性能数据归档

OnCommand Insight 7.3引入了每天归档性能数据的功能。这是对配置和有限性能数据备份的补充。

OnCommand Insight 可保留长达90天的性能和违规数据。但是、在为该数据创建备份时、备份中仅包含最新信息。通过归档、您可以保存其余性能数据、并根据需要加载这些数据。

配置归档位置并激活归档后、Insight将每天将所有对象的前一天性能数据归档到归档位置。每天的归档将保存在归档文件夹中的一个单独文件中。归档会在后台进行、只要Insight正在运行、它就会继续进行。

保留最近90天的归档；创建较新的归档文件时、会删除90天之前的归档文件。

启用性能归档

要启用性能数据归档、请执行以下步骤。

步骤

1. 在工具栏上、单击*管理*>*设置*。
2. 选择*备份和归档*选项卡。
3. 在性能归档部分中、确保选中了"*启用性能归档"。
4. 指定有效的归档位置。

   您不能在Insight安装文件夹下指定文件夹。

   最佳实践：不要为归档指定与Insight备份位置相同的文件夹。

5. 单击 * 保存 * 。

   归档过程在后台处理、不会干扰其他Insight活动。

正在加载性能归档

要加载性能数据归档、请执行以下步骤。

开始之前

在加载性能数据归档之前、您必须还原有效的每周备份或手动备份。

步骤

1. 在工具栏上、单击*管理*>*故障排除*。
2. 在还原部分的*加载性能归档*下、单击*加载*。

> 归档加载在后台处理。加载完整归档可能需要很长时间、因为每天的归档性能数据都会填充到Insight中。归档加载的状态将显示在此页面的归档部分中。

配置电子邮件

您必须将OnCommand Insight 配置为访问电子邮件系统、以便OnCommand Insight服务器可以使用您的电子邮件交付您订阅的报告、并将故障排除支持信息传输给NetApp技术支持。

电子邮件配置前提条件

在将OnCommand Insight 配置为访问电子邮件系统之前、您需要先发现主机名或IP地址以标识(SMTP或Exchange)邮件服务器并为OnCommand Insight 报告分配电子邮件帐户。

请您的电子邮件管理员为OnCommand Insight 创建一个电子邮件帐户。您需要以下信息：

- 用于标识组织使用的(SMTP或Exchange)邮件服务器的主机名或IP地址。您可以通过用于阅读电子邮件的应用程序找到此信息。例如、在Microsoft Outlook中、您可以通过查看帐户配置来查找服务器的名称：Tools - E-Mail accounts -查看或更改现有电子邮件帐户。
- OnCommand Insight 用于发送定期报告的电子邮件帐户的名称。此帐户必须是您组织中的有效电子邮件地址。(大多数邮件系统不会发送消息、除非这些消息是从有效用户发送的。) 如果电子邮件服务器需要用户名和密码才能发送邮件、请从系统管理员处获取此信息。

为**Insight**配置电子邮件

如果用户希望在其电子邮件帐户中接收Insight报告、则需要配置电子邮件服务器以启用此功能。

步骤

1. 在Insight工具栏上、单击*管理*并选择*通知*。
2. 向下滚动到页面的*电子邮件*部分。
3. 在*服务器*框中、输入组织中SMTP服务器的名称、该名称使用主机名或IP地址(_nnn.nnn.nnn.nnn_格式)进

行标识。

如果指定主机名、请确保可以通过DNS解析此名称。

4. 在*用户名*框中、输入您的用户名。
5. 在*密码*框中、输入用于访问电子邮件服务器的密码、只有当SMTP服务器受密码保护时才需要此密码。此密码与您用于登录到允许您阅读电子邮件的应用程序的密码相同。如果需要密码、您必须再次输入密码进行验证。
6. 在*发件人电子邮件*框中、输入将在所有OnCommand Insight 报告中标识为发件人的发件人电子邮件帐户。

   此帐户必须是您组织中的有效电子邮件帐户。

7. 在*电子邮件签名*框中、输入要在发送的每个电子邮件中插入的文本。
8. 在收件人框中、单击 +、输入电子邮件地址、然后单击*确定*。

   要编辑电子邮件地址、请选择该地址、然后单击 。要删除电子邮件地址、请选择该地址、然后单击 ✖。

9. 要向指定收件人发送测试电子邮件、请单击 ✔。
10. 单击 * 保存 * 。

配置SNMP通知

OnCommand Insight 支持针对配置和全局路径策略更改以及违规发出SNMP通知。例如、超过数据源阈值时会发送SNMP通知。

开始之前

必须已完成以下操作：

- 确定用于整合每种类型事件的陷阱的服务器的IP地址。

  要获取此信息、您可能需要咨询系统管理员。

- 确定指定计算机为每种类型的事件获取SNMP陷阱所使用的端口号。

  SNMP陷阱的默认端口为162。

- 编译站点上的MIB。

  专有MIB随安装软件一起提供、用于支持OnCommand Insight 陷阱。NetApp MIB与所有标准SNMP管理软件兼容、可在Insight服务器上的中找到 `<install dir>\SANscreen\MIBS\sanscreen.mib`。

步骤

1. 单击*管理*并选择*通知*。
2. 向下滚动到页面的* SNMP *部分。
3. 单击*操作*并选择*添加陷阱源*。

4. 在*添加SNMP陷阱收件人*对话框中、输入以下值：
   - * IP *

     OnCommand Insight 将SNMP陷阱消息发送到的IP地址。

   - * 端口 *

     OnCommand Insight 将SNMP陷阱消息发送到的端口号。

   - 社区字符串

     对于SNMP陷阱消息、请使用"`public`"。

5. 单击 * 保存 * 。

启用系统日志工具

您可以确定OnCommand Insight 违规和性能警报以及审核消息日志的位置、并激活日志记录过程。

开始之前

- 您必须具有用于存储系统日志的服务器的IP地址。
- 您必须知道与记录消息的程序类型对应的设施级别、例如LOCA1或用户。

关于此任务

系统日志包含以下类型的信息：

- 违规消息
- 性能警报
- 也可以选择审核日志消息

系统日志中使用以下单位：

- 利用率指标：百分比
- 流量指标：MB
- 流量速率：MB/秒

步骤

1. 在Insight工具栏上、单击*管理*并选择*通知*。
2. 向下滚动到页面的*系统日志*部分。
3. 选中*启用syslog*复选框。
4. 如果需要、请选中*发送审核*复选框。除了显示在Audit页面上之外、还会将新的审核日志消息发送到系统日志。请注意、现有审核日志消息不会发送到系统日志；只会发送新生成的日志消息。

5. 在*服务器*字段中、输入日志服务器的IP地址。

   您可以通过在服务器IP (例如server：port)末尾的冒号后面附加自定义端口来指定此端口。如果未指定端口、则使用默认系统日志端口514。

6. 在*设施*字段中、选择与记录消息的程序类型对应的设施级别。
7. 单击 * 保存 * 。

Insight系统日志内容

您可以在服务器上启用系统日志来收集Insight违规和性能警报消息、其中包括利用率和流量数据。

消息类型

Insight系统日志列出了三种类型的消息：

- SAN路径违规
- 常规违规
- 性能警报

提供的数据

违规说明包括相关元素、事件时间以及违规的相对严重性或优先级。

性能警报包括以下数据：

- 利用率百分比
- 流量类型
- 流量速率以MB为单位

配置性能并确保违规通知

OnCommand Insight 支持发出性能通知并确保违规。默认情况下、Insight不会针对这些违规发送通知；您必须将Insight配置为发送电子邮件、向系统日志服务器发送系统日志消息或在发生违规时发送SNMP通知。

开始之前

您必须已为违规配置电子邮件、系统日志和SNMP发送方法。

步骤

1. 单击*管理*>*通知*。
2. 单击*事件*。

3. 在*性能违规事件*或*确保违规事件*部分中、单击所需通知方法(电子邮件、系统日志*或 SNMP)的列表、然后选择违规的严重性级别(*警告及以上*或*严重)。
4. 单击 * 保存 * 。

配置系统级别的事件通知

OnCommand Insight 支持针对采集单元故障或数据源错误等系统级事件发出通知。要接收通知、您必须将Insight配置为在发生其中一个或多个事件时发送电子邮件。

开始之前

您必须已在*管理*>*通知*>*发送方法*中为接收通知配置了电子邮件收件人。

步骤

1. 单击*管理*>*通知*。
2. 单击*事件*。
3. 在*系统警报事件*电子邮件部分中、选择通知的严重性级别(警告及以上*或*严重)、或者如果您不希望接收系统级别事件的通知、则选择*不发送*。
4. 单击 * 保存 * 。
5. 单击*管理*>*系统警报*以自行配置警报。
6. 要添加新警报、请单击*+添加*并为警报提供唯一的*名称*。您也可以单击右侧图标*编辑*现有警报。
7. 选择要警报的*事件类型*、例如_Acquisition Unit failure_。
8. 选择*暂停*间隔可禁止在选定时间间隔内收到有关选定类型重复事件的通知。如果选择_never、则您将每分钟收到一次重复通知、直到事件不再发生为止。
9. 为事件通知选择*严重性*(警告或严重)。
10. 默认情况下、电子邮件通知将发送到全局电子邮件收件人列表、或者您也可以单击提供的链接以覆盖全局列表并向特定收件人发送通知。
11. 单击保存以添加警报。

配置ASUP处理

所有NetApp产品都配备了自动化功能、可为客户提供最佳支持。自动化支持(ASUP)会定期向客户支持发送预定义的特定信息。您可以控制要转发给NetApp的信息以及发送频率。

开始之前

您必须将OnCommand Insight 配置为在发送任何数据之前转发数据。

关于此任务

ASUP数据使用HTTPS协议进行转发。

步骤

1. 在Insight工具栏上、单击*管理*。
2. 单击*设置*。
3. 单击* ASUP & Proxe*选项卡。
4. 在* ASUP*部分中、选择*启用ASUP*以激活ASUP工具。
5. 如果要更改公司信息、请更新以下字段：
   - 公司名称
   - 站点名称
   - 发送内容：日志、配置数据、性能数据
6. 单击*测试连接*以确保您指定的连接正常工作。
7. 单击 * 保存 * 。
8. 在*代理*部分中、选择是否*启用代理*、并指定代理*主机*、*端口*和*用户*信息。
9. 单击*测试连接*以确保您指定的代理正常工作。
10. 单击 * 保存 * 。

AutoSupport (ASUP)软件包中包含的内容

AutoSupport 软件包包含数据库备份以及扩展信息。

AutoSupport 软件包包括以下内容：

- 清单数据
- 性能数据(如果选择包含在ASUP中)
- 数据源和数据源设置
- 集成软件包
- 远程采集单元
- ASUP/代理设置
- 备份位置设置
- 归档位置设置
- 通知设置
- 用户
- 性能策略
- 业务实体和应用程序
- 设备解析规则和设置
- 信息板和小工具
- 自定义资产页面信息板和小工具

- 查询
- 标注和标注规则
- 日志
- licenses
- 采集/数据源状态
- MySQL状态
- 系统信息

AutoSupport 软件包不包括：

- 安全工具设置/存储信息(通过单独的命令行界面过程进行备份)
- 性能数据(如果未选择包含在ASUP中)

> 如果选择在ASUP中包含性能数据、则会包括最近七天的数据。如果启用了此功能、则其余数据将保存在归档中。归档数据不包含在ASUP中。

定义应用程序

如果要跟踪与环境中运行的特定应用程序关联的数据、则需要定义这些应用程序。

开始之前

如果要将应用程序与业务实体关联、必须已创建业务实体。

关于此任务

您可以将应用程序与以下资产相关联：主机，虚拟机，卷，内部卷， qtree ， 共享和虚拟机管理程序。

步骤

1. 登录到OnCommand Insight Web UI。
2. 单击*管理*并选择*应用程序*。

   定义应用程序后、"应用程序"页面将显示应用程序的名称、优先级以及与应用程序关联的业务实体(如果适用)。

3. 单击 * 添加 * 。

   此时将显示添加应用程序对话框。

4. 在*名称*框中输入应用程序的唯一名称。
5. 单击*优先级*、然后为环境中的应用程序选择优先级(关键、高、中或低)。
6. 如果您计划将此应用程序与业务实体结合使用、请单击*业务实体*并从列表中选择实体。
7. 可选：如果不使用卷共享、请单击以清除*验证卷共享*框。

这需要Assure许可证。如果要确保每个主机都可以访问集群中的相同卷、请设置此选项。例如、高可用性集群中的主机通常需要屏蔽到相同的卷才能进行故障转移；但是、不相关应用程序中的主机通常不需要访问相同的物理卷。此外、出于安全原因、监管策略可能要求您明确禁止不相关的应用程序访问相同的物理卷。

8. 单击 * 保存 * 。

   应用程序将显示在"Applications"页面中。如果单击应用程序的名称、Insight将显示应用程序的资产页面。

完成后

定义应用程序后、您可以转到主机、虚拟机、卷、内部卷或虚拟机管理程序的资产页面、以便将应用程序分配给资产。

将应用程序分配给资产

在定义具有或不具有业务实体的应用程序后、您可以将这些应用程序与资产相关联。

步骤

1. 登录到OnCommand Insight Web UI。
2. 通过执行以下任一操作、找到要应用此应用程序的资产(主机、虚拟机、卷或内部卷)：
   - 单击*信息板*、选择*资产信息板*、然后单击资产。
   - 单击 在显示*搜索资产*框的工具栏上、键入资产的名称、然后从列表中选择资产。
3. 在资产页面的*用户数据*部分中、将光标置于当前分配给资产的应用程序的名称上方(如果未分配任何应用程序、则会显示*无*)、然后单击 (编辑应用程序)。

   此时将显示选定资产的可用应用程序列表。当前与此资产关联的应用程序前面带有一个复选标记。

4. 您可以在搜索框中键入以筛选应用程序名称、也可以向下滚动列表。
5. 选择要与资产关联的应用程序。

   您可以将多个应用程序分配给主机、虚拟机和内部卷；但是、您只能将一个应用程序分配给卷。

6. 单击 将选定应用程序分配给资产。

   应用程序名称显示在"User Data"部分中；如果应用程序与业务实体关联、则业务实体的名称也会显示在本部分中。

编辑应用程序

您可能希望更改应用程序的优先级、与应用程序关联的业务实体或卷共享的状态。

步骤

1. 登录到OnCommand Insight Web UI。
2. 单击*管理*并选择*应用程序*。

3. 将光标置于要编辑的应用程序上、然后单击 。

   此时将显示编辑应用程序对话框。

4. 执行以下任一操作：
   - 单击*优先级*并选择其他优先级。

     您不能更改应用程序的名称。

   - 单击*业务实体*并选择要与应用程序关联的其他业务实体、或者选择*无*以删除应用程序与业务实体的关联。
   - 单击以清除或选择*验证卷共享*。

     只有在拥有Assure许可证的情况下、此选项才可用。

5. 单击 * 保存 * 。

删除应用程序

如果某个应用程序不再满足您环境的需求、您可能需要将其删除。

步骤

1. 登录到Insight Web UI。
2. 单击*管理*并选择*应用程序*。
3. 将光标置于要删除的应用程序上、然后单击 。

   此时将显示一个确认对话框、询问您是否要删除此应用程序。

4. 单击 * 确定 * 。

业务实体层次结构

您可以定义业务实体、以便更精细地跟踪和报告环境数据。

在OnCommand Insight 中、业务实体层次结构包含以下级别：

- 服务提供商主要使用*租户*将资源与客户(例如NetApp)相关联。
- *业务部门(LOB)*是公司内的业务部门或产品线、例如数据存储。
- *业务单位*代表传统业务单位、例如法律或营销。
- *项目*通常用于标识业务单位中您希望进行容量成本分摊的特定项目。例如、"专利"可能是法律业务部门的项目名称、"销售活动"可能是营销业务部门的项目名称。请注意、级别名称可能包含空格。

您无需在设计企业层次结构时使用所有级别。

设计业务实体层次结构

您需要了解企业结构的要素以及业务实体中需要呈现的内容、因为它们会成为OnCommand Insight 数据库中的固定结构。您可以使用以下信息设置业务实体。请记住、您不需要使用所有层次结构级别来收集这些类别的数据。

步骤

1. 检查业务实体层次结构的每个级别、以确定是否应将该级别包括在贵公司的业务实体层次结构中：
   - 如果您的公司是ISP且您希望跟踪客户的资源使用情况、则需要*租户*级别。
   - 如果需要跟踪不同产品线的数据、则层次结构中需要*业务部门(LOB)*。
   - 如果需要跟踪不同部门的数据、则需要*业务单位*。此层次结构级别通常对于分离一个部门使用的资源非常有用、而其他部门则不使用。
   - *项目*级别可用于部门内的专业工作。与公司或部门的其他项目相比、此数据可能有助于确定、定义和监控单独项目的技术需求。
2. 创建一个图表、显示每个业务实体以及实体内所有级别的名称。
3. 检查层次结构中的名称、以确保它们在OnCommand Insight 视图和报告中是不言自明的。
4. 确定与每个业务实体关联的所有应用程序。

创建业务实体

在为公司设计业务实体层次结构后、您可以设置应用程序、然后将业务实体与应用程序相关联。此过程将在OnCommand Insight 数据库中创建业务实体结构。

关于此任务

将应用程序与业务实体关联是可选的；但是、这是最佳实践。

步骤

1. 登录到Insight Web UI。
2. 单击*管理*并选择*业务实体*。

   此时将显示"Business Entities"页面。

3. 单击 

开始构建新实体。

   此时将显示*添加业务实体*对话框。

4. 对于每个实体级别(租户、业务部门、业务单位和项目)、您可以执行以下任一操作：
   - 单击实体级别列表并选择一个值。
   - 键入新值并按Enter键。
   - 如果不想对业务实体使用实体级别、请将实体级别值保留为不适用。
5. 单击 * 保存 * 。

将业务实体分配给资产

您可以将业务实体分配给资产(主机、端口、存储、交换机、虚拟机、 qtree、共享、卷或内部卷)未将业务实体与应用程序关联；但是、如果业务实体与某个业务实体相关的应用程序关联、则会自动将该资产分配给该资产。

开始之前

您必须已创建业务实体。

关于此任务

虽然您可以将业务实体直接分配给资产、但建议您将应用程序分配给资产、然后将业务实体分配给资产。

步骤

1. 登录到OnCommand Insight Web UI。
2. 通过执行以下任一操作、找到要应用业务实体的资产：
   - 单击资产信息板中的资产。
   - 单击 在显示*搜索资产*框的工具栏上、键入资产的名称、然后从列表中选择资产。
3. 在资产页面的*用户数据*部分中、将光标置于*业务实体*旁边的*无*上、然后单击 。

   此时将显示可用业务实体的列表。
4. 在*搜索*框中键入以筛选列表中的特定实体、或者向下滚动列表；从列表中选择一个业务实体。

   如果您选择的业务实体与某个应用程序关联、则会显示应用程序名称。在这种情况下、业务实体名称旁边会显示`d已收到`。如果您只希望维护资产的实体、而不希望维护关联应用程序的实体、则可以手动覆盖应用程序的分配。
5. 要覆盖从业务实体派生的应用程序、请将光标置于应用程序名称上方、然后单击 、选择其他业务实体、然后从列表中选择其他应用程序。

将业务实体分配给多个资产或从多个资产中删除业务实体

您可以使用查询将业务实体分配给多个资产或从多个资产中删除业务实体、而无需手动分配或删除它们。

开始之前

您必须已创建要添加到所需资产的业务实体。

步骤

1. 创建新查询或打开现有查询。
2. 如果需要、请筛选要添加业务实体的资产。
3. 在列表中选择所需资产或单击 选择*全部*。

此时将显示*操作*按钮。

4. 要将业务实体添加到选定资产、请单击 Actions ▾ 。如果可以为选定资产类型分配业务实体、您将看到菜单选项*添加业务实体*。选择此项。
5. 从列表中选择所需的业务实体、然后单击*保存*。

   您分配的任何新业务实体将覆盖已分配给资产的任何业务实体。将应用程序分配给资产还会覆盖以相同方式分配的业务实体。将业务实体作为资产分配给也可能会覆盖分配给该资产的任何应用程序。

6. 要删除分配给资产的业务实体、请单击 Actions ▾ 并选择*删除业务实体*。
7. 从列表中选择所需的业务实体、然后单击*删除*。

定义标注

在自定义OnCommand Insight 以跟踪符合企业要求的数据时、您可以定义提供完整数据视图所需的任何专用标注：例如、资产使用寿命结束、数据中心、构建位置、存储层或卷、和内部卷服务级别。

步骤

1. 列出环境数据必须关联的任何行业术语。
2. 列出环境数据必须关联的企业术语、尚未使用业务实体对其进行跟踪。
3. 确定您可以使用的任何默认标注类型。
4. 确定需要创建哪些自定义标注。

使用标注监控您的环境

在自定义OnCommand Insight 以根据企业要求跟踪数据时、您可以定义称为_annotations_的 专用注释并将其分配给资产。例如、您可以使用资产生命周期结束、数据中心、构建位置、存储层或卷服务级别等信息为资产添加标注。

使用标注帮助监控您的环境包括以下高级任务：

- 为所有标注类型创建或编辑定义。
- 显示资产页面并将每个资产与一个或多个标注相关联。

  例如，如果某个资产正在租赁，并且租约在两个月内到期，则您可能需要对该资产应用寿命终结标注。这有助于防止他人长时间使用该资产。

- 创建规则以自动将标注应用于同一类型的多个资产。
- 使用标注导入实用程序导入标注。
- 按标注筛选资产。
- 根据标注对报告中的数据进行分组并生成这些报告。

有关OnCommand Insight 报告的详细信息、请参见_RAID报告指南。

管理标注类型

OnCommand Insight 提供了一些默认标注类型、例如资产生命周期(生日或生命周期结束)、建筑物或数据中心位置以及层、您可以自定义这些标注类型以显示在报告中。您可以为默认标注类型定义值、也可以创建自己的自定义标注类型。您可以稍后编辑这些值。

默认标注类型

OnCommandInsight提供了一些默认标注类型。这些标注可用于筛选或分组数据以及筛选数据报告。

您可以将资产与以下默认标注类型关联：

- 资产生命周期，例如，生日，日出或生命周期结束
- 有关设备的位置信息，例如数据中心，建筑物或楼层
- 按质量（层），已连接设备（交换机级别）或服务级别等对资产进行分类
- 状态，例如热（高利用率）

下表列出了默认标注类型。您可以根据需要编辑其中任何标注名称。

标注类型	Description	Type
别名	资源的用户友好名称。	文本
生日	设备已联机或将联机的日期。	Date
构建	主机、存储、交换机和磁带资源的物理位置。	列表
城市	主机、存储、交换机和磁带资源的市政位置。	列表
计算资源组	主机和VM文件系统数据源使用的组分配。	列表
大陆	主机、存储、交换机和磁带资源的地理位置。	列表
国家 / 地区	主机、存储、交换机和磁带资源的国家位置。	列表
数据中心	资源的物理位置、可用于主机、存储阵列、交换机和磁带。	列表

直连	指示(是或否)存储资源是否直接连接到主机。	布尔值
生命周期结束	设备脱机的日期、例如租约到期或硬件停用。	Date
网络结构别名	网络结构的用户友好名称。	文本
楼层	设备在建筑物楼层的位置。可以为主机、存储阵列、交换机和磁带设置。	列表
热	设备已定期频繁使用或已达到容量阈值。	布尔值
注意	要与资源关联的注释。	文本
机架	资源所在的机架。	文本
房间	主机、存储、交换机和磁带资源位于建筑物或其他位置的房间。	列表
SAN	网络的逻辑分区。适用于主机、存储阵列、磁带、交换机和应用程序。	列表
服务级别	一组可分配给资源的受支持服务级别。提供内部卷， qtree 和卷的有序选项列表。编辑服务级别以设置不同级别的性能策略。	列表
省/自治区/直辖市	资源所在的省/自治区/直辖市。	列表
《日出》	设置的阈值，超过此阈值后，无法为该设备进行新分配。适用于计划内迁移和其他待定网络更改。	Date
交换机级别	包括用于设置交换机类别的预定义选项。通常、这些指定值在设备生命周期内保持不变、但您可以根据需要对其进行编辑。仅适用于交换机。	列表

层	可用于定义环境中的不同服务级别。层可以定义级别的类型，例如所需的速度（例如金牌或银牌）。此功能仅适用于内部卷， qtree ，存储阵列，存储池和卷。	列表
违规严重性	在重要性从高到低的层次结构中对违规（例如，缺少主机端口或缺少冗余）进行排名（例如，重大）。	列表

别名、数据中心、热、服务级别、Sunset、 交换机级别、服务级别、层和违规严重性均为系统级别标注、您无法删除或重命名这些标注；您只能更改其分配的值。

如何分配标注

您可以手动分配标注、也可以使用标注规则自动分配标注。OnCommand Insight 还会在资产采集和继承时自动分配一些标注。分配给资产的任何标注都会显示在资产页面的User Data部分中。

标注的分配方式如下：

- 您可以手动为资产分配标注。

  如果标注直接分配给资产、则标注在资产页面上显示为普通文本。手动分配的标注始终优先于标注规则继承或分配的标注。

- 您可以创建一个标注规则、以便自动将标注分配给同一类型的资产。

  如果标注是按规则分配的、Insight会在资产页面上的标注名称旁边显示规则名称。

- Insight会自动将层级别与存储层模式关联起来、以便在采集资产时加快向资源分配存储标注的速度。

  某些存储资源会自动与预定义的层(第1层和第2层)关联。例如、Symmetrix存储层基于Symmetrix和VMAX系列、并与第1层关联。您可以根据层要求更改默认值。如果标注由Insight分配(例如、层)、则在将光标置于资产页面上标注名称上方时、您会看到`Ssystem-defined`。

- 少数资源(资产的子级)可以从其资产(父级)派生预定义的层标注。

  例如、如果为存储分配了标注、则层标注将由属于该存储的所有存储池、内部卷、卷、qtree和共享派生。如果对存储的内部卷应用了不同的标注、则标注随后会由所有卷、qtree和共享派生。资产页面上的标注名称旁边会显示`d已收到`。

将成本与标注相关联

在运行成本相关报告之前、您应将成本与服务级别、交换机级别和系统级别标注关联起来、以便根据存储用户的实际生产和复制容量使用情况向其进行成本分摊。例如、对于层级别、您可能具有黄金层和白银层值、并为黄金层分配比白银层更高的成本。

步骤

1. 登录到InsightWeb UI。
2. 单击Manage并选择*标注*。

   此时将显示"Annotation"页面。

3. 将光标置于服务级别、交换机级别或层标注上、然后单击 。

   此时将显示编辑标注对话框。

4. 在*成本*字段中输入任何现有级别的值。

   "层"和"服务级别"标注分别具有"自动层"和"对象存储"值、您无法删除这些值。

5. 单击 Add 以添加其他级别。
6. 完成后、单击*保存*。

创建自定义标注

通过标注，您可以将符合业务需求的自定义业务特定数据添加到资产中。虽然OnCommand Insight 提供了一组默认标注、但您可能会发现您希望以其他方式查看数据。自定义标注中的数据可补充已收集的设备数据，例如交换机制造商，端口数量和性能统计信息。Insight不会发现您使用标注添加的数据。

步骤

1. 登录到Insight Web UI。
2. 单击*管理*并选择*标注*。

   " 标注 " 页面将显示标注列表。

3. 单击 Add 。

   此时将显示*添加标注*对话框。

4. 在*名称*和*问题描述 *字段中输入名称和问题描述。

   您最多可以在这些字段中输入 255 个字符。

   > 以圆点""开头或结尾的标注名称。 不支持。

5. 单击 * 类型 * ，然后选择以下选项之一，以表示此标注中允许的数据类型：

   - 布尔值

     此时将创建一个下拉列表、其中包含yes和no选项例如、"`Direct attached`"标注为布尔值。

   - Date

此操作将创建一个包含日期的字段。例如，如果标注将是日期，请选择此项。

- 列表

  此操作可以创建以下任一项：

  - 固定下拉列表

    当其他用户在设备上分配此标注类型时，他们无法向列表中添加更多值。

  - 下拉灵活列表

    如果在创建此列表时选择*在实时*中添加新值*选项、则当其他用户在设备上分配此标注类型时、他们可以向列表中添加更多值。

- 数字

  这将创建一个字段、分配标注的用户可以在该字段中输入一个数字。例如、如果标注类型为"`Floor`"、则用户可以选择"`Number`"的值类型并输入楼层号。

- 文本

  此操作将创建一个允许自由格式文本的字段。例如、您可以输入"`Language`"作为标注类型、选择"`Text`"作为值类型、然后输入语言作为值。

> 设置类型并保存更改后，您将无法更改标注的类型。如果需要更改类型，则必须删除标注并创建一个新标注。

6. 如果选择"**List"*作为标注类型、请执行以下操作：
   a. 如果您希望在资产页面上为标注添加更多值，请选择 * 即时添加新值 * ，这样可以创建灵活列表。

      例如，假设您位于资产页面上，并且资产的 City 标注值为 Detroit ， TampA 和 Boston 。如果您选择了 * 实时添加新值 * 选项，则可以直接在资产页面上将其他值添加到 City ，例如旧金山和芝加哥，而无需转到标注页面进行添加。如果不选择此选项，则在应用标注时无法添加新标注值；这将创建一个固定列表。

   b. 在*值*和*问题描述 *字段中输入一个值和一个名称。
   c. 单击 ✚ Add 以添加其他值。
   d. 单击 🗑 删除值。
7. 单击 * 保存 * 。

   您的标注将显示在标注页面的列表中。

- 相关信息 *

"导入和导出用户数据"

手动为资产分配标注

为资产分配标注有助于您按照与业务相关的方式对资产进行排序，分组和报告。尽管您可以使用标注规则自动为特定类型的资产分配标注、但您可以使用资产页面为单个资产分配标注。

开始之前

您必须已创建要分配的标注。

步骤

1. 登录到OnCommand Insight Web UI。
2. 执行以下任一操作、找到要应用标注的资产：
   - 单击资产信息板中的资产。
   - 单击 在显示*搜索资产*框的工具栏上、键入资产的类型或名称、然后从显示的列表中选择资产。

     此时将显示资产页面。
3. 在资产页面的*用户数据*部分中、单击 Add 。

   此时将显示添加标注对话框。
4. 单击*标注*、然后从列表中选择一个标注。
5. 单击*值*、然后根据您选择的标注类型执行以下操作之一：
   - 如果标注类型为 list ， date 或 boolean ，请从列表中选择一个值。
   - 如果标注类型为文本，请键入一个值。
6. 单击 * 保存 * 。
7. 如果要在分配后更改标注的值、请单击 并选择其他值。

   如果标注的列表类型选择了*标注分配时动态添加值*选项、则除了选择现有值之外、您还可以键入以添加新值。

修改标注

您可能需要更改标注的名称、问题描述 或值、或者删除不再需要使用的标注。

步骤

1. 登录到OnCommand InsightWeb UI。
2. 单击*管理*并选择*标注*。

   此时将显示"Annotations"页面。
3. 将光标置于要编辑的标注上并单击 。

   此时将显示*编辑标注*对话框。

4. 您可以对标注进行以下修改：

   a. 更改名称、问题描述 或两者。

      但是、请注意、您可以为名称和问题描述 最多输入255个字符、并且不能更改任何标注的类型。此外、对于系统级标注、您不能更改名称或问题描述；但是、如果标注是列表类型、则可以添加或删除值。

      > 如果将自定义标注发布到数据仓库并对其进行重命名、则会丢失历史数据。

   a. 要向列表类型的标注添加另一个值、请单击 + Add 。
   b. 要从列表类型的标注中删除值、请单击 🗑 。

      如果某个标注值与标注规则、查询或性能策略中包含的标注关联、则不能删除该标注值。

5. 完成后、单击*保存*。

完成后

如果要在数据仓库中使用标注、则需要强制更新数据仓库中的标注。请参见_Data OnCommand Insight Warehouse管理指南_。

删除标注

您可能希望删除不再需要使用的标注。您不能删除系统级别的标注或在标注规则、查询或性能策略中使用的标注。

步骤

1. 登录到OnCommand Insight Web UI。
2. 单击*管理*并选择*标注*。

   此时将显示"Annotations"页面。

3. 将光标置于要删除的标注上、然后单击 🗑 。

   此时将显示确认对话框。

4. 单击 * 确定 * 。

使用标注规则为资产分配标注

要根据定义的条件自动为资产分配标注，请配置标注规则。OnCommand Insight 会根据这些规则为资产分配标注。Insight还提供了两个默认标注规则、您可以根据需要修改这些规则、如果不想使用这些规则、则可以将其删除。

默认存储标注规则

为了加快向资源分配存储标注的速度、OnCommand Insight 提供了21个默认标注规则、这些规则会将层级别与存储层模型相关联。在您的环境中获取资产后、您的所有存储资源都

会自动与某个层相关联。

默认标注规则按以下方式应用层标注：

- 第1层、存储质量层

  第1层标注适用于以下供应商及其指定系列：EMC (Symmetrix)、HDS (HDS9500V、HDS9900、HDS9900V、R600、 R700、USP r、USP V)、IBM (DS8000)、NetApp (FAS6000或FAS6200)和Violin (内存)。

- 第2层、存储质量层

  第2层标注适用于以下供应商及其指定系列：HP (3PAR StoreServ或EVA)、EMC (CLARiiON)、HDS (AMS或D800)、IBM (XIV)和NetApp (FAS3000、FAS3100和FAS3200)。

您可以根据层要求编辑这些规则的默认设置、也可以在不需要时将其删除。

正在创建标注规则

除了手动将标注应用于单个资产之外，您还可以使用标注规则自动将标注应用于多个资产。在 Insight 评估标注规则时，在单个资产页面上手动设置的标注优先于基于规则的标注。

开始之前

您必须已为标注规则创建查询。

关于此任务

虽然您可以在创建规则时编辑标注类型，但您应提前定义这些类型。

步骤

1. 登录到OnCommand Insight Web UI。
2. 单击*管理*并选择*标注规则*。

   " 标注规则 " 页面将显示现有标注规则的列表。

3. 单击 + Add 。

   此时将显示添加规则对话框。

4. 执行以下操作：
   a. 在 * 名称 * 框中，输入用于描述规则的唯一名称。

      此名称将显示在 "Annotation Rules" 页面中。

   b. 单击*查询*、然后选择OnCommand Insight 将标注应用于资产时应使用的查询。
   c. 单击 * 标注 * 并选择要应用的标注。

d. 单击 * 值 * 并为标注选择一个值。

   例如，如果选择 " 生日 " 作为标注，则可以为此值指定日期。

5. 单击 * 保存 * 。
6. 如果要立即运行所有规则，请单击 * 运行所有规则 * ；否则，这些规则将按计划的定期间隔运行。

设置标注规则优先级

默认情况下、OnCommand Insight 会按顺序评估标注规则；但是、如果您希望Insight按特定顺序评估规则、则可以配置OnCommand Insight 评估标注规则的顺序。

步骤

1. 登录到InsightWeb UI。
2. 单击*管理*并选择*标注规则*。

   " 标注规则 " 页面将显示现有标注规则的列表。

3. 将光标置于标注规则上。

   优先级箭头显示在规则的右侧。

4. 要在列表中上移或下移规则、请单击向上箭头或向下箭头。

   默认情况下、新规则会按顺序添加到规则列表中。在 Insight 评估标注规则时，在单个资产页面上手动设置的标注优先于基于规则的标注。

修改标注规则

您可以修改标注规则以更改规则的名称，标注，标注值或与规则关联的查询。

步骤

1. 登录到OnCommand InsightWeb UI。
2. 单击*管理*并选择*标注规则*。

   " 标注规则 " 页面将显示现有标注规则的列表。

3. 找到要修改的规则：
   - 在标注规则页面上、您可以通过在筛选器框中输入值来筛选标注规则。
   - 如果规则较多而无法在页面上显示、请单击页码以按页浏览标注规则。
4. 执行以下操作之一以显示*编辑规则*对话框：
   - 如果位于"Annotation Rules"页面上、请将光标置于标注规则上方、然后单击 。
   - 如果您位于资产页面上、请将光标置于与规则关联的标注上、将光标置于显示的规则名称上、然后单击规则名称。

5. 进行所需的更改并单击*保存*。

正在删除标注规则

如果不再需要某个标注规则来监控网络中的对象、则可以删除该规则。

步骤

1. 登录到OnCommand InsightWeb UI。
2. 单击*管理*、然后选择*标注规则*。

   " 标注规则 " 页面将显示现有标注规则的列表。

3. 找到要删除的规则：
   - 在标注规则页面上、您可以通过在筛选器框中输入值来筛选标注规则。
   - 如果规则数量超出单个页面的大小、请单击页码以按页浏览标注规则。
4. 将光标指向要删除的规则、然后单击 🗑 。

   此时将显示一条确认消息，提示您是否要删除此规则。

5. 单击 * 确定 * 。

正在导入标注值

如果在CSV文件中维护SAN对象(例如存储、主机和虚拟机)的标注、则可以将该信息导入到OnCommand Insight 中。您可以导入应用程序、业务实体或标注、例如层和建筑物。

关于此任务

以下规则适用：

- 如果标注值为空、则该标注将从对象中删除。
- 为卷或内部卷添加标注时、对象名称是使用短划线和箭头(->)分隔符的存储名称和卷名称的组合：

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

- 为存储、交换机或端口添加标注后、应用程序列将被忽略。
- 租户列、Line__of_Business列、Business-Unit列和Project列构成一个业务实体。

  任何值均可留空。如果某个应用程序已与与与输入值不同的业务实体相关、则会将该应用程序分配给新的业务实体。

导入实用程序支持以下对象类型和密钥：

Type	密钥

主机	id-><id> 或 <Name> 或 <IP>
虚拟机	id-><id> 或 <Name>
存储池	id-><id> 或 <Storage_name>-><Storage_Pool_name>
内部卷	id-><id> 或 <Storage_name>-><Internal_volume_name>
Volume	id-><id> 或 <Storage_name>-><Volume_name>
存储	id-><id> 或 <Name> 或 <IP>
交换机	id-><id> 或 <Name> 或 <IP>
Port	id-><id> 或 <WWN>
共享	id-><id> 或 <Storage Name>-><Internal Volume Name>-><Share Name>-><Protocol><Qtree> 如果存在默认qtree、则为可选。
qtree	id-><id> 或 <Storage Name>-><Internal Volume Name>-><Qtree Name>

CSV文件应使用以下格式：

```
, , <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>]
```

步骤

1. 登录到Insight Web UI。
2. 单击*管理*并选择*故障排除*。

   此时将显示Troubleshooting页面。

3. 在页面的*其他任务部分*中、单击* OnCommand Insight Portal"链接。
4. 单击* Insight Connect APi*。
5. 登录到门户。
6. 单击*标注导入实用程序*。
7. 保存 `.zip` 文件、解压缩并读取 `readme.txt` 追加信息 和示例的文件。
8. 将CSV文件置于与相同的文件夹中 `.zip` 文件
9. 在命令行窗口中、输入以下内容：

```
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
```

默认情况下、启用额外日志记录的-l选项和启用区分大小写的-c选项均设置为false。因此、只有在要使用这些功能时、才必须指定这些功能。

> 选项与其值之间没有空格。

> 以下关键字为保留关键字、可防止用户将其指定为标注名称：-应用程序-应用程序优先级-租户- Line__of_Business -业务单位-如果您尝试使用其中一个保留关键字导入标注类型、则会生成项目错误。如果您已使用这些关键字创建标注名称、则必须对其进行修改、以使导入实用程序工具能够正常工作。

> 标注导入实用程序需要Java 8或Java 11。在运行导入实用程序之前、请确保已安装其中一个。建议使用最新的OpenJDK 11。

使用查询为多个资产分配标注

为一组资产分配标注有助于您更轻松地在查询或信息板中识别或使用这些相关资产。

开始之前

您要分配给资产的标注必须事先已创建。

关于此任务

您可以使用查询来简化为多个资产分配标注的任务。例如、如果要为特定数据中心位置的所有阵列分配自定义地

址标注。

步骤

1. 创建新查询以确定要分配标注的资产。单击*查询*>*+新建查询*。
2. 在*搜索…下拉列表中、选择*存储。您可以设置筛选器以进一步缩小显示的存储列表范围。
3. 在显示的存储列表中、单击存储名称旁边的复选框以选择一个或多个存储。您也可以通过单击列表顶部的主复选框来选择显示的所有存储。
4. 选择所有所需存储后、单击*操作*>*编辑标注*。

   系统将显示添加标注对话框。

5. 选择要分配给存储的*标注*和*值*、然后单击*保存*。

   如果要显示该标注的列、则该列将显示在所有选定存储上。

6. 现在、您可以使用标注在小工具或查询中筛选存储。在小工具中、您可以执行以下操作：

   a. 创建信息板或打开现有信息板。添加*变量*并选择您在上述存储上设置的标注。变量将添加到信息板中。
   b. 在刚刚添加的变量字段中、单击*任何*并输入相应的值进行筛选。单击复选标记以保存变量值。
   c. 添加小工具。在小工具的"Query"中、单击"筛选方式"。
   d. 单击*任何*并选择您在上面添加的标注变量。您创建的变量以"`$`"开头、并显示在下拉列表中。
   e. 设置所需的任何其他筛选器或字段、然后在根据您的喜好自定义小工具后单击*保存*。

   信息板上的小工具仅显示分配了标注的存储的数据。

正在查询资产

通过查询、您可以根据用户选择的标准(标注和性能指标)在粒度级别搜索环境中的资产、从而监控网络并对其进行故障排除。此外、自动为资产分配标注的标注规则需要查询。

查询和信息板中使用的资产

Insight查询和信息板小工具可用于各种资产类型

以下资产类型可用于查询、信息板小工具和自定义资产页面。可用于筛选器，表达式和显示的字段和计数器因资产类型而异。并非所有资产都可以在所有小工具类型中使用。

- 应用程序
- 数据存储库
- Disk
- 网络结构
- 通用设备
- 主机

- 内部卷
- iSCSI 会话
- iSCSI 网络门户
- 路径
- Port
- qtree
- 配额
- 共享
- 存储
- 存储节点
- 存储池
- 交换机
- 磁带
- VMDK
- 虚拟机
- Volume
- 分区
- 区域成员

创建查询

您可以创建查询、以便在粒度级别搜索环境中的资产。通过查询、您可以通过添加筛选器并对结果进行排序来对数据进行分区、以便在一个视图中查看清单和性能数据。

关于此任务

例如、您可以为卷创建查询、添加筛选器以查找与选定卷关联的特定存储、添加筛选器以查找选定存储上的特定标注、例如第1层、 最后、添加另一个筛选器以查找IOPS -读取(IO/s)大于25的所有存储。显示结果后，您可以按升序或降序对与查询关联的信息列进行排序。

添加新的数据源以获取资产或进行任何标注或应用程序分配时、您可以在为查询编制索引后按定期计划的间隔查询这些资产、标注或应用程序。

步骤

1. 登录到OnCommand Insight Web UI。
2. 单击*查询*并选择*+新建查询*。
3. 单击*选择资源类型*并选择一种资产类型。

   为查询选择资源时、系统会自动显示多个默认列；您可以随时删除这些列或添加新列。

4. 在*名称*文本框中、键入资产的名称或键入部分文本以筛选资产名称。

您可以单独使用或组合使用以下任一项、以便在"新建查询"页面上的任何文本框中细化搜索范围：

- 星号可用于搜索所有内容。例如： `vol*rhel` 显示以"`vol`"开头、以"`RHEL`"结尾的所有资源。
- 问号用于搜索特定数量的字符。例如： `BOS-PRD??-S12` 显示BOS-PRD12-S12、BOS-PRD13-S12等。
- 或运算符可用于指定多个实体。例如： `FAS2240 OR CX600 OR FAS3270` 查找多个存储型号。
- 使用 NOT 运算符可以从搜索结果中排除文本。例如： `NOT EMC*` 查找不以"`EMC`"开头的所有内容。您可以使用 `NOT *` 以显示不包含任何值的字段。

5. 单击 ✔ 以显示资产。
6. 要添加条件、请单击 More ▾ 、并执行以下操作之一：
   - 键入以搜索特定条件、然后选择它。
   - 向下滚动列表并选择一个条件。
   - 如果选择IOPS -读取(IO/s)等性能指标、请输入一个值范围。Insight提供的默认标注以表示 🏷；可以使用名称重复的标注。

   此时将在查询结果列表中为条件添加一列、并且列表中的查询结果将更新。
7. 您也可以单击 ▦ 从查询结果中删除标注或性能指标。

   例如、如果您的查询显示数据存储库的最大延迟和最大吞吐量、而您希望在查询结果列表中仅显示最大延迟、请单击此按钮、然后清除*吞吐量-最大*复选框。"吞吐量-最大(MB/秒)"列将从"查询结果"列表中删除。

   > ⓘ 根据查询结果表中显示的列数、您可能无法查看其他添加的列。您可以删除一个或多个列、直到显示所需的列为止。

8. 单击*保存*、输入查询的名称、然后再次单击*保存*。

   如果您的帐户具有管理员角色、则可以创建自定义信息板。自定义信息板可以包含小工具库中的任何小工具、其中几个小工具可用于在自定义信息板中表示查询结果。有关自定义信息板的详细信息、请参见OnCommand Insight 入门指南_。

   - 相关信息 *

"导入和导出用户数据"

查看查询

您可以查看查询以监控资产并更改查询显示资产相关数据的方式。

步骤

1. 登录到OnCommand Insight Web UI。
2. 单击 * 查询 * 并选择 * 显示所有查询 * 。
3. 您可以通过执行以下任一操作来更改查询的显示方式：

- 您可以在*筛选器*框中输入文本进行搜索、以显示特定查询。
- 您可以通过单击列标题中的箭头将查询表中各列的排序顺序更改为升序（向上箭头）或降序（向下箭头）。
- 要调整列大小，请将鼠标悬停在列标题上，直到出现蓝条。将鼠标放在该条上并向右或向左拖动。
- 要移动列，请单击列标题并向右或向左拖动。
- 滚动浏览查询结果时、请注意、由于Insight会自动轮询数据源、结果可能会发生变化。这可能会导致某些项目丢失，或者某些项目出现无序，具体取决于它们的排序方式。

将查询结果导出到 .CSV 文件

您可能希望将查询结果导出到.CSV文件中、以便将数据导入到其他应用程序中。

步骤

1. 登录到OnCommand Insight Web UI。
2. 单击 * 查询 * 并选择 * 显示所有查询 * 。

   此时将显示 "Queries" 页面。

3. 单击一个查询。
4. 单击 将查询结果导出到.CSV 文件
5. 执行以下操作之一：
   - 单击 * 打开方式 * ，然后单击 * 确定 * 以使用 Microsoft Excel 打开文件并将文件保存到特定位置。
   - 单击 * 保存文件 * ，然后单击 * 确定 * 将文件保存到 "Downloads" 文件夹。仅导出显示列的属性。某些显示的列、尤其是属于复杂嵌套关系的列、不会导出。

     如果资产名称中显示逗号、则导出将以引号将名称括起来、从而保留资产名称和正确的.csv格式。

     +导出查询结果时、请注意、结果表中的*所有*行将被导出、而不仅仅是那些在屏幕上选择或显示的行、最多可导出10、000行。

使用 Excel 打开导出的 .CSV 文件时，如果您的对象名称或其他字段的格式为 NN： NN （两位数后跟一个冒号，再后跟两个数字），则 Excel 有时会将该名称解释为时间格式，而不是文本格式。这可能会导致 Excel 在这些列中显示不正确的值。例如，名为 "81： 45" 的对象将在 Excel 中显示为 "81： 45： 00" 。要解决此问题，请按照以下步骤将 .CSV 导入到 Excel 中：

+

```
-   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.
```

+

修改查询

如果要更改要查询的资产的搜索条件，可以更改与查询关联的条件。

步骤

1. 登录到InsightWeb UI。
2. 单击 * 查询 * 并选择 * 显示所有查询 * 。

   此时将显示 "Queries" 页面。

3. 单击查询名称。
4. 要从查询中删除条件、请单击 🗑 。
5. 要向查询添加条件，请单击 More ▾ 、然后从列表中选择一个条件。
6. 执行以下操作之一：
   - 单击*保存*以使用最初使用的名称保存查询。
   - 单击*另存为*以使用其他名称保存查询。
   - 单击*重命名*以更改最初使用的查询名称。
   - 单击*还原*将查询名称改回您最初使用的名称。

删除查询

当查询不再收集有关资产的有用信息时、您可以将其删除。如果查询在标注规则中使用、

则不能将其删除。

步骤

1. 登录到InsightWeb UI。
2. 单击 * 查询 * 并选择 * 显示所有查询 * 。

   此时将显示 "Queries" 页面。

3. 将光标置于要删除的查询上方并单击 🗑 。

   此时将显示一条确认消息、询问您是否要删除此查询。

4. 单击 * 确定 * 。

为资产分配多个应用程序或从资产中删除多个应用程序

您可以使用查询为资产分配多个应用程序或从资产中删除多个应用程序、而无需手动分配或删除这些应用程序。

开始之前

您必须已创建一个查询，用于查找要编辑的所有资产。

步骤

1. 单击 * 查询 * 并选择 * 显示所有查询 * 。

   此时将显示 "Queries" 页面。

2. 单击用于查找资产的查询的名称。

   此时将显示与查询关联的资产列表。

3. 在列表中选择所需资产或单击 ☐ ▾ 选择*全部*。

   此时将显示*操作*按钮。

4. 要将应用程序添加到选定资产，请单击 Actions ▾ 、然后选择*编辑应用程序*。
   a. 单击*应用程序*并选择一个或多个应用程序。

      您可以为主机、内部卷和虚拟机选择多个应用程序；但是、您只能为一个卷选择一个应用程序。

   b. 单击 * 保存 * 。
5. 要删除分配给资产的应用程序，请单击 Actions ▾ 并选择 * 删除应用程序 * 。
   a. 选择要删除的一个或多个应用程序。
   b. 单击 * 删除 * 。

您分配的任何新应用程序将覆盖资产上从其他资产派生的任何应用程序。例如，卷会继承主机中的应用程序，而在将新应用程序分配给卷时，新应用程序会优先于派生应用程序。

编辑或删除资产中的多个标注

您可以使用查询编辑资产的多个标注、也可以从资产中删除多个标注、而无需手动编辑或删除它们。

开始之前

您必须已创建一个查询、用于查找要编辑的所有资产。

步骤

1. 单击 * 查询 * 并选择 * 显示所有查询 * 。

   此时将显示 "Queries" 页面。

2. 单击用于查找资产的查询的名称。

   此时将显示与查询关联的资产列表。

3. 在列表中选择所需资产或单击 ☐ ▾ 选择*全部*。

   此时将显示*操作*按钮。

4. 要向资产添加标注或编辑分配给资产的标注的值、请单击 Actions ▾ 、然后选择*编辑标注*。
   a. 单击*标注*并选择要更改其值的标注、或者选择一个新标注以将其分配给所有资产。
   b. 单击 * 值 * 并为标注选择一个值。
   c. 单击 * 保存 * 。
5. 要删除分配给资产的标注、请单击 Actions ▾ 、然后选择*删除标注*。
   a. 单击*标注*、然后选择要从资产中删除的标注。
   b. 单击 * 删除 * 。

正在复制表值

您可以复制表中的值、以便在搜索框或其他应用程序中使用。

关于此任务

您可以使用两种方法从表或查询结果中复制值。

步骤

1. 方法 1 ： 使用鼠标突出显示所需文本，复制该文本并将其粘贴到搜索字段或其他应用程序中。

2. 方法2：对于长度超过表列宽度的单值字段(以省略号(…)表示)、请将鼠标悬停在该字段上、然后单击剪贴板图标。该值将复制到剪贴板，以在搜索字段或其他应用程序中使用。

   请注意、只能复制指向资产的链接值。另请注意、只有包含单个值的字段(即非列表)才会显示复制图标。

管理性能策略

通过OnCommand Insight 、您可以创建性能策略来监控网络中的各种阈值、并在超过这些阈值时发出警报。通过使用性能策略、您可以立即检测到违反阈值的情况、确定影响、并分析问题的影响和根发生原因 、从而可以快速有效地进行更正。

通过性能策略、您可以为任何对象(数据存储库、磁盘、虚拟机管理程序、内部卷、端口、 存储、存储节点、存储池、VMDK、虚拟机、 和卷)、并报告性能计数器(例如总IOPS)。如果发生违反阈值的情况、Insight会在相关资产页面中检测并报告该阈值、方法是显示一个红色实心圆；通过电子邮件警报(如果已配置)；以及在违规信息板或任何报告违规的自定义信息板中。

Insight为以下对象提供了一些默认性能策略、如果这些策略不适用于您的环境、您可以修改或删除这些策略：

- 虚拟机管理程序

  有ESX交换和ESX利用率策略。

- 内部卷和卷

  每个资源有两个延迟策略、一个用于标注第1层、另一个用于标注第2层。

- Port

  有一项BB信用零策略。

- 存储节点

  有一个节点利用率策略。

- 虚拟机

  有VM交换以及ESX CPU和内存策略。

- Volume

  存在按层划分的延迟以及未对齐的卷策略。

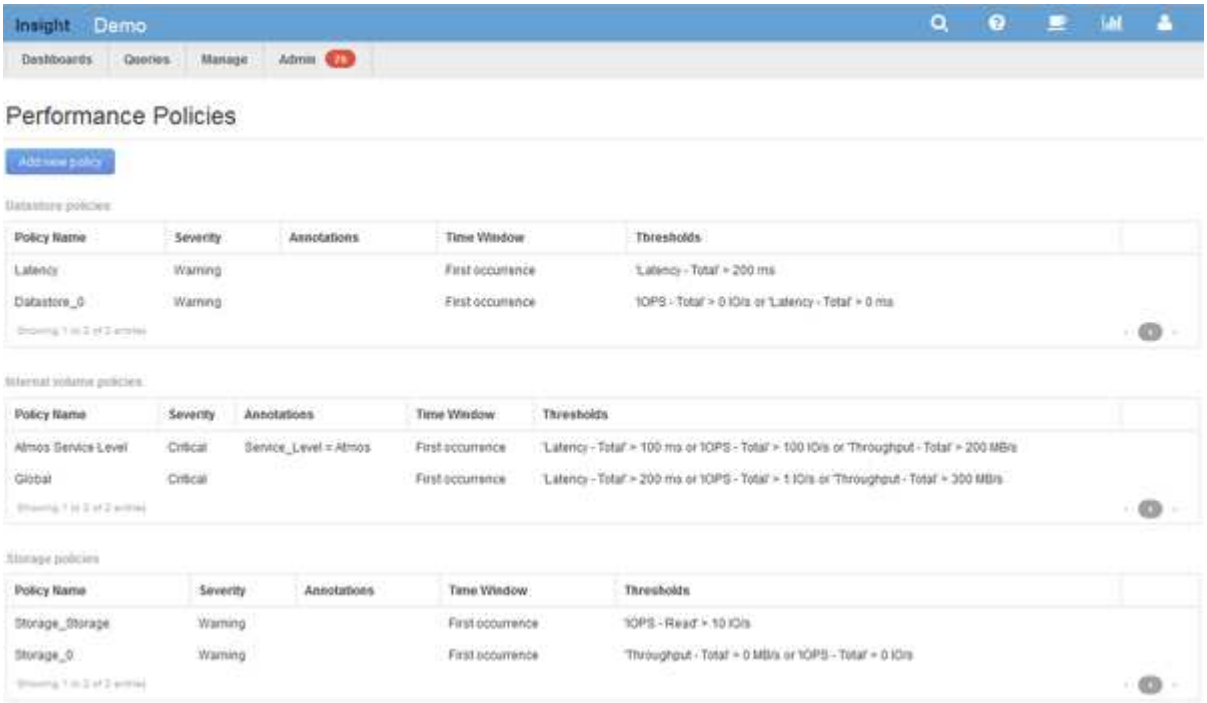
创建性能策略

您可以创建性能策略来设置阈值，这些阈值会触发警报，以向您通知与网络中资源相关的问题。例如，您可以创建一个性能策略，以便在存储池的总利用率超过 60% 时向您发出警报。

步骤

1. 在浏览器中打开OnCommand Insight。
2. 选择*管理*>*性能策略*。

   此时将显示性能策略页面。



   策略按对象进行组织、并按其在该对象的列表中显示的顺序进行评估。

3. 单击*添加新策略*。

   此时将显示添加策略对话框。

4. 在*策略名称*字段中、输入策略的名称。

   您必须使用与对象的所有其他策略名称不同的名称。例如、内部卷不能具有两个名为"`Latency`"的策略；但是、您可以为内部卷使用"`Latency`"策略、而为其他卷使用另一个"`Latency`"策略。最佳做法是，无论对象类型如何，始终为任何策略使用唯一名称。

5. 从*应用于类型*的对象列表中、选择策略所应用的对象类型。
6. 从*带标注*列表中、选择一个标注类型(如果适用)、然后在*值*框中为标注输入值、以便仅将策略应用于设置了此特定标注的对象。
7. 如果选择*端口*作为对象类型、请从*连接到*列表中选择端口连接到的对象。
8. 从*应用窗口后*列表中、选择何时发出警报以指示阈值违规。

   首次出现选项会在第一个数据样本超过阈值时触发警报。所有其他选项都会在超过阈值一次且至少在指定时间内持续超过阈值时触发警报。

9. 从 * 严重性 * 列表中，选择违规的严重性。
10. 默认情况下、有关策略违规的电子邮件警报将发送给全局电子邮件列表中的收件人。您可以覆盖这些设置，

以便将特定策略的警报发送给特定收件人。

- 单击链接打开收件人列表、然后单击*+*按钮添加收件人。该策略的违规警报将发送到列表中的所有收件人。

11. 单击*如果以下任一情况属实、则创建警报*部分中的*任何*链接、以控制警报的触发方式：
    - 任意

      这是默认设置、当超过与策略相关的任何阈值时、系统会创建警报。

    - 全部

      此设置会在超出策略的所有阈值时创建警报。如果选择*全部*、则为性能策略创建的第一个阈值称为主规则。您必须确保主规则阈值是您最关心的性能策略违规。

12. 在 * 创建警报 if* 部分中，选择性能计数器和运算符，然后输入一个值以创建阈值。
13. 单击*添加阈值*以添加更多阈值。
14. 要删除阈值、请单击垃圾桶图标。
15. 如果希望策略在发生警报时停止处理、请选中*如果生成警报、则停止处理其他策略*复选框。

    例如、如果数据存储库有四个策略、而第二个策略配置为在发生警报时停止处理、则在第二个策略违规处于活动状态时、不会处理第三个和第四个策略。

16. 单击 * 保存 * 。

    此时将显示"性能策略"页面、并且性能策略将显示在对象类型的策略列表中。

性能策略评估优先级

"性能策略"页面按对象类型对策略进行分组、Insight将按照策略在对象的性能策略列表中的显示顺序对策略进行评估。您可以更改Insight评估策略的顺序、以显示对您网络中最重要的信息。

Insight会在将某个对象的性能数据样本提取到系统中时按顺序评估适用于该对象的所有策略；但是、根据标注、并非所有策略都适用于一组对象。例如、假设内部卷具有以下策略：

- 策略1 (Insight提供的默认策略)
- 策略2 (标注为`Sservice level = Silver`)、并带有*如果生成警报、则停止处理其他策略*选项
- 策略3 (标注为"`S服务级别=金牌`")
- 策略4

对于标注为Gold的内部卷层、Insight会评估策略1、忽略策略2、然后评估策略3和策略4。对于未标注的层、Insight按策略顺序进行评估；因此、Insight仅评估策略1和策略4。对于标注为银牌的内部卷层、Insight会评估策略1和策略2； 但是、如果在超出策略阈值一次并在策略中指定的时间范围内连续超出此阈值时触发警报、则Insight将不再评估列表中的其他策略、而是评估对象的当前计数器。当Insight捕获对象的下一组性能示例时、它再次开始按筛选器评估对象的性能策略、然后进行排序。

更改性能策略的优先级

默认情况下、Insight会按顺序评估对象的策略。您可以配置Insight评估性能策略的顺序。例如、如果您已将某个策略配置为在黄金层存储发生违规时停止处理、则可以将该策略放在列表中的第一位、并避免看到同一存储资产的更多常规违规。

步骤

1. 在浏览器中打开Insight。
2. 从*管理*菜单中、选择*性能策略*。

   此时将显示性能策略页面。

3. 将光标悬停在对象类型的性能策略列表中的策略名称上。

   优先级箭头显示在策略右侧。

4. 要在列表中将策略上移、请单击向上箭头；要在列表中将策略下移、请单击向下箭头。

   默认情况下、新策略会按顺序添加到对象的策略列表中。

编辑性能策略

您可以编辑现有和默认性能策略、以更改Insight监控网络中您感兴趣的条件的方式。例如、您可能希望更改策略的阈值。

步骤

1. 在浏览器中打开Insight。
2. 从*管理*菜单中、选择*性能策略*。

   此时将显示性能策略页面。

3. 将光标悬停在对象性能策略列表中的策略名称上。
4. 单击 。

   此时将显示编辑策略对话框。

5. 进行所需的更改。

   如果更改策略名称以外的任何选项、Insight将删除该策略的所有现有违规。

6. 单击*保存。*

正在删除性能策略

如果您认为某个性能策略不再适用于监控网络中的对象、则可以将其删除。

步骤

1. 在浏览器中打开Insight。
2. 从*管理*菜单中、选择*性能策略*。

   此时将显示性能策略页面。

3. 将光标悬停在对象性能策略列表中的策略名称上。
4. 单击 ✖。

   此时将显示一条消息、询问您是否要删除此策略。

5. 单击 * 确定 * 。

导入和导出用户数据

通过导入和导出功能、您可以将标注、标注规则、查询、性能策略和自定义信息板导出到一个文件。然后、可以将此文件导入到不同的OnCommand Insight 服务器中。

只有运行相同版本OnCommand Insight 的服务器之间才支持导出和导入功能。

要导出或导入用户数据、请单击*管理*并选择*设置*、然后选择*导入/导出用户数据*选项卡。

在导入操作期间，系统会根据要导入的对象和对象类型添加，合并或替换数据。

- 标注类型
  - 如果目标系统中不存在同名标注、则添加标注。
  - 如果标注类型为列表，并且目标系统中存在同名标注，则合并标注。
  - 如果标注类型不是列表，并且目标系统中存在同名标注，则替换标注。

  > 如果目标系统中存在同名但类型不同的标注、导入将失败。如果对象依赖于失败的标注，则这些对象可能显示不正确或不需要的信息。导入操作完成后，您必须检查所有标注依赖关系。

- 标注规则
  - 如果目标系统中不存在同名标注规则、则添加标注规则。
  - 如果目标系统中存在同名标注规则、则替换标注规则。

  > 标注规则取决于查询和标注。导入操作完成后、您必须检查所有标注规则的准确性。

- 策略
  - 如果目标系统中不存在同名策略、则添加策略。
  - 如果目标系统中存在同名策略、则替换策略。

> 导入操作完成后、策略可能会无序。必须在导入后检查策略顺序。如果标注不正确、则依赖于标注的策略可能会失败。您必须在导入后检查所有标注依赖关系。
>
> +

- 查询
  - 如果目标系统中不存在同名查询、则添加查询。
  - 如果目标系统中存在同名查询、则替换查询、即使查询的资源类型不同也是如此。

> 如果查询的资源类型不同、则在导入后、使用该查询的任何信息板小工具可能会显示不需要的或不正确的结果。导入后、您必须检查所有基于查询的小工具的准确性。如果标注不正确、则依赖于标注的查询可能会失败。您必须在导入后检查所有标注依赖关系。
>
> +

- 信息板
  - 如果目标系统中不存在同名信息板、则添加信息板。
  - 如果目标系统中存在同名信息板、则替换信息板、即使查询的资源类型不同也是如此。

> 导入后、您必须检查信息板中所有基于查询的小工具的准确性。如果源服务器具有多个同名信息板、则所有信息板都将导出。但是、只会将第一个导入到目标服务器中。为了避免导入期间出现错误、您应确保信息板在导出之前具有唯一的名称。
>
> +